Workplace Monitoring Laws

There are no federal statutes which regulate private employers on broad workplace privacy issues; however, federal laws do regulate specific aspects of privacy that arise during the employment relationship. For example, the **Federal Privacy Act** restricts the collection of information and regulates access to information for federal employees and covers private employers who have federal contracts requiring specific recordkeeping obligations. The **Federal Wiretapping Act/Electronic Communications Privacy Act** prohibits the intentional interception or disclosure of any wire, oral, or electronic communication where there is a reasonable expectation of privacy. There are two exceptions: (1) if one party to the communication has consented, electronic monitoring is allowed, and (2) a business use exemption permits telephone extension equipment used to monitor communications within the ordinary course of business. In addition to the federal privacy laws, many states have adopted comparable statutes that may impact an employee monitoring program. A great number of states have either wiretapping laws or statutes regulating employee monitoring, or both. As is normally the case, a thorough review of relevant state law should precede the implementation of any policy that may appear to impact employees' privacy interests.

To check whether there is pending legislative issues or recently enacted legislative changes for your state(s) please click here.

To access additional SHRM State Law & Regulation Resources click here.

If a state does not appear on the following chart it is due to our not finding any evidence a statute exists for that state. In some cases provisions only exist for public employers.

Click the letter corresponding to the state name below.

A | **C** | **D** | **F** | **G** | **H** | **I** | **K** | **L** | **M** | **N** | **O** | **P** | **R** | **S** | **T** | **U** | **V** | **W**

State	Statute
Alabama	**13A-11-31. Criminal eavesdropping.** (a) A person commits the crime of criminal eavesdropping if he intentionally uses any device to eavesdrop, whether or not he is present at the time. (b) Criminal eavesdropping is a Class A misdemeanor.
Alaska	**42.20.310. Eavesdropping.** (a) A person may not (1) use an eavesdropping device to hear or record all or any part of an oral conversation without the consent of a party to the conversation; (2) use or divulge any information which the person knows or reasonably should know was obtained through the illegal use of an eavesdropping device for personal benefit or another's benefit; (3) publish the existence, contents, substance, purport, effect, or meaning of any conversation the person has heard through the illegal use of an eavesdropping device; (4) divulge, or publish the existence, contents, substance, purport, effect, or meaning of any conversation the person has become acquainted with after the person knows or reasonably should know that the conversation and the information contained in the conversation was obtained through the illegal use of an eavesdropping device. (b) In this section "eavesdropping device" means any device capable of being used to hear or record oral conversation whether the conversation is conducted in person, by telephone, or by any other means;

	provided that this definition does not include devices used for the restoration of the deaf or hard-of-hearing to normal or partial hearing.
Arizona	**13-3005. Interception of wire, electronic and oral communications; installation of pen register or trap and trace device; classification; exceptions** A. Except as provided in this section and section 13-3012, a person is guilty of a class 5 felony who either: 1. Intentionally intercepts a wire or electronic communication to which he is not a party, or aids, authorizes, employs, procures or permits another to so do, without the consent of either a sender or receiver thereof. 2. Intentionally intercepts a conversation or discussion at which he is not present, or aids, authorizes, employs, procures or permits another to so do, without the consent of a party to such conversation or discussion. 3. Intentionally intercepts the deliberations of a jury or aids, authorizes, employs, procures or permits another to so do. B. Except as provided in sections 13-3012 and 13-3017, a person who intentionally and without lawful authority installs or uses a pen register or trap and trace device on the telephone lines or communications facilities of another person which are utilized for wire or electronic communication is guilty of a class 6 felony.
Arkansas	**5-60-120. Interception and recording.** (a) It is unlawful for a person to intercept a wire, landline, oral,telephonic communication, or wireless communication, and to record or possess a recording of the communication unless the person is a party to the communication or one (1) of the parties to the communication has given prior consent to the interception and recording. (b) Any violation of this section is a Class A misdemeanor. (c)(1) It is not unlawful for the act to be committed by a person acting under the color of law. (2) It is an exception to the application of subsection (a) of this section that an officer, employee, or agent of a public telephone utilityor company that is licensed by a federal or state agency to provide wire or wireless telecommunication service to the public provides information, facilities, or technical assistance to a person acting under the color of law to intercept a wire, wireless, oral, or telephonic communication. (3) It is not unlawful under this section for an operator of a switchboard, or an officer, employee, or agent of any public telephone utility or telecommunications provider whose facilities are used in the transmission of a wire communication to intercept, disclose, or use that communication in the normal course of his or her employment while engaged in any activity which is a necessary incident to the rendition of his or her service or to the protection of the rights or property of the telecommunications provider or public telephone utility of the communication. (d) The provisions of this section do not apply to a: (1) Telecommunication service offered by a telecommunications provider or public telephone utility; or (2) Federal Communications Commission licensed amateur radio operator. (e) Nothing in this section shall be interpreted to prohibit or restrict a Federal Communications Commission licensed amateur radio operator or anyone operating a police scanner from intercepting a communication for pleasure. (f) Consistent with the provisions of 18 U.S.C. § 2703, as it existed on January 1, 2003, the issuance of a court order for disclosure of a customer communication or record to a governmental entity requiring the information as part of an ongoing criminal investigation is not prohibited by the laws of this state. (g) Consistent with the provisions of 18 U.S.C. §§ 3122 — 3127, as they existed on January 1, 2003, the issuance of a court order authorizing or approving the installation and use of a pen register or a trap-and-trace device as part of an ongoing criminal investigation is not prohibited by the laws of this state.
California	**631 Penal--(**a) Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by imprisonment in the state prison, or by both a fine and imprisonment in the county jail or in the state prison. If the person has previously been convicted of a violation of this section or Section 632, 632.5, 632.6, 632.7, or 636, he or she is punishable by a fine not exceeding ten thousand dollars

	($10,000), or by imprisonment in the county jail not exceeding one year, or by imprisonment in the state prison, or by both a fine and imprisonment in the county jail or in the state prison. (b) This section shall not apply (1) to any public utility engaged in the business of providing communications services and facilities, or to the officers, employees or agents thereof, where the acts otherwise prohibited herein are for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility, or (2) to the use of any instrument, equipment, facility, or service furnished and used pursuant to the tariffs of a public utility, or (3) to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility. (c) Except as proof in an action or prosecution for violation of this section, no evidence obtained in violation of this section shall be admissible in any judicial, administrative, legislative, or other proceeding. **435. Monitoring employees in restrooms, locker rooms or dressing rooms prohibited; Exception**—(a) No employer may cause an audio or video recording to be made of an employee in a restroom, locker room, or room designated by an employer for changing clothes, unless authorized by court order. (b) No recording made in violation of this section may be used by an employer for any purpose. This section applies to a private or public employer, except the federal government. (c) A violation of this section constitutes an infraction. **15 M.R.S.A. § 710. Offenses 1. Interception, oral communications prohibited**. Any person, other than an employee of a common carrier as defined in this chapter, a law enforcement officer or an investigative officer as defined in this chapter, carrying out practices otherwise permitted by this chapter, who intentionally or knowingly intercepts, attempts to intercept or procures any other person to intercept or attempt to intercept, any wire or oral communication is guilty of a Class C crime. **2. Editing of tape recordings in judicial proceedings prohibited**. Any person who knowingly or intentionally edits, alters or tampers with any tape, transcription or other sound recording, or knows of such editing, altering or tampering, and presents that recording in any judicial proceeding or proceeding under oath, without fully indicating the nature of the changes made and the original state of the recording, is guilty of a Class C crime. **3. Disclosure, or use of wire or oral communications prohibited**. A person is guilty of a Class C crime if he: A. Intentionally or knowingly discloses or attempts to disclose to any person the contents of any wire or oral communication, knowing that the information was obtained through interception; or B. Intentionally or knowingly uses or attempts to use the contents of any wire or oral communication, knowing that the information was obtained through interception. **4. Duty to report**. Any communications common carrier shall promptly report to the Attorney General any facts coming to its attention in the conduct of its business which may indicate a possible violation of this section and such carrier shall adopt reasonable rules to assure compliance with this subsection, provided such carrier shall not be liable to any person who may claim an injury arising out of any such report, if made in good faith. Any person violating this subsection shall be subject to a civil penalty not to exceed $5,000, payable to the State, to be recovered in a civil action. **5. Possession of interception devices prohibited**. A person, other than an employee of a common carrier as defined in this chapter, a law enforcement officer or an investigative officer as defined in this chapter, carrying out practices otherwise permitted by this chapter, who has in his possession any device, contrivance, machine or apparatus designed or commonly used for intercepting wire or oral communications defined in this chapter, is guilty of a Class C crime. **6. Sale of interception devices prohibited**. A person who sells, exchanges, delivers, barters, gives or furnishes or possesses with an intent to sell any device, contrivance, machine or apparatus designed or commonly used for the interception of wire or oral communications as defined in this chapter is guilty of a Class B crime. This subsection shall not include devices manufactured under written contract for sale to common carriers, law enforcement agencies and the Department of Corrections, provided that the production of any such device shall not have commenced prior to the signing of the contract by both parties.
Colorado	**18-9-302. Wiretapping and eavesdropping devices prohibited — penalty.** --Any person who manufactures, buys, sells, or knowingly has in his possession any instrument, device, contrivance, machine, or apparatus designed or commonly used for wiretapping or eavesdropping, as prohibited in sections 18-9-303 and 18-9-304, with the intent to unlawfully use or employ or allow the same to be

	so used or employed, or who knowingly aids, authorizes, agrees with, employs, permits, or conspires with any person to unlawfully manufacture, buy, sell, or have the same in his possession is guilty of a class 2 misdemeanor. Upon commission of a second or subsequent offense, any person committing the same commits a class 5 felony.
Connecticut	**53a-188. Tampering with private communications: Class A misdemeanor.** (a) A person is guilty of tampering with private communications when: (1) Knowing that he does not have the consent of the sender or receiver, he obtains from an employee, officer or representative of a telephone or telegraph corporation, by connivance, deception, intimidation or in any other manner, information with respect to the contents or nature of a telephonic or telegraphic communication; or (2) knowing that he does not have the consent of the sender or receiver, and being an employee, officer or representative of a telephone or telegraph corporation, he knowingly divulges to another person the contents or nature of a telephonic or telegraphic communication. (b) Tampering with private communications is a class A misdemeanor. **52-570d. Action for illegal recording of private telephonic communications.** (a) No person shall use any instrument, device or equipment to record an oral private telephonic communication unless the use of such instrument, device or equipment (1) is preceded by consent of all parties to the communication and such prior consent either is obtained in writing or is part of, and obtained at the start of, the recording, or (2) is preceded by verbal notification which is recorded at the beginning and is part of the communication by the recording party, or (3) is accompanied by an automatic tone warning device which automatically produces a distinct signal that is repeated at intervals of approximately fifteen seconds during the communication while such instrument, device or equipment is in use. (b) The provisions of subsection (a) of this section shall not apply to: (1) Any federal, state or local criminal law enforcement official who in the lawful performance of his duties records telephonic communications; (2) Any officer, employee or agent of a public or private safety agency, as defined in section 28-25, who in the lawful performance of his duties records telephonic communications of an emergency nature; (3) Any person who, as the recipient of a telephonic communication which conveys threats of extortion, bodily harm or other unlawful requests or demands, records such telephonic communication; (4) Any person who, as the recipient of a telephonic communication which occurs repeatedly or at an extremely inconvenient hour, records such telephonic communication; (5) Any officer, employee or agent of any communication common carrier who in the lawful performance of his duties records telephonic communications or provides facilities to an investigative officer or criminal law enforcement official authorized pursuant to chapter 959a to intercept a wire communication; (6) Any officer, employee or agent of a Federal Communications Commission licensed broadcast station who records a telephonic communication solely for broadcast over the air; (7) Any officer, employee or agent of the United States Secret Service who records telephonic communications which concern the safety and security of the President of the United States, members of his immediate family or the White House and its grounds; and (8) Any officer, employee or agent of a Federal Communications Commission broadcast licensee who records a telephonic communication as part of a broadcast network or cooperative programming effort solely for broadcast over the air by a licensed broadcast station. (c) Any person aggrieved by a violation of subsection (a) of this section may bring a civil action in the Superior Court to recover damages, together with costs and a reasonable attorney's fee. **31-48b. Use of electronic surveillance devices by employers limited. Prohibition on recording negotiations between employers and employees.** (a) For purposes of this section, "employer" means the owner or owners in the case of an unincorporated business, the partners in the case of a partnership, the officers in the case of a corporation or in the case of the state, any town, city or borough, or district, local or regional board of education, or housing authority or district department of health, the chief executive officer thereof. (b) No employer or agent or representative of an employer shall operate any electronic surveillance device or system, including but not limited to the recording of sound or voice or a closed circuit television system, or any combination thereof, for the purpose of recording or monitoring the activities of his employees in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as rest rooms, locker rooms or lounges. (c) Any employer, who violates any provision of subsection (b) of this section shall, for the first offense, be fined five hundred dollars, for the second offense be fined one thousand dollars and

	for the third and any subsequent offense be imprisoned thirty days. (d) No employer or his agent or representative and no employee or his agent or representative shall intentionally overhear or record a conversation or discussion pertaining to employment contract negotiations between the two parties, by means of any instrument, device or equipment, unless such party has the consent of all parties to such conversation or discussion. (e) Any employer or his agent or representative or any employee or his agent or representative who violates any provision of subsection (d) of this section shall be fined one thousand dollars or imprisoned one year, or both. **31-48d.** Employers must give employees written notice prior to electronic monitoring; Exception where criminal conduct suspect; Penalty for violations—(a) As used in this section (1) "Employer" means any person, firm or corporation, including the state and any political subdivision of the state which has employees; (2) "Employee" means any person who performs services for an employer in a business of the employer, if the employer has the right to control and direct the person as to (A) the result to be accomplished by the services, and (B) the details and means by which such result is accomplished; and (3) "Electronic monitoring" means the collection of information on an employer's premises concerning employees' activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems, but not including the collection of information (A) for security purposes in common areas of the employer's premises which are held out for use by the public, or (B) which is prohibited under state or federal law. (b) (1) Except as provided in subdivision (2) of this subsection, each employer who engages in any type of electronic monitoring shall give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur. Each employer shall post, in a conspicuous place which is readily available for viewing by its employees, a notice concerning the types of electronic monitoring which the employer may engage in. Such posting shall constitute such prior written notice. (2) When (A) an employer has reasonable grounds to believe that employees are engaged in conduct which (i) violates the law, (ii) violates the legal rights of the employer or the employer's employees, or (iii) creates a hostile workplace environment, and (B) electronic monitoring may produce evidence of this misconduct, the employer may conduct monitoring without giving prior written notice. (c) The Labor Commissioner may levy a civil penalty against any person that the commissioner finds to be in violation of subsection (b) of this section, after a hearing conducted in accordance with sections 4-176e to 4-184, inclusive, of the general statutes. The maximum civil penalty shall be five hundred dollars for the first offense, one thousand dollars for the second offense and three thousand dollars for the third and each subsequent offense. (d) The provisions of this section shall not apply to a criminal investigation. Any information obtained in the course of a criminal investigation through the use of electronic monitoring may be used in a disciplinary proceeding against an employee. **31-48b. Electronic surveillance devices, Restricted use; Negotiations between employers and employees not to be recorded unless there is consent**—(a) For purposes of this section, "employer" means the owner or owners in the case of an unincorporated business, the partners in the case of a partnership, the officers in the case of a corporation or in the case of the state, any town, city or borough, or district, local or regional board of education, or housing authority or district department of health, the chief executive officer thereof. (b) No employer or agent or representative of an employer shall operate any electronic surveillance device or system, including but not limited to the recording of sound or voice or a closed circuit television system, or any combination thereof, for the purpose of recording or monitoring the activities of his employees in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as rest rooms, locker rooms or lounges. (c) Any employer, who violates any provision of subsection (b) of this section shall, for the first offense, be fined five hundred dollars, for the second offense be fined one thousand dollars and for the third and any subsequent offense be imprisoned thirty days. (d) No employer or his agent or representative and no employee or his agent or representative shall intentionally overhear or record a conversation or discussion pertaining to employment contract negotiations between the two parties, by means of any instrument, device or equipment, unless such party has the consent of all parties to such conversation or discussion. (e) Any employer or his agent or representative or any employee or his agent or representative who violates any provision of subsection (d) of this section shall be fined one thousand dollars or imprisoned one year, or both.

Delaware	**1335. Violation of privacy; class A misdemeanor; class G felony.** (a) A person is guilty of violation of privacy when, except as authorized by law, the person: (1) Trespasses on property intending to subject anyone to eavesdropping or other surveillance in a private place; or (2) Installs in any private place, without consent of the person or persons entitled to privacy there, any device for observing, photographing, recording, amplifying or broadcasting sounds or events in that place; or (3) Installs or uses outside a private place any device for hearing, recording, amplifying or broadcasting sounds originating in that place which would not ordinarily be audible or comprehensible outside, without the consent of the person or persons entitled to privacy there; or (4) Intercepts without the consent of all parties thereto a message by telephone, telegraph, letter or other means of communicating privately, including private conversation; or (5) Divulges without the consent of the sender and the receiver the existence or contents of any message by telephone, telegraph, letter or other means of communicating privately if the accused knows that the message was unlawfully intercepted or if the accused learned of the message in the course of employment with an agency engaged in transmitting it. (6) Tape records, photographs, films, videotapes or otherwise reproduces the image of another person who is getting dressed or undressed or has his/her genitals, buttocks or her breasts exposed, without consent, in any place where persons normally disrobe including but not limited to a fitting room, dressing room, locker room or bathroom, where there is a reasonable expectation of privacy. This paragraph shall not apply to any acts done by a parent or guardian inside of his or her dwelling, or upon his or her real property, when a subject of victim of such acts is intended to be any child of such parent or guardian who has not yet reached his or her eighteenth birthday and whose primary residence is in or upon the dwelling or real property of the parent or guardian, unless the acts done by the parent or guardian are intended to produce sexual gratification for any person in which case this paragraph shall apply. (7) Secretly or surreptitiously videotapes, films, photographs or otherwise records another person under or through his or her clothing for the purpose of viewing the body of or the undergarments worn by that other person. (8) knowingly installs an electronic or mechanical location tracking device in or on a motor vehicle without the consent of the registered owner, less or or lessee of said vehicle. This paragraph shall not apply to the lawful use of an electronic tracking device by a law enforcement officer, nor shall it apply to a parent or legal guardian who installs such a device for the purpose of tracking the location of a minor child thereof. (b) This section does not apply to: (1) Overhearing of messages through a regularly installed instrument on a telephone party line or an extension or any other regularly installed instrument or equipment; or (2) Acts done by the telephone company or subscribers incident to the enforcement of telephone company regulations or subscriber rules relating to the use of facilities; or (3) Acts done by personnel of any telephone or telegraph carrier in the performance of their duties in connection with the construction, maintenance or operation of a telephone or telegraph system; or (4) The divulgence of the existence of any message in response to a subpoena issued by a court of competent jurisdiction or a governmental body having subpoena powers; or (5) Acts done by police officers as provided in §§ 1336 [Repealed] and 1431 of this title. (c) Any violation of subdivisions (a)(1), (a)(2), (a)(3), (a)(4) (a)(5), or (a)(8) of this section shall be a class A misdemeanor. Any violation of subdivision (a)(6) or (a)(7) of this section shall be a class G felony. **705. Monitoring of employees' telephone calls/transmissions, E-mail, and/or internet use; "Employer" defined; Prior notification required; Applicability; Penalty for violations**—(a) As used in this section, "employer" includes any individual, corporation, partnership, firm, association, and the State of Delaware or any agency or political subdivision thereof. (b) No employer, nor any agent or any representative of any employer, shall monitor or otherwise intercept any telephone conversation or transmission, electronic mail or transmission, or Internet access or usage of or by a Delaware employee unless the employer either: (1) provides an electronic notice of such monitoring or intercepting policies or activities to the employee at least once during each day the employee accesses the employer provided E-mail or Internet access services; or (2) has first given a one-time notice to the employee of such monitoring or intercepting activity or policies. The notice required by this subsection (b)(2) shall be in writing, in an electronic record, or in another electronic form and acknowledged by the employee either in writing or electronically. The notice required by this subsection shall not apply to activities of any law enforcement officer acting under the order of a Court issued pursuant to Chapter 24 of Title 11. (c) Whoever violates this section shall be subject to a civil penalty of $100 for each such violation. A civil penalty claim may be filed in any court of

	competent jurisdiction. (d) The provisions of this section shall not be deemed to be an exclusive remedy and shall not otherwise limit or bar any person from pursuing any other remedies available under any other law, state or federal statute, or the common law. The violations of this section by an employer shall not be admitted into evidence for the purpose of, or used as, a defense to criminal liability of any person in any Court in this State. (e) The provisions of this section shall not apply to processes that are designed to manage the type or volume of incoming or outgoing electronic mail or telephone voice mail or internet usage, that are not targeted to monitor or intercept the electronic mail or telephone voice mail or internet usage of a particular individual, and that are performed solely for the purpose of computer system maintenance and/or protection.
District of Columbia	**23-542. Interception, disclosure, and use of wire or oral communications prohibited. (**a) Except as otherwise specifically provided in this subchapter, any person who in the District of Columbia (1) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire or oral communication; (2) willfully discloses or endeavors to disclose to any other person the contents of any wire or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication; or (3) willfully uses or endeavors to use the contents of any wire or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the interception of a wire or oral communication; shall be fined not more than $10,000 or imprisoned not more than five years, or both; except that paragraphs (2) and (3) of this subsection shall not apply to the contents of any wire or oral communication, or evidence derived therefrom, that has become common knowledge or public information. (b) It shall not be unlawful under this section for (1) an operator of a switchboard, or an officer, agent, or employee of a communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication, in the normal course of his employment while engaged in any activity which is a necessary incident to the rendering of his service or to the protection of the rights or property of the carrier of such communication, or to provide information, facilities, or technical assistance to an investigative or law enforcement officer who, under this subchapter, is authorized to intercept a wire or oral communication, but no communication common carrier shall utilize service observing or random monitoring except for mechanical or service quality control checks; (2) a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication, or where one of the parties to the communication has given prior consent to such interception; or (3) a person not acting under color of law to intercept a wire or oral communication, where such person is a party to the communication, or where one of the parties to the communication has given prior consent to such interception, unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States, any State, or the District of Columbia, or for the purpose of committing any other injurious act. **23-543. Possession, sale, distribution, manufacture, assembly, and advertising of wire or oral communication intercepting devices prohibited. (**a) Except as otherwise specifically provided in subsection (b) of this section, any person who in the District of Columbia (1) willfully possesses, sells, distributes, manufactures, or assembles an intercepting device, the design of which renders it primarily useful for the purpose of the surreptitious interception of a wire or oral communication; or (2) willfully places in any newspaper, magazine, handbill, or other publication any advertisement of (A) any intercepting device, the design of which renders it primarily useful for the purpose of the surreptitious interception of a wire or oral communication; or (B) any intercepting device where such advertisement promotes the use of such device for the purpose of the surreptitious interception of a wire or oral communication; shall be fined not more than $10,000 or imprisoned not more than five years, or both. (b) It shall not be unlawful under this section for (1) a communication common carrier or an officer, agent, or employee of, or a person under contract with a communication common carrier, in the usual course of the communication common carrier's business; or (2) a person under contract with the Government of the United States, a State or a political subdivision thereof, or the District of Columbia, or an officer, agent, or employee of the Government of the United States, a State or a political subdivision thereof, or the District of Columbia; to possess, sell, distribute, manufacture or assemble, or advertise any intercepting device, while acting in furtherance of the appropriate activities of the United States, a State or political subdivision thereof, the District of Columbia, or a

	communication common carrier. **23-544. Confiscation of wire or oral communication intercepting devices.** Any intercepting device in the District of Columbia (1) possessed; (2) used; (3) sold; 4) distributed; or (5) manufactured or assembled; in violation of section 23-542 or 23-543 may be seized and forfeited to the District of Columbia. Insofar as applicable and not inconsistent with the provisions of this chapter, all provisions of law relating to the seizure, summary and judicial forfeiture, and condemnation of property for violation of the customs laws; the disposition of such property; the remission or mitigation of such forfeitures; the compromise of claims; and the award of compensation to informers in respect of such forfeitures shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this title; except that such duties as are imposed upon the customs officer or any other person with respect to the seizure and forfeiture of property under the customs laws shall be performed with respect to seizures and forfeitures of property under this section by such officers, agents or other persons as may be authorized or designated for that purpose by the Mayor, except to the extent that such duties arise from seizures and forfeitures effected by any customs officer. The proceeds from the sale of any property forfeited under this section shall be deposited in the Treasury to the credit of the general fund of the District of Columbia. **23-545. Immunity of witnesses**--Repealed. **23-546. Applications for authorization or approval of interception of wire or oral communications**. (a) The United States attorney may authorize, in writing, any investigative or law enforcement officer to make application to a court for an order authorizing the interception of wire or oral communications. (b)The United States attorney may authorize, in writing, any investigative or law enforcement officer to make application to a court for an order of approval of the previous interception of any wire or oral communication, when the contents of such communication (1) relate to an offense other than that specified in an order of authorization; (2) were intercepted in an emergency situation; or (3) were intercepted in an emergency situation and relate to an offense other than that contemplated at the time the interception was made. (c) An application for an order of authorization (as provided in subsection (a) of this section) or of approval (as provided in paragraph (2) of subsection (b) of this section) may be authorized only when the interception of wire or oral communications may provide or has provided evidence of the commission of or a conspiracy to commit any of the following offenses: (1) Any of the offenses specified in the Act entitled "An Act to establish a code of law for the District of Columbia", approved March 3, 1901. (2) Bribery as specified in the Act of February 26, 1936 (D.C. Code, sec. 22-704). (3) Threats as specified in section 1501 of the Omnibus Crime Control and Safe Streets Act of 1968 (D.C. Code, secs. 22-5106, 22-1810). (4) Offenses involving the manufacture, distribution, or possession with intent to manufacture or distribute controlled substances as specified in sections 401 through 403 of the District of Columbia Uniform Controlled Substances Act of 1981, effective August 5, 1981 (D.C. Code, secs. 48-904.01 through 48-904.03). (5) Any of the offenses specified in the District of Columbia Theft and White Collar Crimes Act of 1982. **131 23-547. Procedure for authorization or approval of interception of wire or oral communications.** (a) Each application for an order authorizing or approving the interception of a wire or oral communication shall be made in writing upon oath or affirmation to a judge and shall state the applicant's authority to make the application. Each application shall include (1) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application; (2) a full and complete statement of the facts and circumstances relied upon by the applicant to justify his belief that an order should be issued, including (A) details as to the particular offense that has been, is being, or is about to be committed, (B) a particular description of the nature and location of the facilities from which or the place where the communication is to be or was intercepted, (C) a particular description of the type of communications sought to be or which were intercepted, and (D) the identity of the person, if known, who committed, is committing, or is about to commit the offense and whose communications are to be or were intercepted; (3) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear or appeared to be unlikely to succeed if tried or to be too dangerous; (4) a statement

	of the period of time for which the interception is or was required to be maintained, and if the nature of the investigation is or was such that the authorization for interception should not automatically terminate or should not have automatically terminated when the described type of communication has been or was first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will or would occur thereafter; (5) a full and complete statement of the facts concerning all previous applications, known to the individual authorizing or making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire or oral communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application; and (6) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain results. (b) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application. (c) Upon application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire or oral communications within the District of Columbia, if the judge determines on the basis of the facts submitted by the applicant that (1) there is or was probable cause for belief that the person whose communication is to be or was interpreted is or was committing, has committed, or is about to commit a particular offense enumerated in section 23-546; (2) there is or was probable cause for belief that particular communications concerning that offense will or would be obtained through the interception; (3) normal investigative procedures have or would have been tried and have or had failed or reasonably appear or appeared to be unlikely to succeed if tried or to be too dangerous; and (4) there is or was probable cause for belief that the facilities from which, or the place where, the wire or oral communications are to be or were intercepted were used, are being used, or are about to be used, in connection with the commission of the offense, or are or were leased to, listed in the name of, or commonly used by the person referred to in paragraph (1). (d) If the facilities from which a wire communication is to be or was intercepted are or were being used by, are or were about to be used by, or are or were leased to, listed in the name of, or commonly used by, a licensed physician, a licensed attorney, or practicing clergyman, or if the place where an oral communication is to be or was intercepted is or was a place used primarily for habitation by a spouses or domestic partners, or primarily by a licensed physician, licensed attorney, or practicing clergyman for his own professional purposes, no order authorizing or approving such interception may be issued unless the court, in addition to the matters provided in subsection (c) of this section, determines that (1) such facilities or place are or were being used or are or were about to be used in connection with conspiratorial activities characteristic of organized crime; and (2) such interceptions will be so conducted as to minimize or eliminate the number of interceptions of privileged wire or oral communications between licensed physicians and patients, licensed attorneys and clients, practicing clergymen and confidants, and spouses or domestic partners. No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this subchapter shall lose its privileged character. (e) Each order authorizing or approving the interception of any wire or oral communication shall specify (1) the identity of the person, if known, or otherwise a particular description of the person, if known, whose communications are to be or were intercepted; (2) the nature and location of the communication facilities as to which, or the place where, authority to intercept or any approval of interception is or was granted; (3) a particular description of the type of communication sought to be or which was intercepted, and a statement of the particular offense to which it relates; (4) the identity of the agency authorized to intercept or whose interception is approved, and of the person authorizing the application; and (5) the period of time during or for which the interception is authorized or approved, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. (f) An order authorizing the interception of a wire or oral communication shall, upon request of the applicant, direct that a communication common carrier, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such carrier, landlord, custodian, or person is according the person whose communications are to be intercepted. Any communication common carrier, landlord, custodian, or other person furnishing such facilities or technical assistance shall be compensated therefore by the applicant at the prevailing rates. (g) No order entered under this section may authorize or approve the interception of any wire or oral communication for any period longer than is necessary to achieve the objective of the authorization,

	nor in any event longer than thirty days. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (a) of this section and the court making the findings required by subsection (c) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize or eliminate the interception of communications not otherwise subject to interception under this subchapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. (h) Whenever an order authorizing interception is entered pursuant to this subchapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Reports shall be made at such intervals as the judge may require. **23-548. Additional procedure for approval of interception of wire or oral communications.** **(a)** Notwithstanding any other provision of this subchapter, any investigative or law enforcement officer, specially designated by the United States attorney for the District of Columbia, who reasonably determines that (1) an emergency situation exists with respect to conspiratorial activities characteristic of organized crime that requires a wire or oral communication to be intercepted before an order authorizing the interception can with due diligence be obtained, and (2) there are grounds upon which an order could be entered under this subchapter to authorize interception, may intercept the wire or oral communication if an application for an order approving the interception is initiated in accordance with this section within twelve hours and is completed within seventy-two hours after the interception has occurred, or begins to occur. In the absence of an order, the interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event the application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this subchapter, and an inventory shall be served as provided for in section 23-550 on the person named in the application. (b) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized by this subchapter, intercepts wire or oral communications relating either to offenses other than those specified in the order of authorization or to offenses other than those offenses for which interception was made pursuant to subsection (a) of this section, he shall make an application to a judge as soon as practicable for approval for disclosure and use, in accordance with section 23-553, of the information intercepted.
Florida	**934.03 Interception and disclosure of wire, oral, or electronic communications prohibited.** — (1) Except as otherwise specifically provided in this chapter, any person who: (a) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication; (b) Intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when: 1. Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or 2. Such device transmits communications by radio or interferes with the transmission of such communication; (c) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; (d) Intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or (e) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication intercepted by means authorized by subparagraph (2)(a)2., paragraph (2)(b), paragraph (2)(c), s. 934.07, or s. 934.09 when that person knows or has reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, has obtained or received the information in connection with a criminal investigation, and intends to improperly obstruct, impede, or interfere with a duly authorized criminal investigation; shall be punished as provided in subsection (4). (2)(a)1. It is lawful under ss. 934.03-934.09 for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication

	service whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his or her employment while engaged in any activity which is a necessary incident to the rendition of his or her service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks. 2. Notwithstanding any other law, a provider of wire, oral, or electronic communication service, or an officer, employee, or agent thereof, or landlord, custodian, or other person, may provide information, facilities, or technical assistance to a person authorized by law to intercept wire, oral, or electronic communications if such provider, or an officer, employee, or agent thereof, or landlord, custodian, or other person, has been provided with: a. A court order directing such assistance signed by the authorizing judge; or b. A certification in writing by a person specified in s. 934.09(7) that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. 3. A provider of wire, oral, or electronic communication service, or an officer, employee, or agent thereof, or landlord, custodian, or other person may not disclose the existence of any interception or the device used to accomplish the interception with respect to which the person has been furnished an order under ss. 934.03-934.09, except as may otherwise be required by legal process and then only after prior notice to the Governor, the Attorney General, the statewide prosecutor, or a state attorney, as may be appropriate. Any such disclosure renders such person liable for the civil damages provided under s. 934.10, and such person may be prosecuted under s. 934.43. An action may not be brought against any provider of wire, oral, or electronic communication service, or an officer, employee, or agent thereof, or landlord, custodian, or other person for providing information, facilities, or assistance in accordance with the terms of a court order under ss. 934.03-934.09. (b) It is lawful under ss. 934.03-934.09 for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his or her employment and in discharge of the monitoring responsibilities exercised by the commission in the enforcement of 47 U.S.C. ch. 5, to intercept a wire, oral, or electronic communication transmitted by radio or to disclose or use the information thereby obtained. (c) It is lawful under ss. 934.03-934.09 for an investigative or law enforcement officer or a person acting under the direction of an investigative or law enforcement officer to intercept a wire, oral, or electronic communication when such person is a party to the communication or one of the parties to the communication has given prior consent to such interception and the purpose of such interception is to obtain evidence of a criminal act. (d) It is lawful under ss. 934.03-934.09 for a person to intercept a wire, oral, or electronic communication when all of the parties to the communication have given prior consent to such interception. (e) It is unlawful to intercept any wire, oral, or electronic communication for the purpose of committing any criminal act. (f) It is lawful under ss. 934.03-934.09 for an employee of a telephone company to intercept a wire communication for the sole purpose of tracing the origin of such communication when the interception is requested by the recipient of the communication and the recipient alleges that the communication is obscene, harassing, or threatening in nature. The individual conducting the interception shall notify local police authorities within 48 hours after the time of the interception. (g) It is lawful under ss. 934.03-934.09 for an employee of: 1. An ambulance service licensed pursuant to s. 401.25, a fire station employing firefighters as defined by s. 633.30, a public utility as defined by ss.[fn1] 365.01 and 366.02, a law enforcement agency as defined by s. 934.02(10), or any other entity with published emergency telephone numbers; 2. An agency operating an emergency telephone number "911" system established pursuant to s. 365.171; or 3. The central abuse hotline operated pursuant to s. 39.201, to intercept and record incoming wire communications; however, such employee may intercept and record incoming wire communications on designated "911" telephone numbers and published nonemergency telephone numbers staffed by trained dispatchers at public safety answering points only. It is also lawful for such employee to intercept and record outgoing wire communications to the numbers from which such incoming wire communications were placed when necessary to obtain information required to provide the emergency services being requested. (h) It shall not be unlawful under ss. 934.03-934.09 for any person: 1. To intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public. 2. To intercept any radio communication which is transmitted: a. By any station for the use of the general public, or that relates

	to ships, aircraft, vehicles, or persons in distress; b. By any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including any police or fire communications system, readily accessible to the general public; c. By a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or d. By any marine or aeronautical communications system. 3. To engage in any conduct which: a. Is prohibited by s. 633 of the Communications Act of 1934; or b. Is excepted from the application of s. 705(a) of the Communications Act of 1934 by s. 705(b) of that act. 4. To intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station of consumer electronic equipment to the extent necessary to identify the source of such interference. 5. To intercept, if such person is another user of the same frequency, any radio communication that is not scrambled or encrypted made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system. 6. To intercept a satellite transmission that is not scrambled or encrypted and that is transmitted: a. To a broadcasting station for purposes of retransmission to the general public; or b. As an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, when such interception is not for the purposes of direct or indirect commercial advantage or private financial gain. 7. To intercept and privately view a private satellite video communication that is not scrambled or encrypted or to intercept a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted, if such interception is not for a tortuous of advantage or private commercial gain. (i) It shall not be unlawful under ss. 934.03-934.09: 2. For a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful, or abusive use of such service. (j) It is not unlawful under ss. 934.03-934.09 for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser which are transmitted to, through, or from a protected computer if: 1. The owner or operator of the protected computer authorizes the interception of the communications of the computer trespasser; 2. The person acting under color of law is lawfully engaged in an investigation; 3. The person acting under color of law has reasonable grounds to believe that the contents of the communications of the computer trespasser will be relevant to the investigation; and 4. The interception does not acquire communications other than those transmitted to, through, or from the computer trespasser. (3)(a) Except as provided in paragraph (b), a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient. (b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication: 1. As otherwise authorized in paragraph (2)(a) or s. 934.08; 2. With the lawful consent of the originator or any addressee or intended recipient of such communication; 3. To a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or 4. Which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency. (4)(a) Except as provided in paragraph (b), whoever violates subsection (1) is guilty of a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, s. 775.084, or s. 934.41. (b) If the offense is a first offense under paragraph (a) and is not for any tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) was committed is a radio communication that is not scrambled, encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication, then: 1. If the communication is not the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication, or a paging service communication, and the conduct is not that described in subparagraph (2)(h)7., the person committing the offense is guilty of a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083. 2. If the communication is the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless

	telephone handset and the base unit, a public land mobile radio service communication, or a paging service communication, the person committing the offense is guilty of a misdemeanor of the second degree, punishable as provided in s. 775.082 or s. 775.083.
Georgia	**16-11-62. It shall be unlawful for:** It shall be unlawful for: (1) Any person in a clandestine manner intentionally to overhear, transmit, or record or attempt to overhear, transmit, or record the private conversation of another which shall originate in any private place; (2) Any person, through the use of any device, without the consent of all persons observed, to observe, photograph, or record the activities of another which occur in any private place and out of public view; provided, however, that it shall not be unlawful: (A) To use any device to observe, photograph, or record the activities of persons incarcerated in any jail, correctional institution, or any other facility in which persons who are charged with or who have been convicted of the commission of a crime are incarcerated, provided that such equipment shall not be used while the prisoner is discussing his or her case with his or her attorney; (B) For an owner or occupier of real property to use for security purposes, crime prevention, or crime detection any device to observe, photograph, or record the activities of persons who are on the property or an approach thereto in areas where there is no reasonable expectation of privacy; or (C) To use for security purposes, crime prevention, or crime detection any device to observe, photograph, or record the activities of persons who are within the curtilage of the residence of the person using such device. A photograph, videotape, or record made in accordance with this subparagraph, or a copy thereof, may be disclosed by such resident to the district attorney or a law enforcement officer and shall be admissible in a judicial proceeding, without the consent of any person observed, photographed, or recorded; (3) Any person to go on or about the premises of another or any private place, except as otherwise provided by law, for the purpose of invading the privacy of others by eavesdropping upon their conversations or secretly observing their activities; (4) Any person intentionally and secretly to intercept by the use of any device, instrument, or apparatus the contents of a message sent by telephone, telegraph, letter, or by any other means of private communication; (5) Any person to divulge to any unauthorized person or authority the content or substance of any private message intercepted lawfully in the manner provided for in Code Section 16-11-65; (6) Any person to sell, give, or distribute, without legal authority, to any person or entity any photograph, videotape, or record, or copies thereof, of the activities of another which occur in any private place and out of public view without the consent of all persons observed; or (7) Any person to commit any other acts of a nature similar to those set out in paragraphs (1) through (6) of this Code section which invade the privacy of another. **Sec. 16-11-135(a)** --Except as provided in this section, no private or public employer, including the state and its political subdivisions, shall establish, maintain, or enforce any policy or rule that has the effect of allowing such employer or its agents to search the locked privately owned vehicles of employees or invited guests on the employer's parking lot and access thereto. (b)Except as provided in this section, no private or public employer, including the state and its political subdivisions, shall condition employment upon any agreement by a prospective employee that prohibits an employee from entering the parking lot and access thereto when the employee's privately owned motor vehicle contains a firearm that is locked out of sight within the trunk, glove box, or other enclosed compartment or area within such privately owned motor vehicle, provided that any applicable employees possess a Georgia firearms license. (c) (1)To searches by certified law enforcement officers pursuant to valid search warrants or valid warrantless searches based upon probable cause under exigent circumstances;(2)To vehicles owned or leased by an employer; (3)To any situation in which a reasonable person would believe that accessing a locked vehicle of an employee is necessary to prevent an immediate threat to human health, life, or safety; or (4)When an employee consents to a search of their locked privately owned vehicle by licensed private security officers for loss prevention purposes based on probable cause that the employee unlawfully possesses employer property. (d) section 16-11-135(a) and (b) (just above) shall not apply--(1) To an employer providing applicable employees with a secure parking area which restricts general public access through the use of a gate, security station, security officers, or other similar means which limit public access into the parking area, provided that any employer policy allowing vehicle searches upon entry shall be applicable to all vehicles entering the property and applied on a uniform and frequent basis; (2) To any penal institution, correctional institution, detention facility, diversion center, jail, or similar place of confinement or confinement alternative; (3) To facilities associated with electric generation owned or

	operated by a public utility; (4) To any United States Department of Defense contractor, if such contractor operates any facility on or contiguous with a United States military base or installation or within one mile of an airport; (5) To an employee who is restricted from carrying or possessing a firearm on the employer's premises due to a completed or pending disciplinary action; (6) Where transport of a firearm on the premises of the employer is prohibited by state or federal law or regulation; (7) To parking lots contiguous to facilities providing natural gas transmission, liquid petroleum transmission, water storage and supply, and law enforcement services determined to be so vital to the State of Georgia, by a written determination of the Georgia Department of Homeland Security, that the incapacity or destruction of such systems and assets would have a debilitating impact on public health or safety; or (8) To any area used for parking on a temporary basis. No employer, property owner, or property owner's agent shall be held liable in any criminal or civil action for damages resulting from or arising out of an occurrence involving the transportation, storage, possession, or use of a firearm, including, but not limited to, the theft of a firearm from an employee's automobile, pursuant to this section unless such employer commits a criminal act involving the use of a firearm or unless the employer knew that the person using such firearm would commit such criminal act on the employer's premises. (e)Nothing contained in this section shall create a new duty on the part of the employer, property owner, or property owner's agent. An employee at will shall have no greater interest in employment created by this section and shall remain an employee at will. (f) In any action relating to the enforcement of any right or obligation under this section, an employer, property owner, or property owner's agent's efforts to comply with other applicable federal, state, or local safety laws, regulations, guidelines, or ordinances shall be a complete defense to any employer, property owner, or property owner's agent's liability. (g) In any action brought against an employer, employer's agent, property owner, or property owner's agent relating to the criminal use of firearms in the workplace, the plaintiff shall be liable for all legal costs of such employer, employer's agent, property owner, or property owner's agent if such action is concluded in such employer, employer's agent, property owner, or property owner's agent's favor. (h)This section shall not be construed so as to require an employer, property owner, or property owner's agent to implement any additional security measures for the protection of employees, customers, or other persons. Implementation of remedial security measures to provide protection to employees, customers, or other persons shall not be admissible in evidence to show prior negligence or breach of duty of an employer, property owner, or property owner's agent in any action against such employer, its officers or shareholders, or property owners. (i) All actions brought based upon a violation of Sec. 16-11-135(a) shall be brought exclusively by the Attorney General. (j) In the event that Sec. 16-11-135(e) is declared or adjudged by any court to be invalid or unconstitutional for any reason, the remaining portions of this section shall be invalid and of no further force or effect. The General Assembly declares that it would not have enacted the remaining provisions of this section if it had known that such portion hereof would be declared or adjudged invalid or unconstitutional. (k)Nothing in this section shall restrict the rights of private property owners or persons in legal control of property through a lease, a rental agreement, a contract, or any other agreement to control access to such property. When a private property owner or person in legal control of property through a lease, a rental agreement, a contract, or any other agreement is also an employer, his or her rights as a private property owner or person in legal control of property shall govern.
Hawaii	**803-42. Interception, access, and disclosure of wire, oral, or electronic communications, use of pen register, trap and trace device, and mobile tracking device prohibited.** (a) Except as otherwise specifically provided in this part, any person who: (1) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (2) Intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any wire, oral, or electronic communication when: (A) Such a device is affixed to, or otherwise transmits a signal through, a wire, cable, or other similar connection used in wire communication; or (B) Such a device transmits communications by radio, or interferes with the transmission of such communication; (3) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this part; (4) Intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a

	wire, oral, or electronic communication in violation of this part; (5)(A) Intentionally accesses without authorization a facility through which an electronic communication service is provided; or (B) Intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage; (6) Intentionally discloses, or attempts to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by subsection (b)(1), (2), or (3), or section 803-44 or 803-46; and (A) Either: (i) Knowing or having reason to know that the information was obtained through the interception of the communication in connection with a criminal investigation; or (ii) Having obtained or received the information in connection with a criminal investigation; and (B) With the intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation[;] (7) Intentionally installs or uses a pen register or a trap and trace device without first obtaining a court order; or (8) Intentionally installs or uses a mobile tracking device without first obtaining a search warrant or other order authorizing the installation and use of such device, unless the device is installed by or with consent of the owner of the property on which the device is installed; shall be guilty of a class C felony. (b)(1) It shall not be unlawful under this part for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication services, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of the officer's, employee's, or agent's employment while engaged in any activity that is either a necessary incident to the rendition of the officer's, employee's, or agent's service or to the protection of the rights or property of the provider of that service; provided that providers of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks. (2) It shall not be unlawful under this part for an officer, employee, or agent of the Federal Communications Commission, in the normal course of the officer's, employee's, or agent's employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of Title 47, chapter 5, of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained. (3)(A) It shall not be unlawful under this part for a person not acting under color of law to intercept a wire, oral, or electronic communication when the person is a party to the communication or when one of the parties to the communication has given prior consent to the interception unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of this State. (B) It shall not be unlawful for a person acting under color of law to install in any private place, without consent of the person or persons entitled to privacy therein, any device for recording, amplifying, or broadcasting sounds or events in that place, or use of any such unauthorized installation, or installation or use outside a private place of such device to intercept sounds originating in that place which would not ordinarily be audible or comprehensible outside. (4) It shall not be unlawful under this part for a person acting under color of law to intercept a wire, oral, or electronic communication, when the person is a party to the communication or one of the parties to the communication has given prior consent to the interception. (5) It shall not be unlawful under this part for any person to intercept a wire, oral, or electronic communication or to disclose or use the contents of an intercepted communication, when such interception is pursuant to a valid court order under this chapter or as otherwise authorized by law; provided that a communications provider with knowledge of an interception of communications accomplished through the use of the communications provider's facilities shall report the fact and duration of the interception to the administrative director of the courts of this State. (6) Notwithstanding any other law to the contrary, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept or access wire, oral, or electronic communications, to conduct electronic surveillance, or to install a pen register or trap and trace device if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with: (A) A court order directing such assistance signed by the designated judge; or B) A certification in writing from the Attorney General of the United States, the Deputy Attorney General of the United States, the Associate Attorney General of the United States, the attorney general of the State of Hawaii, or the prosecuting attorney for each county that no warrant or court order is required by law, that all statutory requirements have been met, and that the specific assistance is required, setting forth the period of time during which the providing of the information, facilities, or technical assistance is

	authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any access, interception, or surveillance or the device used to accomplish the interception or surveillance for which the person has been furnished a court order or certification under this part, except as may otherwise be required by legal process and then only after prior notification to the party that provided the court order or certification. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this part. (7) It shall not be unlawful under this part for any person: (A) To intercept or access an electronic communication made through an electronic communication system configured so that the electronic communication is readily accessible to the general public. (B) To intercept any radio communication that is transmitted: (i) By any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (ii) By any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (iii) By a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (iv) By any marine or aeronautical communications system. (C) To engage in any conduct that: (i) Is prohibited by section 633 of the Communications Act of 1934(47 U.S.C. § 553);or (ii) Is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act (47 U.S.C. § 605). (D) To intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment to the extent necessary to identify the source of the interference; (E) For other users of the same frequency to intercept any radio communication made through a system that uses frequencies monitored by individuals engaged in the providing or the use of the system, if the communication is not scrambled or encrypted. (8) It shall not be unlawful under this part: (A) To use a pen register or a trap and trace device as specified in this part. (B) For a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from the fraudulent, unlawful, or abusive use of such service. (C) For a provider of electronic or wire communication service to use a pen register or a trap and trace device for purposes relating to the operation, maintenance, and testing of the wire or electronic communication service or to the protection of the rights or property of the provider, or to the protection of users of that service from abuse of service or unlawful use of service. (D) To use a pen register or a trap and trace device where consent of the user of the service has been obtained. (9) Good faith reliance upon a court order shall be a complete defense to any criminal prosecution for illegal interception, disclosure, or use. (10) Except as provided in this section, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than a communication to the person or entity or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of the communication or an agent of the addressee or intended recipient. (11) A person or entity providing electronic communication service to the public may divulge the contents of any such communication: (A) As otherwise authorized by a court order or under this part; (B) With the lawful consent of the originator, addressee, or intended recipient of the communication; (C) To a person employed or authorized, or whose facilities are used, to forward the communication to its destination; or (D) That was inadvertently obtained by the service provider and that appears to pertain to the commission of a crime, if divulged to a law enforcement agency.
Idaho	**18-6702. Interception and disclosure of wire, electronic or oral communications prohibited. —** (1) Except as otherwise specifically provided in this chapter, any person shall be guilty of a felony and is punishable by imprisonment in the state prison for a term not to exceed five (5) years or by a fine not to exceed five thousand dollars ($5,000), or by both fine and imprisonment if that person: (a) Willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication; or (b) Willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when: 1. Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or 2. Such device

	transmits communications by radio or interferes with the transmission of such communication; or (c) Willfully discloses, or endeavors to disclose, to any other person the contents of any wire, electronic or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication in violation of this subsection; or (d) Willfully uses, or endeavors to use, the contents of any wire, electronic or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication in violation of this subsection; or (e) Intentionally discloses or endeavors to disclose to any other person the contents of any wire, electronic or oral communication, intercepted by means authorized by subsection (2)(b), (c), (f) or (g) of this section or by section 18-6708, Idaho Code, if that person: (i) Knows or has reason to know that the information was obtained through the interception of such communication in connection with a criminal investigation; and (ii) Has obtained or received the information in connection with a criminal investigation with the intent to improperly obstruct, impede or interfere with a duly authorized criminal investigation. (2)(a) It is lawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service whose facilities are used in the transmission of a wire or electronic communication to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks. (b) It is lawful under this chapter for an officer, employee, or agent of the federal communications commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the commission in the enforcement of 47 U.S.C. ch. 5, to intercept a wire, electronic or oral communication transmitted by radio or to disclose or use the information thereby obtained. (c) It is lawful under this chapter for a law enforcement officer or a person acting under the direction of a law enforcement officer to intercept a wire, electronic or oral communication when such person is a party to the communication or one (1) of the parties to the communication has given prior consent to such interception. (d) It is lawful under this chapter for a person to intercept a wire, electronic or oral communication when one (1) of the parties to the communication has given prior consent to such interception. (e) It is unlawful to intercept any communication for the purpose of committing any criminal act. (f) It is lawful under this chapter for an employee of a telephone company to intercept a wire communication for the sole purpose of tracing the origin of such communication when the interception is requested by an appropriate law enforcement agency or the recipient of the communication and the recipient alleges that the communication is obscene, harassing, or threatening in nature. (g) It is lawful under this chapter for an employee of a law enforcement agency, fire department or ambulance service, while acting in the scope of his employment, and while a party to the communication, to intercept and record incoming wire or electronic communications. (h) It shall not be unlawful under this chapter for any person: (i) To intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public; (ii) To intercept any radio communication that is transmitted: (A) By any station for the use of the general public, or that relates to ships, aircraft, vehicles or persons in distress; (B) By any governmental, law enforcement, civil defense, private land mobile or public safety communications system, including police and fire, readily accessible to the public; (C) By a station operating on an authorized frequency within the bands allocated to the amateur, citizens band or general mobile radio services; or (D) By any marine or aeronautical communication system; (iii) To engage in any conduct that: (A) Is prohibited by 47 U.S.C. § 553 (federal communications act of 1934); or (B) Is excepted from the application of 47 U.S.C. § 605 (federal communications act of 1934); (iv) To intercept any wire or electronic communication, the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment to the extent it is necessary to identify the source of such interference; or (v) For other users of the same frequency to intercept any radio communication, if such communication is not scrambled or encrypted, made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system. (i) It shall be lawful under this chapter for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication or a user of that service from the fraudulent, unlawful or abusive use of

	such service. (3)(a) Except as provided in subsection (3)(b) of this section, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication other than to such person or entity or an agent thereof while in transmission on that service, to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient. (b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication: (i) As otherwise authorized in section 18-6707, Idaho Code, or subsection (2)(a) of this section; (ii) With the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) To a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or (iv) If such contents were inadvertently obtained by the service provider and appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency. **E.O. 2001-12. Executive Order No. 2001-12, Statewide policy on state employee use of the computer, the Internet, & electronic mail; Monitoring—ESTABLISHING STATEWIDE POLICIES ON COMPUTER, THE INTERNET AND ELECTRONIC MAIL USAGE BY STATE EMPLOYEES REPEALING AND REPLACING EXECUTIVE ORDER NO. 98-05 WHEREAS**, computers, the Internet and electronic mail are powerful research, communication, commerce and time-saving tools that are made available to state employees; and WHEREAS, use of this efficient and effective communication tool is critical but, like any tools, computers, the Internet and electronic mail have the potential to be used for inappropriate purposes; and WHEREAS, perceptions are important and state employees must constantly be aware of how their actions are perceived by the public; NOW, THEREFORE, I, DIRK KEMPTHORNE, Governor of the State of Idaho, by the authority vested in me under the Constitution and laws of this state do hereby order as follows: The following statewide policies on computer, the Internet and electronic mail usage shall be observed by all state employees: 1. Users of the Internet and electronic mail are to comply with all appropriate laws, regulations and generally accepted Internet etiquette. 2. Primary purpose of the Internet and electronic mail is to conduct official business. Occasionally, employees may use the Internet and electronic mail for individual, nonpolitical purposes on their personal time, if such use does not violate the terms and conditions of this policy. Use of the Internet and electronic mail offers employees an opportunity to develop research and communication skills valuable to the effectiveness and efficiency of our state government. 3. Users should identify themselves properly when using the Internet and electronic mail, conduct themselves professionally, as representatives of Idaho State Government, and be aware that their activities reflect on the reputation and integrity of all state employees. 4. Each user is individually responsible for the content of any communication sent over or placed on the Internet and electronic mail. 5. All employees have a responsibility to ensure a respectful workplace. State equipment must not be used to visit Internet sites that contain pornographic or sexually explicit information, pictures, or cartoons. 6. Exceptions to this executive order are only allowed when preapproved in writing by appointing authorities and deemed necessary for official state business, research or investigatory work. 7**.** THE FOLLOWING ACTIONS ARE PROHIBITED. IT IS UNACCEPTABLE FOR EMPLOYEES TO: a) Knowingly or intentionally publish, display, transmit, retrieve or store inappropriate or offensive material on any department computer system; b) Create or distribute defamatory, false, inaccurate, abusive, threatening, racially offensive or otherwise biased, discriminatory or illegal material; c) View or distribute obscene, pornographic, profane, or sexually oriented material; d) Violate laws, rules, and regulations prohibiting sexual harassment; e) Encourage the use of controlled substances or for criminal or illegal purposes; f) Engage in any unauthorized activities for personal financial gain; g) Place advertisements for commercial enterprises, including but not limited to, goods, services or property; h) Download, disseminate, store or print materials including articles and software, in violation of copyright laws; i) Violate or infringe on the rights of others; j) Conduct business unauthorized by the department; k) Restrict or inhibit other users from using the system or the efficiency of the computer systems; l) Cause congestion or disruption of networks or systems, including distribution of chain letters; m) Transmit incendiary statements, which might incite violence or describe or promote the use of weapons; n) Conduct political activity; o) Use the system for any illegal purpose. 8. Disregard for the policies or other improper use of the Internet may result in cancellation of a persons access and/or disciplinary action, up to and including dismissal. 9. Internet and electronic mail may be subject to monitoring. 10. The above policies are the minimum standards for usage of computers, the Internet

	and electronic mail. Individual state agencies may implement more restrictive policies as long as those policies are consistent with those developed by the Governor's Information Technology Resource Management Council (ITRMC).
Illinois	5/14-1.Definitions.—(a) Eavesdropping device. An eavesdropping device is any device capable of being used to hear or record oral conversation whether such conversation is conducted in person, by telephone, or by any other means; Provided, however, that this definition shall not include devices used for the restoration of the deaf or hard-of-hearing to normal or partial hearing. (b) Eavesdropper. An eavesdropper is any person, including law enforcement officers, who operates or participates in the operation of any eavesdropping device contrary to the provisions of this Article. (c) Principal. A principal is any person who:(1) Knowingly employs another who illegally uses an eavesdropping device in the course of such employment; or (2) Knowingly derives any benefit or information from the illegal use of an eavesdropping device by another; or (3) Directs another to use an eavesdropping device illegally on his behalf. (d) Conversation. For the purposes of this Article, the term conversation means any oral communication between 2 or more persons regardless of whether one or more of the parties intended their communication to be of a private nature under circumstances justifying that expectation. **5/14-2. Acts considered "Eavesdropping**"—A person commits eavesdropping when he: (a) Uses an eavesdropping device to hear or record all or any part of any conversation unless he does so (1) with the consent of all of the parties to such conversation or (2) in accordance with Article 108A or Article 108B of the "Code of Criminal Procedure of 1963", approved August 14, 1963, as amended; or (b) Uses or divulges, except as authorized by this Article or by Article 108A or 108B of the "Code of Criminal Procedure of 1963", approved August 14, 1963, as amended, any information which he knows or reasonably should know was obtained through the use of an eavesdropping device. (c) It is an affirmative defense to a charge brought under this Article relating to the interception of a privileged communication that the person charged: 1. was a law enforcement officer acting pursuant to an order of interception, entered pursuant to Section 108A-1 or 108B-5 of the Code of Criminal Procedure of 1963; and 2. at the time the communication was intercepted, the officer was unaware that the communication was privileged; and 3. stopped the interception within a reasonable time after discovering that the communication was privileged; and 4. did not disclose the contents of the communication. **5/14-3. Eavesdropping/monitoring activities allowed in the course of certain employments, broadcasts, communications; Telephone marketing research or solicitations; Notice to employees of monitoring**—The following activities shall be exempt from the provisions of this Article: (a) Listening to radio, wireless and television communications of any sort where the same are publicly made; (b) Hearing conversation when heard by employees of any common carrier by wire incidental to the normal course of their employment in the operation, maintenance or repair of the equipment of such common carrier by wire so long as no information obtained thereby is used or divulged by the hearer; (c) Any broadcast by radio, television or otherwise whether it be a broadcast or recorded for the purpose of later broadcasts of any function where the public is in attendance and the conversations are overheard incidental to the main purpose for which such broadcasts are then being made; (d) Recording or listening with the aid of any device to any emergency communication made in the normal course of operations by any federal, state or local law enforcement agency or institutions dealing in emergency services, including, but not limited to, hospitals, clinics, ambulance services, fire fighting agencies, any public utility, emergency repair facility, civilian defense establishment or military installation; (e) Recording the proceedings of any meeting required to be open by the Open Meetings Act, as amended; and (f) Recording or listening with the aid of any device to incoming telephone calls of phone lines publicly listed or advertised as consumer "hotlines" by manufacturers or retailers of food and drug products. Such recordings must be destroyed, erased or turned over to local law enforcement authorities within 24 hours from the time of such recording and shall not be otherwise disseminated. Failure on the part of the individual or business operating any such recording or listening device to comply with the requirements of this subsection shall eliminate any civil or criminal immunity conferred upon that individual or business by the operation of this Section. (g) With prior notification to the State's Attorney of the county in which it is to occur, recording or listening with the aid of any device to any conversation where a law enforcement officer, or any

	person acting at the direction of law enforcement, is a party to the conversation and has consented to it being intercepted or recorded under circumstances where the use of the device is necessary for the protection of the law enforcement officer or any person acting at the direction of law enforcement, in the course of an investigation of a forcible felony, a felony violation of the Illinois Controlled Substances Act, a felony violation of the Cannabis Control Act, or any "streetgang related" or "gang-related" felony as those terms are defined in the Illinois Streetgang Terrorism Omnibus Prevention Act. Any recording or evidence derived as the result of this exemption shall be inadmissible in any proceeding, criminal, civil or administrative, except (i) where a party to the conversation suffers great bodily injury or is killed during such conversation, or (ii) when used as direct impeachment of a witness concerning matters contained in the interception or recording. The Director of the Department of State Police shall issue regulations as are necessary concerning the use of devices, retention of tape recordings, and reports regarding their use. (h) Recordings made simultaneously with a video recording of an oral conversation between a peace officer, who has identified his or her office, and a person stopped for an investigation of an offense under the Illinois Vehicle Code. (i) Recording of a conversation made by or at the request of a person, not a law enforcement officer or agent of a law enforcement officer, who is a party to the conversation, under reasonable suspicion that another party to the conversation is committing, is about to commit, or has committed a criminal offense against the person or a member of his or her immediate household, and there is reason to believe that evidence of the criminal offense may be obtained by the recording. (j) The use of a telephone monitoring device by either (1) a corporation or other business entity engaged in marketing or opinion research or (2) a corporation or other business entity engaged in telephone solicitation, as defined in this subsection, to record or listen to oral telephone solicitation conversations or marketing or opinion research conversations by an employee of the corporation or other business entity when: (i) the monitoring is used for the purpose of service quality control of marketing or opinion research or telephone solicitation, the education or training of employees or contractors engaged in marketing or opinion research or telephone solicitation, or internal research related to marketing or opinion research or telephone solicitation; and (ii) the monitoring is used with the consent of at least one person who is an active party to the marketing or opinion research conversation or telephone solicitation conversation being monitored. No communication or conversation or any part, portion, or aspect of the communication or conversation made, acquired, or obtained, directly or indirectly, under this exemption (j), may be, directly or indirectly, furnished to any law enforcement officer, agency, or official for any purpose or used in any inquiry or investigation, or used, directly or indirectly, in any administrative, judicial, or other proceeding, or divulged to any third party. When recording or listening authorized by this subsection (j) on telephone lines used for marketing or opinion research or telephone solicitation purposes results in recording or listening to a conversation that does not relate to marketing or opinion research or telephone solicitation; the person recording or listening shall, immediately upon determining that the conversation does not relate to marketing or opinion research or telephone solicitation, terminate the recording or listening and destroy any such recording as soon as is practicable. Business entities that use a telephone monitoring or telephone recording system pursuant to this exemption (j) shall provide current and prospective employees with notice that the monitoring or recordings may occur during the course of their employment. The notice shall include prominent signage notification within the workplace. Business entities that use a telephone monitoring or telephone recording system pursuant to this exemption (j) shall provide their employees or agents with access to personal-only telephone lines which may be pay telephones, that are not subject to telephone monitoring or telephone recording. For the purposes of this subsection (j), "telephone solicitation" means a communication through the use of a telephone by live operators: (i) soliciting the sale of goods or services; (ii) receiving orders for the sale of goods or services; (iii) assisting in the use of goods or services; or (iv) engaging in the solicitation, administration, or collection of bank or retail credit accounts. For the purposes of this subsection (j), "marketing or opinion research" means a marketing or opinion research interview conducted by a live telephone interviewer engaged by a corporation or other business entity whose principal business is the design, conduct, and analysis of polls and surveys measuring the opinions, attitudes, and responses of respondents toward products and services, or social or political issues, or both. **5/14-3A. Law enforcement recordings; Interception of private conversations; Recordkeeping—** (a) Any private oral communication intercepted in accordance with subsection (g) of Section 14-3

	shall, if practicable, be recorded by tape or other comparable method. The recording shall, if practicable, be done in such a way as will protect it from editing or other alteration. During an interception, the interception shall be carried out by a law enforcement officer, and the officer shall keep a signed, written record, including: (1) The day and hours of interception or recording; (2) The time and duration of each intercepted communication; (3) The parties, if known, to each intercepted communication; and (4) A summary of the contents of each intercepted communication. (b) Both the written record of the interception or recording and any and all recordings of the interception or recording shall immediately be inventoried and shall be maintained where the chief law enforcement officer of the county in which the interception or recording occurred directs. The written records of the interception or recording conducted under subsection (g) of Section 14-3 shall not be destroyed except upon an order of a court of competent jurisdiction and in any event shall be kept for 10 years. **5/14-3B. Law enforcement recordings; Interception of private conversations; Notice of; Deadlines**—(a) Within a reasonable time, but not later than 60 days after the termination of the investigation for which the interception or recording was conducted, or immediately upon the initiation of criminal proceedings, the person who was the subject of an interception or recording under subsection (g) of Section 14-3 shall be served with an inventory that shall include: (1) Notice to any person who was the subject of the interception or recording; (2) Notice of any interception or recording if the defendant was arrested or indicted or otherwise charged as a result of the interception of his or her private oral communication; (3) The date of the interception or recording; (4) The period of interception or recording; and (5) Notice of whether during the period of interception or recording devices were or were not used to overhear and record various conversations and whether or not the conversations are recorded. (b) A court of competent jurisdiction, upon filing of a motion, may in its discretion make available to those persons or their attorneys for inspection those portions of the intercepted communications as the court determines to be in the interest of justice. **5/14-4. Eavesdropping violations as felonies**—Eavesdropping, for a first offense, is a Class 4 felony, and, for a second or subsequent offense, is a Class 3felony. **5/14-5. Eavesdropping violations; Admissibility of evidence**—Any evidence obtained in violation of this Article is not admissible in any civil or criminal trial, or any administrative or legislative inquiry or proceeding, nor in any grand jury proceedings; provided, however, that so much of the contents of an alleged unlawfully intercepted, overheard or recorded conversation as is clearly relevant, as determined as a matter of law by the court in chambers, to the proof of such allegation may be admitted into evidence in any criminal trial or grand jury proceeding brought against any person charged with violating any provision of this Article. **5/14-6. Eavesdropping violations; Civil remedies**—(1) Any or all parties to any conversation upon which eavesdropping is practiced contrary to this Article shall be entitled to the following remedies: (a) To an injunction by the circuit court prohibiting further eavesdropping by the eavesdropper and by or on behalf of his principal, or either; (b) To all actual damages against the eavesdropper or his principal or both; (c) To any punitive damages which may be awarded by the court or by a jury; (d) To all actual damages against any landlord, owner or building operator, or any common carrier by wire who aids, abets, or knowingly permits the eavesdropping concerned; (e) To any punitive damages which may be awarded by the court or by a jury against any landlord, owner or building operator, or common carrier by wire who aids, abets, or knowingly permits the eavesdropping concerned. (2) No cause of action shall lie in any court against any common carrier by wire or its officers, agents or employees for providing information, assistance or facilities in accordance with the terms of a court order entered under Article 108A of the Code of Criminal Procedure of 1963. **5/14-7. Eavesdropping; Common carriers to assist in detection of eavesdropping at subscriber's request**—Subject to regulation by the Illinois Commerce Commission, any common carrier by wire shall, upon request of any subscriber and upon responsible offer to pay the reasonable cost thereof, furnish whatever services may be within its command for the purpose of detecting any eavesdropping involving its wires which are used by said subscriber. All such requests by subscribers shall be kept confidential unless divulgence is authorized in writing by the requesting subscriber.

	5/14-8. Eavesdropping; Discovery of eavesdropping devices; Notice of illegal device; Fine for violation—Any agent, officer or employee of a private investigative agency or nongovernmental corporation, or of a common carrier by wire, or any individual, who discovers any physical evidence of an eavesdropping device being used which such person does not know to be a legal eavesdropping device shall, within a reasonable time after such discovery disclose the existence of such eavesdropping device to the State's Attorney of the county where such device was found. The State's Attorney shall within a reasonable time notify the person or persons apparently being eavesdropped upon of the existence of that device if the device is illegal. A violation of this Section is a Business Offense for which a fine shall be imposed not to exceed $500. **5/14-9. Eavesdropping; Discovery of eavesdropping device by common carrier; Notice to State's Attorney, subscribers; Fine for violation**—Any agent, officer or employee of any common carrier by wire who discovers any physical evidence of an eavesdropping device which such person does not know to be a legal eavesdropping device shall, within a reasonable time after such discovery, disclose the existence of the eavesdropping device to the State's Attorney of the County where such device was found. The State's Attorney shall within a reasonable time notify the person or persons apparently being eavesdropped upon of the existence of that device if the device is illegal. A violation of this Section is a Business Offense for which a fine shall be imposed not to exceed $500. **5/26-4. Unauthorized video recording; Recording or transmitting a live video of another person without that person's consent in a restroom, tanning bed, tanning salon, locker room, changing room or hotel bedroom prohibited; Exceptions; Violation as a felony offense**—Unauthorized video recording and live video transmission. (a) It is unlawful for any person to knowingly make a video record or transmit live video of another person without that person's consent in a restroom, tanning bed, tanning salon, locker room, changing room, or hotel bedroom . **(a-5)** It is unlawful for any person to knowingly make a video record or transmit live video of another person in that other person's residence without that person's consent. **(a-10)** It is unlawful for any person to knowingly make a video record or transmit live video of another person under or through the clothing worn by that other person for the purpose of viewing the body of or the undergarments worn by that other person without that person's consent. **(a-15)** It is unlawful for any person to place or cause to be placed a device that makes a video record or transmits a live video in a restroom, tanning bed, tanning salon, locker room, changing room, or hotel bedroom with the intent to make a video record or transmit live video of another person without that person's consent. **(a-20)** It is unlawful for any person to place or cause to be placed a device that makes a video record or transmits a live video with the intent to make a video record or transmit live video of another person in that other person's residence without that person's consent. **(a-25)** It is unlawful for any person to, by any means, knowingly disseminate, or permit to be disseminated, a video record or live video that he or she knows to have been made or transmitted in violation of (a), (a-5), (a-10), (a-15), or (a-20). (b) Exemptions. The following activities shall be exempt from the provisions of this Section: (1) The making of a video record or transmission of live video by law enforcement officers pursuant to a criminal investigation, which is otherwise lawful; (2) The making of a video record or transmission of live video by correctional officials for security reasons or for investigation of alleged misconduct involving a person committed to the Department of Corrections. (3) The making of a video record or transmission of live video in a locker room by a reporter or news medium, as those terms are defined in Section 8-902 of the Code of Civil Procedure, where the reporter or news medium has been granted access to the locker room by an appropriate authority for the purpose of conducting interviews. (c) The provisions of this Section do not apply to any sound recording or transmission of an oral conversation made as the result of the making of a video record or transmission of live video, and to which Article 14 of this Code applies. (d) Sentence. (1) A violation of subsection (a-10), (a-15), or (a-20) is a Class A misdemeanor. (2) A violation of subsection (a) or (a-5) is a Class 4 felony. (3) A violation of subsection (a-25) is a Class 3 felony. (4) A violation of subsection (a), (a-5), (a-10), (a-15) or (a-20) is a Class 3 felony if the victim is a person under 18 years of age or if the violation is committed by an individual who is required to register as a sex offender under the Sex Offender Registration Act. (5) A violation of subsection (a-25) is a Class 2 felony if the victim is a person under 18 years of age or if the violation is committed by an individual who is required to register as a sex offender under the Sex

	Offender Registration Act. (e) For purposes of this Section, "video record" means and includes any videotape, photograph, film, or other electronic or digital recording of a still or moving visual image; and "live video" means and includes any real-time or contemporaneous electronic or digital transmission of a still or moving visual image.
Indiana	**35-33.5-1-1 This article does not apply to the ordinary course of....** This article does not apply to the ordinary course of business pertaining to the operation of a business entity that provides or facilitates electronic communications in accordance with the business entity's tariffs.
Iowa	**727.8 Electronic and mechanical eavesdropping.** Any person, having no right or authority to do so, who taps into or connects a listening or recording device to any telephone or other communication wire, or who by any electronic or mechanical means listens to, records, or otherwise intercepts a conversation or communication of any kind, commits a serious misdemeanor; provided, that the sender or recipient of a message or one who is openly present and participating in or listening to a communication shall not be prohibited hereby from recording such message or communication; and further provided, that nothing herein shall restrict the use of any radio or television receiver to receive any communication transmitted by radio or wireless signal.
Kansas	**21-4001. Eavesdropping.** (a) Eavesdropping is knowingly and without lawful authority: (1) Entering into a private place with intent to listen surreptitiously to private conversations or to observe the personal conduct of any other person or persons therein; (2) installing or using outside a private place any device for hearing, recording, amplifying or broadcasting sounds originating in such place, which sounds would not ordinarily be audible or comprehensible outside, without the consent of the person or persons entitled to privacy therein; (3) installing or using any device or equipment for the interception of any telephone, telegraph or other wire communication without the consent of the person in possession or control of the facilities for such wire communication; or (4) installing or using a concealed camcorder, motion picture camera or photographic camera of any type, to secretly videotape, film, photograph or record by electronic means, another, identifiable person under or through the clothing being worn by that other person or another, identifiable person who is nude or in a state of undress, for the purpose of viewing the body of, or the undergarments worn by, that other person, without the consent or knowledge of that other person, with the intent to invade the privacy of that other person, under circumstances in which the other person has a reasonable expectation of privacy. (b) A "private place" within the meaning of this section is a place where one may reasonably expect to be safe from uninvited intrusion or surveillance, but does not include a place to which the public has lawful access. (c) It shall not be unlawful for an operator of a switchboard, or any officer, employee, or agent of any public utility providing telephone communications service, whose facilities are used in the transmission of a communication, to intercept, disclose or use that communication in the normal course of employment while engaged in any activity which is incident to the rendition of public utility service or to the protection of the rights of property of such public utility. (d) Eavesdropping is a class A nonperson misdemeanor. **21-4002. Breach of privacy.** (a) Breach of privacy is knowingly and without lawful authority: (1) Intercepting, without the consent of the sender or receiver, a message by telephone, telegraph, letter or other means of private communication; or (2) Divulging, without the consent of the sender or receiver, the existence or contents of such message if such person knows that the message was illegally intercepted, or if such person illegally learned of the message in the course of employment with an agency in transmitting it. (b) Subsection (a)(1) shall not apply to messages overheard through a regularly installed instrument on a telephone party line or on an extension. (c) Breach of privacy is a class A nonperson misdemeanor. **22-2514. Authorized interception of wire, oral or electronic communications; definitions.** This act shall be a part of and supplemental to the code of criminal procedure. As used in this act: (1) "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection between the point of origin and the point of reception, including the use of such connection in a switching station, furnished or operated by any person engaged in providing or operating such facilities for the transmission of intrastate, interstate or foreign communications. Wire communication shall include any electronic storage of such communication; (2) "oral communication" means any oral communication uttered by a

	person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication; (3) "intercept" means the aural or other acquisition of the contents of any wire, oral or electronic communication through the use of any electronic, mechanical or other device; (4) "persons" means any individual, partnership, association, joint stock company, trust or corporation, including any official, employee or agent of the United States or any state or any political subdivision thereof; (5) "investigative or law enforcement officer" means any law enforcement officer who is empowered by the law of this state to conduct investigations of or to make arrests for offenses enumerated in this act, including any attorney authorized by law to prosecute or participate in the prosecution of such offenses and agents of the United States federal bureau of investigation, drug enforcement administration, marshals service, secret service, treasury department, customs service, justice department and internal revenue service; (6) "contents" when used with respect to any wire, oral or electronic communication, includes any information concerning the substance, purport or meaning of such communication; (7) "aggrieved person" means a person who was a party to any intercepted wire, oral or electronic communication or a person against whom the interception was directed; (8) "judge of competent jurisdiction" means a justice of the supreme court, a judge of the court of appeals or any district judge but does not include a district magistrate judge; (9) "electronic, mechanical or other device" means any device or apparatus which can be used to intercept a wire, oral or electronic communication other than: (a) Any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of the officer's duties; or (b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal; (10) "communication common carrier" means common carrier, as defined by section 153(h) of title 47 of the United States Code; (11) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system but does not include: (a) Any wire or oral communication; (b) any communication made through a tone-only paging device; or (c) any communication from a tracking device, as defined in section 3117, chapter 205 of title 18, United States Code; (12) "user" means any person or entity who: (a) Uses an electronic communication service; and (b) is duly authorized by the provider of such service to engage in such use; (13) "electronic communications system" means any wire, radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; (14) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications; (15) "readily accessible to the general public" means, with respect to a radio communication, that such communication 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 such 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; or (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; (16) "electronic storage" means: (a) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and (17) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.
Kentucky	**526.010. Definition.** The following definition applies in this chapter, unless the context otherwise requires: "Eavesdrop" means to overhear, record, amplify or transmit any part of a wire or oral

	communication of others without the consent of at least one party thereto by means of any electronic, mechanical or other device. **526.020 Eavesdropping.** (1) A person is guilty of eavesdropping when he intentionally uses any device to eavesdrop, whether or not he is present at the time. (2) Eavesdropping is a Class D felony. **526.030 Installing eavesdropping device.** (1) A person is guilty of installing an eavesdropping device when he intentionally installs or places such a device in any place with the knowledge that it is to be used for eavesdropping. (2) Installing an eavesdropping device is a Class D felony. **526.040 Possession of eavesdropping device.** (1) A person is guilty of possession of an eavesdropping device when he possesses any electronic, mechanical or other device designed or commonly used for eavesdropping with intent to use that device to eavesdrop or knowing that another intends to use that device to eavesdrop. (2) Possession of an eavesdropping device is a Class A misdemeanor. **526.050 Tampering with private communications.** (1) A person is guilty of tampering with private communications when knowing that he does not have the consent of the sender or receiver, he unlawfully: (a) Opens or reads a sealed letter or other sealed private communication; or (b) Obtains in any manner from an employee, officer or representative of a communications common carrier information with respect to the contents or nature of a communication. (2) The provisions of this section do not apply to the censoring of sealed letters or sealed communications for security purposes in official detention or penal facilities. (3) Tampering with private communications is a Class A misdemeanor. **526.060 Divulging illegally obtained information.** (1) A person is guilty of divulging illegally obtained information when he knowingly uses or divulges information obtained through eavesdropping or tampering with private communications or learned in the course of employment with a communications common carrier engaged in transmitting the message. (2) Divulging illegally obtained information is a Class A misdemeanor. **526.070 Eavesdropping -- Exceptions.** A person is not guilty under this chapter when he: (1) Inadvertently overhears the communication through a regularly installed telephone party line or on a telephone extension but does not divulge it; or (2) Is an employee of a communications common carrier who, while acting in the course of his employment, intercepts, discloses or uses a communication transmitted through the facilities of his employer for a purpose which is a necessary incident to the rendition of the service or to the protection of the rights or the property of the carrier of such communication, provided however that communications common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.
Louisiana	**15:1303. Interception and disclosure of wire, electronic, or oral communications** A. Except as otherwise specifically provided in this Chapter, it shall be unlawful for any person to: (1) Willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire or oral communication; (2) Willfully use, endeavor to use, or procure any other person to use or endeavor to use, any electronic, mechanical, or other device to intercept any oral communication when: (a) Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or (b) Such device transmits communications by radio or interferes with the transmission of such communication; (3) Willfully disclose, or endeavor to disclose, to any other person the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this Subsection; or (4) Willfully use, or endeavor to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this Subsection. B. Any person who violates the provisions of this Section shall be fined not more than ten thousand dollars and imprisoned for not less than two years nor more than ten years at hard labor. C. (1) It shall not be unlawful under this Chapter for an operator of a switchboard, or any officer, employee, or agent of any communications common carrier, whose facilities are used in the transmission of a wire

	communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication; however, such communications common carriers shall not utilize service observing or random monitoring, except for mechanical or service quality control checks. (2) It shall not be unlawful under this Chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the commission in the enforcement of Chapter 5 of Title 47 of the United States Code, to intercept a wire communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained. (3) It shall not be unlawful under this Chapter for a person acting under color of law to intercept a wire or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception. Such a person acting under color of law is authorized to possess equipment used under such circumstances. (4) It shall not be unlawful under this Chapter for a person not acting under color of law to intercept a wire or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception, unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the United States or of the state or for the purpose of committing any other injurious act. (5) It shall not be unlawful under this Chapter: (a) For the ultimate receiver of wire or electronic communication, or an investigative or law enforcement officer to use a pen register or trap and trace device as provided in Part III of this Chapter. (b) For a provider of electronic communication services to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, or another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful, or abusive use of such service. (c) To use a device which captures the incoming electronic or other impulses which identify the numbers of an instrument from which a wire communication was transmitted. (6) A person or entity providing electronic communication services to the public shall not intentionally divulge the contents of any communication while in transmission of that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient except: (a) As otherwise authorized by federal or state law. (b) To a person employed or authorized, or whose facilities are used, to forward such communication to its destination. (c) Any electronic communication inadvertently obtained by the service provider and which appears to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency. (7) It shall not be unlawful under this Chapter for an officer or investigator of a law enforcement agency to intercept, conduct, use, or disclose electronic, wire, or oral communications obtained during a hostage situation or situation involving a barricaded individual. For the purposes of this Section, "hostage situation" means any situation which involves the unlawful abduction or restraint of one or more individuals with intent to restrict their freedom. For the purposes of this Section, "barricaded individual" means any situation that involves the use of a residence, or other structure, belonging to another to seek refuge from law enforcement after attempting or committing a crime or threatening suicide. D. (1) Any investigative or law enforcement officer who, by any means authorized by this Chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose the contents to another investigative or law enforcement officer to the extent that the disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure. (2) Any investigative or law enforcement officer who, by any means authorized by this Chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use the contents to the extent the use is appropriate to the proper performance of his official duties. (3) Any person who has received, by any means authorized by this Chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this Chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any state or political subdivision thereof. (4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this Chapter shall lose its privileged character. E. Upon receipt of the information or evidence sought by the interception,

	the interception shall cease. **15:1313. Pen registers and trap and trace devices, use prohibited** A. Except as provided in this Section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under R.S. 15:1315 of this Part. B. The prohibition of this Section does not apply with respect to the use of a pen register or a trap and trace device by a provider of a wire or electronic communication service: (1) Relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service. (2) To record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful, or abusive use of service, or with the consent of the user of that service. C. Whoever intentionally violates Subsection A of this Section shall be fined not more than five thousand dollars, or imprisoned not more than one year, or both. **14:322. Wire-tapping prohibited; penalty** No person shall tap or attach any devices for the purpose of listening in on wires, cables, or property owned and used by any person, for the transmission of intelligence by magnetic telephone or telegraph, without the consent of the owner. Whoever violates this Section shall be fined not less than ten dollars nor more than three hundred dollars, or imprisoned for not more than three months. This Section shall not be construed to prevent officers of the law, while in the actual discharge of their duties, from tapping in on wires or cables for the purpose of obtaining information to detect crime.
Maine	**15 M.R.S.A. § 710. Offenses 1. Interception, oral communications prohibited**. Any person, other than an employee of a common carrier as defined in this chapter, a law enforcement officer or an investigative officer as defined in this chapter, carrying out practices otherwise permitted by this chapter, who intentionally or knowingly intercepts, attempts to intercept or procures any other person to intercept or attempt to intercept, any wire or oral communication is guilty of a Class C crime. **2. Editing of tape recordings in judicial proceedings prohibited**. Any person who knowingly or intentionally edits, alters or tampers with any tape, transcription or other sound recording, or knows of such editing, altering or tampering, and presents that recording in any judicial proceeding or proceeding under oath, without fully indicating the nature of the changes made and the original state of the recording, is guilty of a Class C crime. **3. Disclosure, or use of wire or oral communications prohibited**. A person is guilty of a Class C crime if he: A. Intentionally or knowingly discloses or attempts to disclose to any person the contents of any wire or oral communication, knowing that the information was obtained through interception; or B. Intentionally or knowingly uses or attempts to use the contents of any wire or oral communication, knowing that the information was obtained through interception. **4. Duty to report**. Any communications common carrier shall promptly report to the Attorney General any facts coming to its attention in the conduct of its business which may indicate a possible violation of this section and such carrier shall adopt reasonable rules to assure compliance with this subsection, provided such carrier shall not be liable to any person who may claim an injury arising out of any such report, if made in good faith. Any person violating this subsection shall be subject to a civil penalty not to exceed $5,000, payable to the State, to be recovered in a civil action. **5. Possession of interception devices prohibited**. A person, other than an employee of a common carrier as defined in this chapter, a law enforcement officer or an investigative officer as defined in this chapter, carrying out practices otherwise permitted by this chapter, who has in his possession any device, contrivance, machine or apparatus designed or commonly used for intercepting wire or oral communications defined in this chapter, is guilty of a Class C crime. **6. Sale of interception devices prohibited**. A person who sells, exchanges, delivers, barters, gives or furnishes or possesses with an intent to sell any device, contrivance, machine or apparatus designed or commonly used for the interception of wire or oral communications as defined in this chapter is guilty of a Class B crime. This subsection shall not include devices manufactured under written contract for sale to common carriers, law enforcement agencies and the Department of Corrections, provided that the production of any such device shall not have commenced prior to the signing of the contract by both parties. **17-A M.R.S.A. § 511. Violation of privacy 1.** A person is guilty of violation of privacy if, except in the execution of a public duty or as authorized by law, that person intentionally: **A.** Commits a civil

	trespass on property with the intent to overhear or observe any person in a private place; **B.** Installs or uses in a private place without the consent of the person or persons entitled to privacy in that place, any device for observing, photographing, recording, amplifying or broadcasting sounds or events in that place; **C.** Installs or uses outside a private place without the consent of the person or persons entitled to privacy therein, any device for hearing, recording, amplifying or broadcasting sounds originating in that place that would not ordinarily be audible or comprehensible outside that place; or **D.** Engages in visual surveillance in a public place by means of mechanical or electronic equipment with the intent to observe or photograph, or record, amplify or broadcast an image of any portion of the body of another person present in that place when that portion of the body is in fact concealed from public view under clothing and a reasonable person would expect it to be safe from surveillance. **1-A.** It is a defense to a prosecution under subsection 1, paragraph D that the person subject to surveillance had in fact attained 14 years of age and had consented to the visual surveillance. **2.** As used in this section, "private place" means a place where one may reasonably expect to be safe from surveillance, including, but not limited to, changing or dressing rooms, bathrooms and similar places. **3.** Violation of privacy is a Class D crime.
Maryland	**10-402 CTS. & JUD. PROC.** Intercepting, disclosing communications. (a) *Unlawful acts.* — Except as otherwise specifically provided in this subtitle it is unlawful for any person to: (1) Willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (2) Willfully disclose, or endeavor to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subtitle; or (3) Willfully use, or endeavor to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subtitle. (b) *Penalty.* — Any person who violates subsection (a) of this section is guilty of a felony and is subject to imprisonment for not more than 5 years or a fine of not more than $10,000, or both. (c) *Lawful acts.* — (1) (i) It is lawful under this subtitle for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communications service to the public may not utilize service observing or random monitoring except for mechanical or service quality control checks. (ii) 1. It is lawful under this subtitle for a provider of wire or electronic communication service, its officers, employees, and agents, landlords, custodians or other persons to provide information, facilities, or technical assistance to persons authorized by federal or State law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, if the provider, its officers, employees, or agents, landlord, custodian, or other specified person has been provided with a court order signed by the authorizing judge directing the provision of information, facilities, or technical assistance. 2. The order shall set forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specify the information, facilities, or technical assistance required. A provider of wire or electronic communication service, its officers, employees, or agents, or landlord, custodian, or other specified person may not disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished an order under this subparagraph, except as may otherwise be required by legal process and then only after prior notification to the judge who granted the order, if appropriate, or the State's Attorney of the county where the device was used. Any such disclosure shall render the person liable for compensatory damages. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order under this subtitle. (2) (i) This paragraph applies to an interception in which: 1. The investigative or law enforcement officer or other person is a party to the communication; or 2. One of the parties to the communication has given prior consent to the interception. (ii) It is lawful under this subtitle for an investigative or law enforcement officer acting in a criminal investigation or any other person acting at the prior direction and under the supervision of an investigative or law enforcement

	officer to intercept a wire, oral, or electronic communication in order to provide evidence: 1. Of the commission of: A. Murder; B. Kidnapping; C. Rape; D. A sexual offense in the first or second degree; E. Child abuse in the first or second degree; F. Child pornography under § 11-207, § 11-208, or § 11-208.1 of the Criminal Law Article; G. Gambling; H. Robbery under § 3-402 or § 3-403 of the Criminal Law Article; I. A felony under Title 6, Subtitle 1 of the Criminal Law Article; J. Bribery; K. Extortion; L. Dealing in a controlled dangerous substance, including a violation of § 5-617 or § 5-619 of the Criminal Law Article; M. A fraudulent insurance act, as defined in Title 27, Subtitle 4 of the Insurance Article; N. An offense relating to destructive devices under § 4-503 of the Criminal Law Article; O. Sexual solicitation of a minor under § 3-324 of the Criminal Law Article; P. An offense relating to obstructing justice under § 9-302, § 9-303, or § 9-305 of the Criminal Law Article; Q. Sexual abuse of a minor under § 3-602 of the Criminal Law Article; or R. A conspiracy or solicitation to commit an offense listed in items A through Q of this item; or 2. If: A. A person has created a barricade situation; and B. Probable cause exists for the investigative or law enforcement officer to believe a hostage or hostages may be involved. (3) It is lawful under this subtitle for a person to intercept a wire, oral, or electronic communication where the person is a party to the communication and where all of the parties to the communication have given prior consent to the interception unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of this State. (4) (i) It is lawful under this subtitle for a law enforcement officer in the course of the officer's regular duty to intercept an oral communication if: 1. The law enforcement officer initially lawfully detained a vehicle during a criminal investigation or for a traffic violation; 2. The law enforcement officer is a party to the oral communication; 3. The law enforcement officer has been identified as a law enforcement officer to the other parties to the oral communication prior to any interception; 4. The law enforcement officer informs all other parties to the communication of the interception at the beginning of the communication; and 5. The oral interception is being made as part of a video tape recording. (ii) If all of the requirements of subparagraph (i) of this paragraph are met, an interception is lawful even if a person becomes a party to the communication following: 1. The identification required under subparagraph (i)3 of this paragraph; or 2. The informing of the parties required under subparagraph (i)4 of this paragraph. (5) It is lawful under this subtitle for an officer, employee, or agent of a governmental emergency communications center to intercept a wire, oral, or electronic communication where the officer, agent, or employee is a party to a conversation concerning an emergency. (6) (i) It is lawful under this subtitle for law enforcement personnel to utilize body wires to intercept oral communications in the course of a criminal investigation if there is reasonable cause to believe that a law enforcement officer's safety may be in jeopardy. (ii) Communications intercepted under this paragraph may not be recorded, and may not be used against the defendant in a criminal proceeding. (7) It is lawful under this subtitle for a person: (i) To intercept or access an electronic communication made through an electronic communication system that is configured so that the electronic communication is readily accessible to the general public; (ii) To intercept any radio communication that is transmitted: 1. By any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; 2. By any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; 3. By a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or 4. By any marine or aeronautical communications system; (iii) To intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of the interference; or (iv) For other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of the system, if the communication is not scrambled or encrypted. (8) It is lawful under this subtitle: (i) To use a pen register or trap and trace device as defined under § 10-4B-01 of this title; or (ii) For a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful, or abusive use of the service. (9) It is lawful under this subtitle for a person to intercept a wire or electronic communication in the course of a law enforcement investigation of possible telephone solicitation theft if: (i) The person is an investigative or law enforcement officer or

	is acting under the direction of an investigative or law enforcement officer; and (ii) The person is a party to the communication and participates in the communication through the use of a telephone instrument. (10) It is lawful under this subtitle for a person to intercept a wire, oral, or electronic communication in the course of a law enforcement investigation in order to provide evidence of the commission of vehicle theft if: (i) The person is an investigative or law enforcement officer or is acting under the direction of an investigative or law enforcement officer; and (ii) The device through which the interception is made has been placed within a vehicle by or at the direction of law enforcement personnel under circumstances in which it is thought that vehicle theft may occur. (d) *Divulging contents of communications.* — (1) Except as provided in paragraph (2) of this subsection, a person or entity providing an electronic communication service to the public may not intentionally divulge the contents of any communication (other than one to the person or entity providing the service, or an agent of the person or entity) while in transmission on that service to any person or entity other than an addressee or intended recipient of the communication or an agent of the addressee or intended recipient. (2) A person or entity providing electronic communication service to the public may divulge the contents of a communication: (i) As otherwise authorized by federal or State law; (ii) To a person employed or authorized, or whose facilities are used, to forward the communication to its destination; or (iii) That were inadvertently obtained by the service provider and that appear to pertain to the commission of a crime, if the divulgence is made to a law enforcement agency. (e) *Violations of subsection (d).* — (1) Except as provided in paragraph (2) of this subsection or in subsection (f) of this section, a person who violates subsection (d) of this section is subject to a fine of not more than $10,000 or imprisonment for not more than 5 years, or both. (2) If an offense is a first offense under paragraph (1) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense occurred is a radio communication that is not scrambled or encrypted, and: (i) The communication is not the radio portion of a cellular telephone communication, a public land mobile radio service communication, or a paging service communication, the offender is subject to a fine of not more than $1,000 or imprisonment for not more than 1 year, or both; or (ii) The communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication, or a paging service communication, the offender is subject to a fine of not more than $500. (3) Unless the conduct is for the purpose of direct or indirect commercial advantage or private financial gain, conduct which would otherwise be an offense under this subsection is not an offense under this subsection if the conduct consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted: (i) To a broadcasting station for purposes of retransmission to the general public; or (ii) As an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls. (f) *Violations of subtitle.* — (1) A person who engages in conduct in violation of this subtitle is subject to suit by the federal government or by the State in a court of competent jurisdiction, if the communication is: (i) A private satellite video communication that is not scrambled or encrypted and the conduct in violation of this subtitle is the private viewing of that communication, and is not for a tortious or illegal purpose, or for purposes of direct or indirect commercial advantage, or private commercial gain; or (ii) A radio communication that is transmitted on frequencies allocated under Subpart D of Part 74 of the Rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this subtitle is not for a tortious or illegal purpose or for purpose of direct or indirect commercial advantage or private commercial gain. (2) (i) The State is entitled to appropriate injunctive relief in an action under this subsection if the violation is the person's first offense under subsection (e)(1) of this section and the person has not been found liable in a prior civil action under § 10-410 of this subtitle. (ii) In an action under this subsection, if the violation is a second or subsequent offense under subsection (e)(1) of this section or if the person has been found liable in a prior civil action under § 10-410 of this subtitle, the person is subject to a mandatory civil fine of not less than $500. (3) The court may use any means within its authority to enforce an injunction issued under paragraph (2)(i) of this subsection, and shall impose a civil fine of not less than $500 for each violation of an injunction issued under paragraph (2)(i) of this subsection. **10-4B-02 CTS. & JUD. PROC.** Court order required to install or use pen register or trap and trace device; exceptions. (a) *Court order required.* — Except as provided in subsection (b) of this section, a person may not install or use a pen register or a trap and trace device without first obtaining a court

	order under § 10-4B-04 of this subtitle. (b) *Exceptions.* — Subsection (a) of this section does not apply to the use of a pen register or a trap and trace device by a provider of wire or electronic communication service: (1) Relating to the operation, maintenance, and testing of a wire or electronic service or to the protection of the rights or property of the provider, or to the protection of users of that service from abuse of service or unlawful use of service; or (2) To record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful, or abusive use of service, or with the consent of the user of that service. (c) *Penalty*. — A person who violates subsection (a) of this section, upon conviction, is subject to a fine not exceeding $5,000 or imprisonment not exceeding 1 year, or both.
Massachusetts	**272, § 99. Interception of wire and oral communications. Interception of wire and oral communications**. —A. Preamble. The general court finds that organized crime exists within the commonwealth and that the increasing activities of organized crime constitute a grave danger to the public welfare and safety. Organized crime, as A exists in the commonwealth today, consists of a continuing conspiracy among highly organized and disciplined groups to engage in supplying illegal goods and services. In supplying these goods and services organized crime commits unlawful acts and employs brutal and violent tactics. Organized crime is infiltrating legitimate business activities and depriving honest businessmen of the right to make a living. The general court further finds that because organized crime carries on its activities through layers of insulation and behind a wall of secrecy, government has been unsuccessful in curtailing and eliminating it. Normal investigative procedures are not effective in the investigation of illegal acts committed by organized crime. Therefore, law enforcement officials must be permitted to use modern methods of electronic surveillance, under strict judicial supervision, when investigating these organized criminal activities. The general court further finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited. The use of such devices by law enforcement officials must be conducted under strict judicial supervision and should be limited to the investigation of organized crime. B. Definitions. As used in this section —1. The term "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception. 2. The term "oral communication" means speech, except such speech as is transmitted over the public air waves by radio or other similar device. 3. The term "intercepting device" means any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication other than a hearing aid or similar device which is being used to correct subnormal hearing to normal and other than any telephone or telegraph instrument, equipment, facility, or a component thereof (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business; or (b) being used by a communications common carrier in the ordinary course of its business. 4. The term "interception" means to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication; provided that it shall not constitute an interception for an investigative or law enforcement officer, as defined in this section, to record or transmit a wire or oral communication if the officer is a party to such communication or has been given prior authorization to record or transmit the communication by such a party and if recorded or transmitted in the course of an investigation of a designated offense as defined herein. 5. The term "contents", when used with respect to any wire or oral communication, means any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication. 6. The term "aggrieved person" means any individual who was a party to an intercepted wire or oral communication or who was named in the warrant authorizing the interception, or who would otherwise have standing to complain that his personal or property interest or privacy was invaded in the course of an interception. 7. The term "designated offense" shall include the following offenses in connection with organized crime as defined in the preamble: arson, assault and battery with a dangerous weapon, extortion, bribery, burglary, embezzlement, forgery, gaming in violation of section seventeen of chapter two hundred and seventy-one of the general laws, intimidation of a witness or juror, kidnapping, larceny, lending of money or

	things of value in violation of the general laws, mayhem, murder, any offense involving the possession or sale of a narcotic or harmful drug, perjury, prostitution, robbery, subornation of perjury, any violation of this section, being an accessory to any of the foregoing offenses and conspiracy or attempt or solicitation to commit any of the foregoing offenses. 8. The term "investigative or law enforcement officer" means any officer of the United States, a state or a political subdivision of a state, who is empowered by law to conduct investigations of, or to make arrests for, the designated offenses, and any attorney authorized by law to participate in the prosecution of such offenses. 9. The term "Judge of competent jurisdiction" means any justice of the superior court of the commonwealth. 10. The term "chief justice" means the chief justice of the superior court of the commonwealth. 11. The term "issuing judge" means any justice of the superior court who shall issue a warrant as provided herein or in the event of his disability or unavailability any other judge of competent jurisdiction designated by the chief justice. 12. The term "communication common carrier" means any person engaged as a common carrier in providing or operating wire communication facilities. 13. The term "person" means any individual, partnership, association, joint stock company, trust, or corporation, whether or not any of the foregoing is an officer, agent or employee of the United States, a state, or a political subdivision of a state. 14. The terms "sworn" or "under oath" as they appear in this section shall mean an oath or affirmation or a statement subscribed to under the pains and penalties of perjury. 15. The terms "applicant attorney general" or "applicant district attorney" shall mean the attorney general of the commonwealth or a district attorney of the Commonwealth who has made application for a warrant pursuant to this section. 16. The term "exigent circumstances" shall mean the showing of special facts to the issuing judge as to the nature of the investigation for which a warrant is sought pursuant to this section which require secrecy in order to obtain the information desired from the interception sought to be authorized. 17. The term "financial institution" shall mean a bank, as defined in section 1 of chapter 167, and an investment bank, securities broker, securities dealer, investment adviser, mutual fund, investment company or securities custodian as defined in section 1.165-12(c)(1) of the United States Treasury regulations. 18. The term "corporate and institutional trading partners" shall mean financial institutions and general business entities and corporations which engage in the business of cash and asset management, asset management directed to custody operations, securities trading, and wholesale capital markets including foreign exchange, securities lending, and the purchase, sale or exchange of securities, options, futures, swaps, derivatives, repurchase agreements and other similar financial instruments with such financial institution. C. Offenses. 1. Interception, oral communications prohibited. Except as otherwise specifically provided in this section any person who: willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two and one half years, or both so fined and given one such imprisonment. Proof of the installation of any intercepting device by any person under circumstances evincing an intent to commit an interception, which is not authorized or permitted by this section, shall be prima facie evidence of a violation of this subparagraph. 2. Editing of tape recordings in judicial proceeding prohibited. Except as otherwise specifically provided in this section any person who willfully edits, alters or tampers with any tape, transcription or recording of oral or wire communications by any means, or attempts to edit alter or tamper with any tape, transcription or recording of oral or wire communications by any means with the intent to present in any judicial proceeding or proceeding under oath, or who presents such recording or permits such recording to be presented in any judicial proceeding or proceeding under oath, without fully indicating the nature of the changes made in the original state of the recording, shall be fined not more than ten thousand dollars or imprisoned in the state prison for not more than five years or imprisoned in a jail or house of correction for not more than two years or both so fined and given one such imprisonment. 3. Disclosure or use of wire or oral communications prohibited. Except as otherwise specifically provided in this section any person who: a. willfully discloses or attempts to disclose to any person the contents of any wire or oral communication, knowing that the information was obtained through interception; or b. willfully uses or attempts to use the contents of any wire or oral communication, knowing that the information was obtained through interception, shall be guilty of a misdemeanor punishable by imprisonment in a jail or a house of correction for not more than two years or by a fine of not more than five thousand dollars or both. 4. Disclosure of contents of applications, warrants, renewals, and returns prohibited. Except as otherwise specifically

	provided in this section any person who: willfully discloses to any person, any information concerning or contained in the application for, the granting or denial of orders for interception, renewals, notice or return on an ex parte order granted pursuant to this section, or the contents of any document, tape, or recording kept in accordance with paragraph N, shall be guilty of a misdemeanor punishable by imprisonment in a jail or a house of correction for not more than two years or by a fine of not more than five thousand dollars or both. 5. Possession of interception devices prohibited. A person who possesses any intercepting device under circumstances evincing an intent to commit an interception not permitted or authorized by this section, or a person who permits an intercepting device to be used or employed for an interception not permitted or authorized by this section, or a person who possesses an intercepting device knowing that the same is intended to be used to commit an interception not permitted or authorized by this section, shall be guilty of a misdemeanor punishable by imprisonment in a jail or house of correction for not more than two years or by a fine of not more than five thousand dollars or both. The installation of any such intercepting device by such person or with his permission or at his direction shall be prima facie evidence of possession as required by this subparagraph. 6. Any person who permits or on behalf of any other person commits or attempts to commit, or any person who participates in a conspiracy to commit or to attempt to commit, or any accessory to a person who commits a violation of subparagraphs 1 through 5 of paragraph C of this section shall be punished in the same manner as is provided for the respective offenses as described in subparagraphs 1 through 5 of paragraph C. D. Exemptions. 1. Permitted interception of wire or oral communications. It shall not be a violation of this section — a. for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the carrier of such communication, or which is necessary to prevent the use of such facilities in violation of section fourteen A of chapter two hundred and sixty-nine of the general laws; provided, that said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks. b. for persons to possess an office intercommunication system which is used in the ordinary course of their business or to use such office intercommunication system in the ordinary course of their business. c. for investigative and law enforcement officers of the United States of America to violate the provisions of this section if acting pursuant to authority of the laws of the United States and within the scope of their authority. d. for any person duly authorized to make specified interceptions by a warrant issued pursuant to this section. e. for investigative or law enforcement officers to violate the provisions of this section for the purposes of ensuring the safety of any law enforcement officer or agent thereof who is acting in an undercover capacity, or as a witness for the commonwealth; provided, however, that any such interception which is not otherwise permitted by this section shall be deemed unlawful for purposes of paragraph P. f. for a financial institution to record telephone communications with its corporate or institutional trading partners in the ordinary course of its business; provided, however, that such financial institution shall establish and maintain a procedure to provide semi-annual written notice to its corporate and institutional trading partners that telephone communications over designated lines will be recorded. 2. Permitted disclosure and use of intercepted wire or oral communications. a. Any investigative or law enforcement officer, who, by any means authorized by this section, has obtained knowledge of the contents of any wire or oral communication, or evidence derived there from, may disclose such contents or evidence in the proper performance of his official duties. b. Any investigative or law enforcement officer, who, by any means authorized by this section has obtained knowledge of the contents of any wire or oral communication, or evidence derived there from, may use such contents or evidence In the proper performance of his official duties. c. Any person who has obtained, by any means authorized by this section, knowledge of the contents of any wire or oral communication, or evidence derived there from, may disclose such contents while giving testimony under oath or affirmation in any criminal proceeding in any court of the United States or of any state or in any federal or state grand jury proceeding. d. The contents of any wire or oral communication intercepted pursuant to a warrant in accordance with the provisions of this section, or evidence derived there from, may otherwise be disclosed only upon a showing of good cause before a judge of competent jurisdiction. e. No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this section shall lose its privileged character. E. Warrants: when issuable: A warrant may issue only: 1. Upon a sworn application in

	conformity with this section; and 2. Upon a showing by the applicant that there is probable cause to believe that a designated offense has been, is being, or is about to be committed and that evidence of the commission of such an offense may thus be obtained or that information which will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit a designated offense may thus be obtained; and 3. Upon a showing by the applicant that normal investigative procedures have been tried and have failed or reasonably appear unlikely to succeed if tried. F. Warrants: application. 1. Application. The attorney general, any assistant attorney general specially designated by the attorney general, any district attorney, or any assistant district attorney specially designated by the district attorney may apply ex parte to a judge of competent jurisdiction for a warrant to intercept wire or oral communications. Each application ex parte for a warrant must be in writing, subscribed and sworn to by the applicant authorized by this subparagraph. 2. The application must contain the following: a. A statement of facts establishing probable cause to believe that a particularly described designated offense has been, is being, or is about to be committed;. And b. A statement of facts establishing probable cause to believe that oral or wire communications of a particularly described person will constitute evidence of such designated offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit a designated offense; and c. That the oral or wire communications of the particularly described person or persons will occur in a particularly described place and premises or over particularly described telephone or telegraph lines; and d. A particular description of the nature of the oral or wire communications sought to be overheard; and e. A statement that the oral or wire communications sought are material to a particularly described investigation or prosecution and that such conversations are not legally privileged; and f. A statement of the period of time for which the interception is required to be maintained. If practicable, the application should designate hours of the day or night during which the oral or wire communications may be reasonably expected to occur. If the nature of the investigation is such that the authorization for the interception should not automatically terminate when the described oral or wire communications have been first obtained, the application must specifically state facts establishing probable cause to believe that additional oral or wire communications of the same nature will occur thereafter; and g. If it is reasonably necessary to make a secret entry upon a private place and premises in order to install an intercepting device to effectuate the interception, a statement to such effect; and h. If a prior application has been submitted or a warrant previously obtained for interception of oral or wire communications, a statement fully disclosing the date, court, applicant, execution, results, and present status thereof and i. If there is good cause for requiring the postponement of service pursuant to paragraph L, subparagraph 2, a description of such circumstances, including reasons for the applicant's belief that secrecy is essential to obtaining the evidence or information sought. 3. Allegations of fact in the application may be based either upon the personal knowledge of the applicant or upon information and belief. If the applicant personally knows the facts alleged, it must be so stated. If the facts establishing such probable cause are derived in whole or part from the statements of persons other than the applicant, the sources of such information and belief must be either disclosed or described; and the application must contain facts establishing the existence and reliability of any informant and the reliability of the information supplied by him. The application must also state, so far as possible, the basis of the informant's knowledge or belief if the applicant's information and belief is derived from tangible evidence or recorded oral evidence, a copy or detailed description thereof should be annexed to or included in the application. Affidavits of persons other than the applicant may be submitted in conjunction with the application if they tend to support any fact or conclusion alleged therein. Such accompanying affidavits may be based either on personal knowledge of the affiant or information and belief with the source thereof and reason therefore, specified. G. Warrants: application to whom made. Application for a warrant authorized by this section must be made to a judge of competent jurisdiction in the county where the interception is to occur, or the county where the office of the applicant is located, or in the event that there is no judge of competent jurisdiction sitting in said county at such time, to a judge of competent jurisdiction sitting in Suffolk County; except that for these purposes, the office of the attorney general shall be deemed to be located in Suffolk County. H. Warrants: application how determined. 1. If the application conforms to paragraph F, the issuing judge may examine under oath any person for the purpose of determining whether probable cause exists for the issuance of the warrant pursuant to paragraph E. A verbatim transcript of every such interrogation or examination must be taken, and a

	transcription of the same, sworn to by the stenographer, shall be attached to the application and be deemed a part thereof. 2. If satisfied that probable, cause exists for the issuance of a warrant the judge may grant the application and issue a warrant in accordance with paragraph I. The application and an attested copy of the warrant shall be retained by the issuing judge and transported to the chief justice of the superior court in accordance with the provisions of paragraph N of this section. 3. If the application does not conform to paragraph F, or if the judge is not satisfied that probable cause has been shown sufficient for the issuance of a warrant, the application must be denied. I. Warrants: form and content. A warrant must contain the following: 1. The subscription and title of the issuing judge; and 2. The date of issuance, the date of effect, and termination date which in no event shall exceed thirty days from the date of effect. The warrant shall permit interception of oral or wire communications for a period not to exceed fifteen days. If physical installation of a device is necessary, the thirty-day period shall begin upon the date of installation. If the effective period of the warrant is to terminate upon the acquisition of particular evidence or information or oral or wire communication, the warrant shall so provide; and 3. A particular description of the person and the place, premises or telephone or telegraph line upon which the interception may be conducted; and 4. A particular description of the nature of the oral or wire communications to be obtained by the interception including a statement of the designated offense to which they relate; and 5. An express authorization to make secret entry upon a private place or premises to install a specified intercepting device, if such entry is necessary to execute the warrant; and 6. A statement providing for service of the warrant pursuant to paragraph L except that if there has been a finding of good cause shown requiring the postponement of such service, a statement of such finding together with the basis therefore must be included and an alternative direction for deferred service pursuant to paragraph L, subparagraph 2. J. Warrants: renewals. 1. Any time prior to the expiration of a warrant or a renewal thereof the applicant may apply to the issuing judge for a renewal thereof with respect to the same person, place, premises or telephone or telegraph line. An application for renewal must incorporate the warrant sought to be renewed together with the application therefore and any accompanying papers upon which it was issued. The application for renewal must set forth the results of the interceptions thus far conducted. In addition, it must set forth present grounds for extension in conformity with paragraph F, and the judge may interrogate under oath and in such an event a transcript must be provided and attached to the renewal application in the same manner as is set forth in subparagraph 1 of paragraph H. 2. Upon such application, the judge may issue an order renewing the warrant and extending the authorization for a period not exceeding fifteen (15) days from the entry thereof. Such an order shall specify the grounds for the issuance thereof. The application and an attested copy of the order shall be retained by the issuing judge to be transported to the chief justice in accordance with the provisions of subparagraph N of this section. In no event shall a renewal be granted which shall terminate later than two years following the effective date of the warrant. K. Warrants: manner and time of execution. 1. A warrant may be executed pursuant to its terms anywhere in the commonwealth. 2. Such warrant may be executed by the authorized applicant personally or by any investigative or law enforcement officer of the commonwealth designated by him for the purpose. 3. The warrant may be executed according to its terms during the hours specified therein, and for the period therein authorized, or a part thereof. The authorization shall terminate upon the acquisition of the oral or wire communications, evidence or information described in the warrant. Upon termination of the authorization in the warrant and any renewals thereof the interception must cease at once, and any device installed for the purpose of the interception must be removed as soon thereafter as practicable. Entry upon private premises for the removal of such device is deemed to be authorized by the warrant. L. Warrants: service thereof. 1. Prior to the execution of a warrant authorized by this section or any renewal thereof, an attested copy of the warrant or the renewal must, except as otherwise provided in subparagraph 2 of this paragraph, be served upon a person whose oral or wire communications are to be obtained, and if an intercepting device is to be installed, upon the owner, lessee, or occupant of the place or premises, or upon the subscriber to the telephone or owner or lessee of the telegraph line described in the warrant. 2. If the application specially alleges exigent circumstances requiring the postponement of service and the issuing judge finds that such circumstances exist the warrant may provide that an attested copy thereof may be served within thirty days after the expiration of the warrant or, in case of any renewals thereof, within thirty days after the expiration of the last renewal; except that upon a showing of important special facts which set forth the need for continued secrecy to the satisfaction of the issuing judge, said judge may direct that the attested copy of the warrant be

	served on such parties as are required by this section at such time as may be appropriate in the circumstances but in no event may he order it to be served later than three (3) years from the time of expiration of the warrant or the last renewal thereof. In the event that the service required herein is postponed in accordance with this paragraph, in addition to the requirements of any other paragraph of this section, service of an attested copy of the warrant shall be made upon any aggrieved person who should reasonably be known to the person who executed or obtained the warrant as a result of the information obtained from the interception authorized thereby. 3. The attested copy of the warrant shall be served on persons required by this section by an investigative or law enforcement officer of the commonwealth by leaving the same at his usual place of abode, or in hand, or if this is not possible by mailing the same by certified or registered mail to his last known place of abode. A return of service shall be made to the issuing judge, except, that if such service is postponed as provided in subparagraph 2 of paragraph L, it shall be made to the chief justice. The return of service shall be deemed a part of the return of the warrant and attached thereto. M. Warrant: return. Within seven days .after termination of the warrant or the last renewal thereof, a return must be made thereon to the judge issuing the warrant by the applicant therefore, containing the following: a. a statement of the nature and location of the communications facilities, if any, and premise or place where the interceptions were made; and b. the periods of time during which such interceptions were made; and c. the names of the parties to the communications intercepted if known; and d. the original recording of the oral or wire communications intercepted, if any; and e. a statement attested under the pains and penalties of perjury by each person who heard oral or wire communications as a result of the interception authorized by the warrant, which were not recorded, stating everything that was overheard to the best of his recollection at the time of the execution of the statement. N. Custody and secrecy of papers and recordings made pursuant to a warrant. 1. The contents of any wire or oral communication intercepted pursuant to a warrant issued pursuant to this section shall, if possible, be recorded on tape or wire or other similar device. Duplicate recordings may be made for use pursuant to subparagraphs 2 (a) and (b) of paragraph D for investigations. Upon examination of the return and a determination that it complies with this section, the issuing judge shall forthwith order that the application, all renewal applications, warrant, all renewal orders and the return thereto be transmitted to the chief justice by such persons as he shall designate. Their contents shall not be disclosed except as provided in this section. The application, renewal applications, warrant, the renewal order and the return or any one of them or any part of them may be transferred to any trial court, grand jury proceeding of any jurisdiction by any law enforcement or investigative officer or court officer designated by the chief justice and a trial justice may allow them to be disclosed in accordance with paragraph D, subparagraph 2, or paragraph O or any other applicable provision of this section. The application, all renewal applications, warrant, all renewal orders and the return shall be stored in a secure place which shall be designated by the chief justice, to which access shall be denied to all persons except the chief justice or such court officers or administrative personnel of the court as he shall designate. 2. Any violation of the terms and conditions of any order of the chief justice, pursuant to the authority granted in this paragraph, shall be punished as a criminal contempt of court in addition to any other punishment authorized by law. 3. The application, warrant, renewal and return shall be kept for a period of five (5) years from the date of the issuance of the warrant or the last renewal thereof at which time they shall be destroyed by a person designated by the chief justice. Notice prior to the destruction shall be given to the applicant attorney general or his successor or the applicant district attorney or his successor and upon a showing of good cause to the chief justice, the application, warrant, renewal, and return may be kept for such additional period as the chief justice shall determine but in no event longer than the longest period of limitation for any designated offense specified in the warrant, after which time they must be destroyed by a person designated by the chief justice. O. Introduction of evidence.1. Notwithstanding any other provisions of this section or any order issued pursuant thereto, in any criminal trial where the commonwealth intends to offer in evidence any portions of the contents of any interception or any evidence derived therefrom the defendant shall be served with a complete copy of each document and item which make up each application, renewal application, warrant, renewal order, and return pursuant to which the information was obtained, except that he shall be furnished a copy of any recording instead of the original. The service must be made at the arraignment of the defendant or, if a period in excess of thirty (30) days shall elapse prior to the commencement of the trial of the defendant, the service may be made at least thirty (30) days before the commencement of the criminal trial. Service shall be made in hand upon the defendant or his

	attorney by any investigative or law enforcement officer of the commonwealth. Return of the service required by this subparagraph including the date of service shall be entered into the record of trial of the defendant by the commonwealth and such return shall be deemed prima facie evidence of the service described therein. Failure by the commonwealth to make such service at the arraignment, or if delayed, at least thirty days before the commencement of the criminal trial, shall render such evidence illegally obtained for purposes of the trial against the defendant; and such evidence shall not be offered nor received at the trial notwithstanding the provisions of any other law or rules of court. 2. In any criminal trial where the commonwealth intends to offer in evidence any portions of a recording or transmission or any evidence derived there from, made pursuant to the exceptions set forth in paragraph B, subparagraph 4, of this section, the defendant shall be served with a complete copy of each recording or a statement under oath of the evidence overheard as a result of the transmission. The service must be made at the arraignment of the defendant or if a period in excess of thirty days shall elapse prior to the commencement of the trial of the defendant, the service may be made at least thirty days before the commencement of the criminal trial. Service shall be made in hand upon the defendant or his attorney by any investigative or law enforcement officer of the commonwealth. Return of the service required by this subparagraph including the date of service shall be entered into the record of trial of the defendant by the commonwealth and such return shall be deemed prima facie evidence of the service described therein. Failure by the commonwealth to make such service at the arraignment, or if delayed at least thirty days before the commencement of the criminal trial, shall render such service illegally obtained for purposes of the trial against the defendant and such evidence shall not be offered nor received at the trial notwithstanding the provisions of any other law or rules of court. P. Suppression of evidence. Any person who is a defendant in a criminal trial in a court of the commonwealth may move to suppress the contents of any intercepted wire or oral communication or evidence derived there from, for the following reasons: 1. That the communication was unlawfully intercepted. 2. That the communication was not intercepted in accordance with the terms of this section. 3. That the application or renewal application fails to set forth facts sufficient to establish probable cause for the issuance of a warrant. 4. That the interception was not made in conformity with the warrant. 5. That the evidence sought to be introduced was illegally obtained. 6. That the warrant does not conform to the provisions of this section. Q. Civil remedy. Any aggrieved person whose oral or wire communications were intercepted, disclosed or used except as permitted or authorized by this section or whose personal or property interests or privacy were violated by means of an interception except as permitted or authorized by this section shall have a civil cause of action against any person who so intercepts, discloses or uses such communications or who so violates his personal, property or privacy interest, and shall be entitled to recover from any such person — 1. actual damages but not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1000, whichever is higher; 2. punitive damages; and 3. a reasonable attorney's fee and other litigation disbursements reasonably incurred. Good faith reliance on a warrant issued under this section shall constitute a complete defense to an action brought under this paragraph. R. Annual report of interceptions of the general court. On the second Friday of January, each year, the attorney general and each district attorney shall submit a report to the general court stating (1) the number of applications made for warrants during the previous year, (2) the name of the applicant, (3) the number of warrants issued, (4) the effective period for the warrants, (5) the number and designation of the offenses for which those applications were sought, and for each of the designated offenses the following: (a) the number of renewals, (b) the number of interceptions made during the previous year, (e) the number of indictments believed to be obtained as a result of those interceptions, (d) the number of criminal convictions obtained in trials where interception evidence or evidence derived therefrom was introduced. This report shall be a public document and be made available to the public at the offices of the attorney general and district attorneys. In the event of failure to comply with the provisions of this paragraph any person may compel compliance by means of an action of mandamus.
Michigan	**750.539c Eavesdropping upon private conversation.** Sec. 539c. Any person who is present or who is not present during a private conversation and who wilfully uses any device to eavesdrop upon the conversation without the consent of all parties thereto, or who knowingly aids, employs or procures another person to do the same in violation of this section, is guilty of a felony punishable by imprisonment in a state prison for not more than 2 years or by a fine of not more than $2,000.00, or both.

	750.539e Use or divulgence of information unlawfully obtained. Sec. 539e. Any person who uses or divulges any information which he knows or reasonably should know was obtained in violation of sections 539b, 539c or 539d is guilty of a felony, punishable by imprisonment in a state prison not more than 2 years, or by a fine of not more than $2,000.00.
Minnesota	**626A.02 INTERCEPTION AND DISCLOSURE OF WIRE OR ORAL COMMUNICATIONS PROHIBITED. Subdivision** 1.Offenses.Except as otherwise specifically provided in this chapter any person who:(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication;(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or(ii) such device transmits communications by radio, or interferes with the transmission of such communication;(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this subdivision; or(d) intentionally uses, or endeavors to use, the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this subdivision; shall be punished as provided in subdivision 4, or shall be subject to suit as provided in subdivision 5.**Subd. 2.Exemptions.(a) It is not unlawful under this chapter for an operator of a switchboard, or an officer,** employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.(b) It is not unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of employment and in discharge of the monitoring responsibilities exercised by the commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.(c) It is not unlawful under this chapter for a person acting under color of law to intercept a wire, electronic, or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.(d) It is not unlawful under this chapter for a person not acting under color of law to intercept a wire, electronic, or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the United States or of any state.(e) It is not a violation of this chapter for a person:(1) to intercept or access an electronic communication made through an electronic communication system that is configured so that the electronic communication is readily accessible to the general public;(2) to intercept any radio communication that is transmitted:(i) by a station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;(ii) by a governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;(iii) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or(iv) by a marine or aeronautical communications system;(3) to engage in any conduct which:(i) is prohibited by section 553 of title 47 of the United States Code; or(ii) is excepted from the application of section 605(a) of title 47 of the United States Code by section 605(b) of that title;(4) to intercept a wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or(5) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if the communication is not scrambled or encrypted.(f) It is not unlawful under this chapter:(1) to use a pen register or a trap and trace device as those terms are defined by section

	626A.39; or (2) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful, or abusive use of the service.(g) It is not unlawful under this chapter for a person not acting under color of law to intercept the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit if the initial interception of the communication was obtained inadvertently. **Subd. 3.Disclosing communications.(**a) Except as provided in paragraph (b), a person or entity providing an electronic communications service to the public must not intentionally divulge the contents of any communication other than one to the person or entity, or an agent of the person or entity, while in transmission on that service to a person or entity other than an addressee or intended recipient of the communication or an agent of the addressee or intended recipient.(b) A person or entity providing electronic communication service to the public may divulge the contents of a communication:(1) as otherwise authorized in subdivision 2, paragraph (a), and section 626A.09; (2) with the lawful consent of the originator or any addressee or intended recipient of the communication;(3) to a person employed or authorized, or whose facilities are used, to forward the communication to its destination; or(4) that were inadvertently obtained by the service provider in the normal course of business if there is reason to believe that the communication pertains to the commission of a crime, if divulgence is made to a law enforcement agency. **Subd. 4.Penalties.(**a) Except as provided in paragraph (b) or in subdivision 5, whoever violates subdivision 1 shall be fined not more than $20,000 or imprisoned not more than five years, or both.(b) If the offense is a first offense under paragraph (a) and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled or encrypted, then:(1) if the communication is not the radio portion of a cellular telephone communication, a public land mobile radio service communication, a cordless telephone communication transmitted between the cordless telephone handset and the base unit, or a paging service communication, and the conduct is not that described in subdivision 5, the offender shall be fined not more than $3,000 or imprisoned not more than one year, or both; and(2) if the communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication, a cordless telephone communication transmitted between the cordless telephone handset and the base unit, or a paging service communication, the offender shall be fined not more than $500.(c) Conduct otherwise an offense under this subdivision that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted:(1) to a broadcasting station for purposes of retransmission to the general public; or(2) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,is not an offense under this subdivision unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain. Subd. 5.Civil action.(a)(1) If the communication is:(i) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or(ii) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of title 47 of the Code of Federal Regulations and that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct is subject to suit by the county or city attorney in whose jurisdiction the violation occurs.(2) In an action under this subdivision:(i) if the violation of this chapter is a first offense for the person under subdivision 4, paragraph (a), and the person has not been found liable in a civil action under section 626A.13, the city or county attorney is entitled to seek appropriate injunctive relief; and (ii) if the violation of this chapter is a second or subsequent offense under subdivision 4, paragraph (a), or the person has been found liable in a prior civil action under section 626A.13, the person is subject to a mandatory $500 civil fine. (b) The court may use any means within its authority to enforce an injunction issued under paragraph (a), clause (2)(i), and shall impose a civil fine of not less than $500 for each violation of such an injunction. **626A.03 MANUFACTURE, DISTRIBUTION, POSSESSION, AND ADVERTISING OF WIRE**

	OR ORALCOMMUNICATION INTERCEPTING DEVICESPROHIBITED. Subdivision 1.Acts; penalties. Except as otherwise specifically provided in this chapter, any person who intentionally:(a) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, electronic, or oral communications;(b) places in any newspaper, magazine, handbill, or other publication any advertisement of:(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, electronic, or oral communications; or(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purposes of the surreptitious interception of wire, electronic, or oral communications, shall be fined not more than $20,000 or imprisoned not more than five years, or both. **Subd. 2.Offenses.** It is not unlawful under this section for:(a) a provider of wire or electronic communications service or an officer, agent or employee of, or a person under contract with, a provider, in the normal course of the business of providing that wire or electronic communications service; or(b) an officer, agent, or employee of, or a person under contract with, the United States, a state, or a political subdivision thereof, in the normal course of the activities of the United States, a state, or a political subdivision thereof, to manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, electronic, or oral communication. **626A.04 PROHIBITION OF USE AS EVIDENCE OF INTERCEPTED WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS.** Whenever any wire, oral, or electronic communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court or grand jury if the disclosure of that information would be in violation of this chapter. **626A.05 AUTHORIZATION FOR INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS.Subdivision 1.Application for warrant.** The attorney general or a county attorney of any county may make application as provided in section 626A.06, to a judge of the district court, of the Court of Appeals, or of the Supreme Court for a warrant authorizing or approving the interception of wire, electronic, or oral communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made. No court commissioner shall issue a warrant under this chapter. Subd. 2.Offenses for which interception of wire or oral communication may be authorized. A warrant authorizing interception of wire, electronic, or oral communications by investigative or law enforcement officers may only be issued when the interception may provide evidence of the commission of, or of an attempt or conspiracy to commit, any of the following offenses:(1) a felony offense involving murder, manslaughter, assault in the first, second, and third degrees, aggravated robbery, kidnapping, criminal sexual conduct in the first, second, and third degrees, prostitution, bribery, perjury, escape from custody, theft, receiving stolen property, embezzlement, burglary in the first, second, and third degrees, forgery, aggravated forgery, check forgery, or financial transaction card fraud, as punishable under sections 609.185, 609.19, 609.195, 609.20, 609.221, 609.222, 609.223, 609.2231, 609.245, 609.25, 609.321 to 609.324, 609.342, 609.343, 609.344, 609.42, 609.48, 609.485, subdivision 4, paragraph (a), clause (1), 609.52, 609.53, 609.54, 609.582, 609.625, 609.63, 609.631, 609.821, and 609.825; (2) an offense relating to gambling or controlled substances, as punishable under section 609.76 or chapter 152; or (3) an offense relating to restraint of trade defined in section 325D.53, subdivision 1 or 2, as punishable under section 325D.56, subdivision 2. **626A.06 PROCEDURE FOR INTERCEPTION OF WIRE OR ORAL COMMUNICATIONS. Subdivision 1.Applications.**Each application for a warrant authorizing or approving the interception of a wire, electronic, or oral communication shall be made in writing upon oath or affirmation to a judge of the district court, of the Court of Appeals, or of the Supreme Court and shall state the applicant's authority to make such application. Each application shall include the following information:(1) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;(2) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify the applicant's belief that an order should be issued, including

	(i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subdivision 11, a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;(3) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;(4) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;(5) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, electronic, or oral communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application;(6) where statements in the application are solely upon the information or belief of the applicant, the grounds for the belief must be given; and(7) the names of persons submitting affidavits in support of the application. **Subd. 2.Additional showing of probable cause.** The court to whom any such application is made, before issuing any warrant thereon, may examine on oath the person seeking the warrant and any witnesses the person may produce, and must take the person's affidavit or other affidavits in writing, and cause them to be subscribed by the party or parties making the same. The court may also require the applicant to furnish additional documentary evidence or additional oral testimony to satisfy itself of the existence of probable cause for issuance of the warrant. **Subd. 3.Finding of probable cause by judge.** Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, electronic, or oral communications within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant that:(1) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 626A.05, subdivision 2; (2) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;(3) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;(4) except as provided in subdivision 11, there is probable cause for belief that the facilities from which, or the place where, the wire, electronic, or oral communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person. Nothing in this chapter is to be considered as modifying in any way the existence or scope of those privileged communications defined in chapter 595. In acting upon an application for a warrant for intercepting communications, the potential contents of any such future communications that are within the provisions of chapter 595 shall not be considered by the court in making its finding as to the probability that material evidence will be obtained by such interception of communications. **Subd. 4.Warrant.** Each warrant to intercept communications shall be directed to a law enforcement officer, commanding the officer to hold the recording of all intercepted communications conducted under said warrant in custody subject to the further order of the court issuing the warrant. The warrant shall contain the grounds for its issuance with findings, as to the existence of the matters contained in subdivision 1 and shall also specify: (1) the identity of the person, if known, whose communications are to be intercepted and recorded; (2) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted, and in the case of telephone or telegraph communications the general designation of the particular line or lines involved; (3) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (4) the identity of the law enforcement office or agency authorized to intercept the communications, the name of the officer or officers thereof authorized to intercept communications, and of the person authorizing the application; (5) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained; (6) any other limitations on the interception of communications being authorized, for the protection of the rights of

	third persons; (7) a statement that using, divulging, or disclosing any information concerning such application and warrant for intercepting communications is prohibited and that any violation is punishable by the penalties of this chapter; (8) a statement that the warrant shall be executed as soon as practicable, shall be executed in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter and must terminate upon attainment of the authorized objective, or in any event in 30 days. The 30-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is received. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An order authorizing the interception of a wire, oral, or electronic communication under this chapter must, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish the applicant immediately all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that the service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. A provider of wire or electronic communication service, landlord, custodian, or other person furnishing facilities or technical assistance must be compensated by the applicant for reasonable expenses incurred in providing the facilities or assistance. Denial of an application for a warrant to intercept communications or of an application for renewal of such warrant shall be by written order that shall include a statement as to the offense or offenses designated in the application, the identity of the official applying for the warrant and the name of the law enforcement office or agency**. Subd. 4a.Personnel used.** An interception under this chapter may be conducted in whole or in part by an employee of the state or any subdivision of the state who is an investigative or law enforcement officer authorized to conduct the investigation. **Subd. 5.Duration of warrant.** No warrant entered under this section may authorize or approve the interception of any wire, electronic, or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days. The effective period of any warrant for intercepting communications shall terminate immediately when any person named in the warrant has been charged with an offense specified in the warrant. **Subd. 6.Extensions.** Any judge of the district court, of the Court of Appeals, or of the Supreme Court may grant extensions of a warrant, but only upon application for an extension made in accordance with subdivision 1 and the court making the findings required by subdivision 3. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than 30 days. In addition to satisfying the requirements of subdivision 1, an application for an extension of any warrant for intercepting communications shall also: (1) contain a statement that all interception of communications under prior warrants has been in compliance with this chapter; (2) contain a statement setting forth the results thus far obtained from the interception or a reasonable explanation of the failure to obtain results; (3) state the continued existence of the matters contained in subdivision 1; and (4) specify the facts and circumstances of the interception of communications under prior warrants which are relied upon by the applicant to show that such continued interception of communications is necessary and in the public interest**. Subd. 7.Delivery and retention of copies.** Any warrant for intercepting communications under this section, or any order renewing a prior warrant, together with the application made therefor and any supporting papers upon which the application was based, shall be delivered to and retained by the applicant as authority for the interception of communications authorized therein. A true copy of such warrant and the application made therefor shall be retained in the possession of the judge issuing the same, and, in the event of the denial of an application for such a warrant, a true copy of the papers upon which the application was based shall in like manner be retained by the judge denying the same. **Subd. 8.Periodic reports to issuing judge.** Whenever a warrant authorizing interception is entered pursuant to this section, the warrant may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require. **Subd. 9.Secrecy of warrant proceedings.** A warrant for intercepting communications and the application, affidavits, and return prepared inconnection therewith, and also any information concerning the application for, the granting of, or the denial of a warrant for intercepting communications shall remain secret and subject to all the penalties of this chapter for unauthorized disclosure to persons not

	lawfully engaged in preparing and executing such a warrant, unless and until the same shall have been disclosed in a criminal trial or proceeding or shall have been furnished to a defendant pursuant to this chapter. **Subd. 10.Persons executing warrant.** A warrant for the interception of communications may in all cases be served by any of the officers mentioned in its direction, but by no other person except if the officer requires aid while present and acting in its execution. **Subd. 11.Requirements inapplicable.** The requirements of subdivision 1, clause (2), item (ii), and subdivision 3, clause (4), relating to the specification of the facilities from which, or the place where, the communication is to be interpreted do not apply if: (1) in the case of an application with respect to the interception of an oral communication: (i) the application contains a full and complete statement as to why the specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and (ii) the judge finds that the specification is not practical; (2) in the case of an application with respect to a wire or electronic communication: (i) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and (ii) the judge finds that the purpose has been adequately shown. **Subd. 12.Motion to quash order.** An interception of a communication under an order with respect to which the requirements of subdivision 1, clause (2), item (ii), and subdivision 3, clause (4), do not apply by reason of subdivision 11 must not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subdivision 11, clause (2), may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the attorney applying for the warrant, shall decide a motion expeditiously. **626A.065 EMERGENCY INTERCEPTION.** Notwithstanding any other provision in this chapter, any investigative or law enforcement officer, specially designated by the attorney general or a county attorney, who:(1) reasonably determines that:(i) an emergency situation exists that involves immediate danger of death or serious physical injury to any person that requires a wire, oral, or electronic communication to be intercepted before a warrant authorizing such interception can, with due diligence, be obtained; and(ii) there are grounds upon which a warrant could be issued under this chapter to authorize the interception; and(2) obtains approval from a judge of the district court, of the Court of Appeals, or of the Supreme Court, may intercept the wire, oral, or electronic communication. The judge's approval may be given orally and may be given in person or by using any medium of communication. The judge shall do one of the following: make written notes summarizing the conversation, tape record the conversation, or have a court reporter record the conversation. An application for a warrant approving the interception must be made in accordance with section 626A.06 within 36 hours after the interception has occurred, or begins to occur. In the absence of a warrant, the interception must immediately end when the communication sought is obtained or when the application for the warrant is denied, whichever is earlier. If application for approval is denied, or in any other case where the interception is ended without a warrant having been issued, the contents of a wire, oral, or electronic communication intercepted must be treated as having been obtained in violation of this chapter and an inventory shall be served as provided for in section 626A.10 on the person named in the application. **626A.15 Duty To Report Violations.** Any officer or employee of a telephone or telegraph company shall report to the police department or county attorney having jurisdiction, any violation of this chapter coming to the officer or employee's attention.
Mississippi	**41-29-507. Bureau of Narcotics only agency authorized to possess, operate, etc. monitoring devices; exceptions.** (1) No person, agency of the state or political subdivision of the state, other than the Bureau of Narcotics, is authorized by this article to own, possess, install, operate or monitor an electronic, mechanical or other device. The Bureau of Narcotics may be assisted by an investigative or law enforcement officer in the operation and monitoring of an interception of wire, oral or other communications, provided that an agent of the Bureau of Narcotics is present at all times. (2) The director shall designate, in writing, the agents of the Bureau of Narcotics who are responsible for the possession, installation, operation and monitoring of electronic, mechanical or other devices for the

	bureau. **97-25-49. Wrongful access to telecommunications messages by cellular telephone; inadmissibility of information obtained in violation of this section.** (1) A person who commits either of the following offenses shall be punished by a fine of not more than One Thousand Dollars ($1,000.00), or by imprisonment in the county jail not exceeding six (6) months, or both: (a) Wrongfully obtains, or attempts to obtain, any knowledge of a private telecommunications message by gaining access to the origination, transmission, emission or reception of signs, signals, data, writings, images and sounds or intelligence of any nature by cellular telephone, when such person is not the lawfully intended recipient of the message or is not authorized to have access to such message, or by connivance with a clerk, operator, messenger or other employee of a telecommunications company; or (b) Being such clerk, operator, messenger or other employee, uses, or suffers to be used, or willfully divulges to anyone but the person for whom it was intended, the contents of a cellular phone message. (c) The provisions of this subsection shall not apply to the use of a telephone monitoring device by either a law enforcement agency acting pursuant to a valid court order or to a corporation or other business entity engaged in marketing research or telephone solicitation conversations by an employee of the corporation or other business entity when the monitoring is used for the purpose of service quality control and the monitoring is used with the consent of at least one (1) person who is a party to the conversation. (d) The provisions of this subsection shall not apply to an employee of a cellular telephone company who discloses or uses an intercepted communication in the normal course of business as a necessary incident to providing service or to the protection of the rights or property of the employer or who provides assistance to an investigative or law enforcement officer acting under a valid court order. (2) Any information obtained in violation of this section shall not be admissible in any civil proceeding unless the information was obtained by the lawful owner of the device that obtained the information.
Missouri	**542.402. Penalty for illegal wiretapping, permitted activities. —** 1. Except as otherwise specifically provided in sections 542.400 to 542.422, a person is guilty of a class D felony and upon conviction shall be punished as provided by law, if such person: (1) Knowingly intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire communication; (2) Knowingly uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when such device transmits communications by radio or interferes with the transmission of such communication; provided, however, that nothing in sections 542.400 to 542.422 shall be construed to prohibit the use by law enforcement officers of body microphones and transmitters in undercover investigations for the acquisition of evidence and the protection of law enforcement officers and others working under their direction in such investigations; (3) Knowingly discloses, or endeavors to disclose, to any other person the contents of any wire communication, when he knows or has reason to know that the information was obtained through the interception of a wire communication in violation of this subsection; or (4) Knowingly uses, or endeavors to use, the contents of any wire communication, when he knows or has reason to know that the information was obtained through the interception of a wire communication in violation of this subsection. 2. It is not unlawful under the provisions of sections 542.400 to 542.422: (1) For an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the carrier of such communication, however, communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks; (2) For a person acting under law to intercept a wire or oral communication, where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception; (3) For a person not acting under law to intercept a wire communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act.
Montana	**45-8-213. Privacy in communications.** (1) Except as provided in 69-6-104, a person commits the offense of violating privacy in communications if the person knowingly or purposely: (a) with the purpose to terrify, intimidate, threaten, harass, annoy, or offend, communicates with a person by

	electronic communication and uses obscene, lewd, or profane language, suggests a lewd or lascivious act, or threatens to inflict injury or physical harm to the person or property of the person. The use of obscene, lewd, or profane language or the making of a threat or lewd or lascivious suggestions is prima facie evidence of an intent to terrify, intimidate, threaten, harass, annoy, or offend. (b) uses an electronic communication to attempt to extort money or any other thing of value from a person or to disturb by repeated communications the peace, quiet, or right of privacy of a person at the place where the communications are received; (c) records or causes to be recorded a conversation by use of a hidden electronic or mechanical device that reproduces a human conversation without the knowledge of all parties to the conversation. This subsection (1)(c) does not apply to: (i) elected or appointed public officials or to public employees when the transcription or recording is done in the performance of official duty; (ii) persons speaking at public meetings; (iii) persons given warning of the transcription or recording, and if one person provides the warning, either party may record; or (iv) a health care facility, as defined in 50-5-101, or a government agency that deals with health care if the recording is of a health care emergency telephone communication made to the facility or agency. (2) Except as provided in 69-6-104, a person commits the offense of violating privacy in communications if the person purposely intercepts an electronic communication. This subsection does not apply to elected or appointed public officials or to public employees when the interception is done in the performance of official duty or to persons given warning of the interception. (3)(a) A person convicted of the offense of violating privacy in communications shall be fined an amount not to exceed $500 or be imprisoned in the county jail for a term not to exceed 6 months, or both. (b) On a second conviction of subsection (1)(a) or (1)(b), a person shall be imprisoned in the county jail for a term not to exceed 1 year or be fined an amount not to exceed $1,000, or both. (c) On a third or subsequent conviction of subsection (1)(a) or (1)(b), a person shall be imprisoned in the state prison for a term not to exceed 5 years or be fined an amount not to exceed $10,000, or both. (4) "Electronic communication" means any transfer between persons of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system. History: En. 94-8-114 by Sec. 1, Ch. 513, L. 1973; amd. Sec. 33, Ch. 359, L. 1977; R.C.M. 1947, 94-8-114; amd. Sec. 1, Ch. 356, L. 1979; amd. Sec. 1, Ch. 177, L. 1991; amd. Sec. 3, Ch. 354, L. 1999; amd. Sec. 8, Ch. 77, L. 2001; amd. Sec. 4, Ch. 344, L. 2003; amd. Sec. 1, Ch. 435, L. 2005; amd. Sec. 1, Ch. 214, L. 2007. Criminal Law Commission Comments: Source: Derived from Revised Codes of Montana 1947, §§ 94-3203, 94-3320, 94-3321, 94-3323, 94-35-220, 94-35-221.5, 94-35-274 and 94-35-275. This statute is merely a recodification of the old Montana law. A comprehensive electronic surveillance proposal was defeated by the 1971 state legislature. Compiler's Comments: 2007 Amendment: Chapter 214 in (1)(c)(iii) at end after "recording" inserted "and if one person provides the warning, either party may record"; and made minor changes in style. Amendment effective July 1, 2007. 2005 Amendment: Chapter 435 in (1)(c)(i) near middle and (2) in second sentence near middle before "employees" inserted "to public"; inserted (1)(c)(iv) excepting from subsection (1)(c) a health care emergency phone communication to a health care facility or to a government agency dealing with health care; and made minor changes in style. Amendment effective October 1, 2005. 2003 Amendment: Chapter 344 in (1)(a) near beginning after "person by" substituted "electronic communication" for "telephone or electronic mail"; in (1)(b) at beginning after "uses" substituted "an electronic communication" for "a telephone or electronic mail", near middle after "repeated" substituted "communications" for "telephone calls or electronic mailings", and at end after "where the" substituted "communications" for "telephone call or calls or electronic mailings"; deleted former (1)(d) through (1)(f) that read: "(d) by means of any machine, instrument, or contrivance or in any other manner: (i) reads or attempts to read a message or learn the contents of a message while it is being sent over a telegraph line or by electronic mail; (ii) learns or attempts to learn the contents of a message while it is in a telegraph office or is being received at or sent from a telegraph office; or (iii) uses, attempts to use, or communicates to others any information obtained as provided in this subsection (1)(d); (e) discloses the contents of a telegraphic message, electronic mail, or any part of a telegraphic message or electronic mail addressed to another person without the permission of the person, unless directed to do so by the lawful order of a court; or (f) opens or reads or causes to be read any sealed letter or electronic mail not addressed to the person opening the letter or reading the electronic mail without being authorized to do so by either the writer of the letter, the sender of the electronic mail, or the person to whom the letter or electronic mail is addressed or, without the like authority, publishes any of the contents of the letter or electronic mail knowing the letter or electronic

	mail to have been unlawfully opened"; deleted former (2) that read: "(2) Subsection (1) does not apply to an employer or a representative of an employer who opens or reads, causes to be opened or read, or further publishes an electronic mail or other message that either originates at or is received by a computer or computer system that is owned, leased, or operated by or for the employer"; in (2) in first sentence after "intercepts" substituted "an electronic" for "a telephonic voice or data"; inserted (4) defining electronic communication; and made minor changes in style. Amendment effective October 1, 2003. 2001 Amendment: Chapter 77 throughout section inserted references to electronic mail and electronic mailings; inserted (2) excepting an employer or representative of an employer who opens or further publishes electronic mail on a computer that is owned, leased, or operated by the employer; and made minor changes in style. Amendment effective July 1, 2001. 1999 Amendment: Chapter 354 in (1)(c) at end before "recording" inserted "transcription or"; inserted (2) establishing that, with certain exceptions, purposeful interception of a telephonic voice or data communication constitutes the offense of violating privacy in communications; and made minor changes in style. Amendment effective October 1, 1999. 1991 Amendment: Inserted (2)(b) establishing a penalty for second conviction involving illegal telephone calls; and inserted (2)(c) establishing a penalty for third or subsequent conviction involving illegal telephone calls. Annotator's Note: This section recodifies prior Montana law. The use of obscene or threatening language is prima facie evidence of an intent to "terrify, intimidate, threaten, harass, annoy, or offend". The 1977 amendment reworded subsection (1)(a). As enacted, this subsection used the term "intent"; as amended the term "intent" was replaced with the term "purpose", and in doing so made the provision consistent with the rest of the Criminal Code of 1973. The 1977 amendment also placed the last sentence of subsection (1)(a) in parentheses; inserted "any conversation" in subsection (1)(c); and made other minor changes in wording and punctuation. Subsection (1)(c) continues the blanket prohibition of R.C.M. 1947, § 94-35-274 on recording conversations without the consent of all the parties and the exceptions contained in R.C.M. 1947, § 94-35-275 for public officials in the course of their official duties and for public meetings. Subsections (1)(d) and (1)(e) prohibit the interception of telegraph messages both by tapping the lines and by inspection in the telegraph office. Disclosure of a telegraphic message addressed to another without the other's permission is also prohibited. These provisions parallel prior law provisions R.C.M. 1947, §§ 94-3322, 94-3323, 94-35-220 and 94-3321. Opening, reading or causing to read a sealed letter addressed to another without that other's authorization is prohibited by subsection (1)(f) which replaces prior law, R.C.M. 1947, § 94-3320. Also made punishable in conformity with prior law are those individuals who, without authority, publish the contents of an unlawfully opened letter. The penalties for these various offenses have been made uniform as misdemeanors. This represents a reduction in most cases since under prior law penalties could range as high as 5 years in some instances (94-35-221.5, 94-3321, 3322, 3323, 94-35-220). The 1979 amendment added the phrase, "except as provided in 69-6-104", in subsection (1). Section 69-6-104 was enacted at the same time to permit supervisory law enforcement personnel to control telephone communications to and from a person holding hostages and to limit the liability of telephone company officials. In St. v. Brackman, 178 Mont. 105, 582 P.2d 1216 (1978), the Montana Supreme Court struck down police use of warrantless consensual participant monitoring, i.e., the use of electronic surveillance equipment concealed on a police informant whose conversations with the defendant are simultaneously transmitted to concealed agents. The court held that electronic interception by third parties of conversations between individuals who neither consent to nor know of the interception was a violation of the right to privacy guaranteed by the Montana Constitution. A "compelling state interest" was held to be required under Montana's constitutional right to privacy before participant electronic monitoring could be engaged in. In St. v. Hanley, decided on March 14, 1980, (opinion after rehearing) the court approved of the procedure whereby officers obtained a search warrant prior to engaging in participant electronic monitoring. The court did not make clear what showing was required to obtain such a search warrant, whether of "probable cause" or "compelling state interest". However, it appears that even a compelling state interest showing requirement would not impose a terribly heavy burden on the state. In State ex rel. Zander v. District Court, 180 Mont. 548, 591 P.2d 656 (1979), the court held that there was no impermissible infringement of the right of privacy guaranteed under Art. II, sec. 10 of Montana's constitution where an officer, informed by a neighbor of the defendant that he thought a burglary was in progress at defendant's trailer, entered defendant's trailer without a warrant (and inadvertently discovered some marijuana plants), since the state has a "compelling state interest" in protecting the home and property of its citizens from unlawful intrusion. It is, in light of this opinion,

	conceivable that the court would find the state's interest in enforcing its laws to be a "compelling state interest" which would permit issuance of a search warrant to allow participant electronic monitoring. Cross References: Right of privacy, Art. II, sec. 10, Mont. Const. Knowingly defined, 45-2-101. Purposely defined, 45-2-101. Threat defined, 45-2-101. Control of telephone communication to and from person holding hostages — nonliability of telephone company officials, 69-6-104. Case Notes: Discretion of Prosecutor in Charging Defendant When Facts Support Possibility of More Than One Crime: After threatening to shoot his estranged wife's boyfriend during a telephone call, Smith was charged with assault with a weapon. Smith contended that he should instead have been charged with violation of privacy in communications through intimidation over the telephone and that the assault with a weapon charge should have been dismissed. The Supreme Court disagreed. The two charges were distinctly different, and the facts of the case supported a charge for either crime. Thus, the crime to be charged was a matter of prosecutorial discretion, and the County Attorney did not abuse those broad discretionary powers in charging Smith with assault with a weapon. St. v. Smith, 2004 MT 191, 322 Mont. 206, 95 P.3d 137 (2004). Sufficient Evidence of Indirect Telephone Conversation to Warrant Conviction of Violating Privacy in Communications: Flowers' wife Pamela received a telephone call from her son, who was at Flowers' residence. While speaking to her son, she heard Flowers yelling in the background that he was going to kill Pamela. As a result of Flowers' statements, he was charged with violating privacy in communications. At trial, Flowers moved for a directed verdict on grounds that because he did not have a telephone conversation with Pamela, he could not have used the telephone to threaten her. The motion was denied, and on appeal, the Supreme Court affirmed. Although Flowers did not have a direct telephone conversation with Pamela, he nevertheless communicated a message over the telephone that was threatening in nature, which constituted sufficient evidence for the jury to find Flowers guilty of violating privacy in communications. St. v. Flowers, 2004 MT 37, 320 Mont. 49, 86 P.3d 3 (2004). No Error in Admission of Recorded Telephone Calls Made While Defendant in Prison — No Expectation of Privacy: At DuBray's homicide trial, the state introduced into evidence recordings of telephone calls between DuBray and others while DuBray was incarcerated in state and federal facilities. DuBray argued that the evidence was inadmissible under state and federal wiretap laws. Although monitoring and recording telephone conversations are a search within the meaning of state and federal constitutions, under St. v. Scheetz, 286 Mont. 41, 950 P.2d 722 (1997), when no reasonable expectation of privacy exists, there is neither a search nor a seizure. At both the state and federal facilities, DuBray was notified that telephone calls were subject to monitoring and recording, so no reasonable expectation of privacy in the calls existed. Evidence of the calls was properly admitted because DuBray consented to the recording. St. v. DuBray, 2003 MT 255, 317 Mont. 377, 77 P.3d 247 (2003). Admissibility of Recording of Warrantless Face-to-Face Conversation by Police Use of Body Wire Transmitting Device: Warrantless consensual electronic monitoring of face-to-face conversations by the use of a body wire transmitting device, when performed by law enforcement officers while pursuing their official duties, does not violate the constitutional right to be free of unreasonable search and seizure or the right of privacy. Consent must be clearly obtained from at least one party to the conversation and must be freely made and without compulsion. As in telephone conversations, the consenting party may be an informant or police officer. Evidence obtained from such monitoring is admissible in a subsequent criminal trial. St. v. Brown, 232 Mont. 1, 755 P.2d 1364, 45 St. Rep. 818 (1988), overruling St. v. Brackman, 178 Mont. 105, 582 P.2d 1216 (1978), and reaffirmed in St. v. Belgarde, 244 Mont. 500, 798 P.2d 539, 47 St. Rep. 1762 (1990). Interpretation of Largely Inaudible Tape Recording by Police — No Prejudice: It was not prejudicial to allow introduction of mostly inaudible tape recordings made with the consent and participation of an informant nor to allow a police officer who was present when the recordings were made to act as an oral transcriber to interpret what was said and what occurred while the tapes were being made. St. v. Morse, 229 Mont. 222, 746 P.2d 108, 44 St. Rep. 1919 (1987). Deputy Sheriff — Public Employee Authorized to Employ Hidden Device: A Deputy Sheriff serving as an undercover officer in a neighboring county is a public employee with an official duty to maintain contact with persons involved in the drug scene and thus is a person authorized by this section to use a hidden electronic device to record conversations so far as it is done in compliance with the guidelines set forth in St. v. Brackman, 178 Mont. 105, 582 P.2d 1216 (1978). St. v. Hanley, 186 Mont. 410, 608 P.2d 104, 37 St. Rep. 427 (1980). Electronic Recording — Consent of One Party in Conversation: The recording of a conversation between an undercover officer and defendant during a drug sale using a hidden electronic monitoring device that was authorized by court order as required by St. v.

	Brackman, 178 Mont. 105, 582 P.2d 1216 (1978), is not subject to suppression by virtue of 18 U.S.C. 2511(2)(c) and is permitted by 45-8-213, if one of the party consents to the recording, as the undercover officer did here. The recording being legal it is then subject only to ordinary rules of admissibility. St. v. Hanley, 186 Mont. 410, 608 P.2d 104, 37 St. Rep. 427 (1980), followed in St. v. Coleman, 189 Mont. 492, 616 P.2d 1090, 37 St. Rep. 1661 (1980), St. v. Canon, 212 Mont. 157, 687 P.2d 705, 41 St. Rep. 1659 (1984), and St. v. Brown, 232 Mont. 1, 755 P.2d 1364, 45 St. Rep. 818 (1988). Effect on Constitutional Requirements: Subsection (1)(c), which excuses certain conduct by public officials or employees from criminal liability, neither addresses nor modifies any constitutional requirements relating to search and seizure. St. v. Leighty, 179 Mont. 366, 588 P.2d 526, 35 St. Rep. 2017 (1978). Police Monitoring: Article II, sec. 10 and 11, Mont. Const., protects the individual from any monitoring and recording by the state without a search warrant or prior showing of compelling state interest of conversations between the individual and police informants even though the informants consented to the monitoring and recording. Section 45-8-213 does not give consensual participant monitoring the status of a compelling state interest. St. v. Brackman, 178 Mont. 105, 582 P.2d 1216, 35 St. Rep. 1103 (1978), followed in St. v. Coleman, 189 Mont. 492, 616 P.2d 1090, 37 St. Rep. 1661 (1980), and St. v. Canon, 212 Mont. 157, 687 P.2d 705, 41 St. Rep. 1659 (1984). Brackman overruled in St. v. Brown, 232 Mont. 1, 755 P.2d 1364, 45 St. Rep. 818 (1988). Law Review Articles: Privacy: This article discusses the growing awareness of the right to privacy in state and federal contexts. An historical perspective of the right is outlined and recent developments are highlighted. Towe, 37 Mont. L.Rev. 39 (1976). Protection for Invasions of Conversational and Communication Privacy by Electronic Surveillance in Family, Marriage, and Domestic Disputes Under Federal and State Wiretap and Store Communications Acts and the Common Law Privacy Intrusion Tort, Turkington, 82 Neb. L.Rev. 693 (2004). Privacy and Power: Computer Databases and Metaphors for Information Privacy, Solove, 53 Stan. L.Rev. 1393 (2001). Collateral References: Telecommunications key 1012, 1013, 1435 through 1440. 86 C.J.S. Telegraphs, Telephones, Radio, and Television §§ 104, 106, 110 through 112. Offense of obtaining telephone services by unauthorized use of another's telephone number — state cases. 61 ALR 4th 1197. **Montana, United States of America, Plaintiff-Appellee v Jeffrey Brian Ziegler, Defendant-Appellant., U.S. Court of Appeals, Ninth Circuit, 153 LC January 30, 2007- Privacy: Workplace Privacy: Locked Office.–** An employee's reasonable expectation of privacy in his locked office was subject to the possibility that his employer could consent to a search of its own premises. **Privacy: Workplace Privacy: Computer.–** Given that an employer owned all workplace computers, routinely monitored those computers, informed employees of this practice, and assigned computers for business use only, an employee could not reasonably have had an expectation of privacy in his computer, even though it was stored in the employee's private, locked office.
Nebraska	86-290 Unlawful acts; penalty. (1) Except as otherwise specifically provided in sections 86-271 to 86-295, it is unlawful to: (a) Intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept any wire, electronic, or oral communication; (b) Intentionally use, endeavor to use, or procure any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication or (ii) such device transmits communications by radio or interferes with the transmission of such communication; (c) Intentionally disclose or endeavor to disclose to any other person the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this subsection; (d) Intentionally use or endeavor to use the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this subsection; or (e) Having knowledge that an investigative or law enforcement officer has been authorized or has applied for authorization under sections 86-271 to 86-2,115 to intercept a wire, oral, or electronic communication, give notice or attempt to give notice of the possible interception to any person in order to obstruct, impede, or prevent such interception. Except as provided in subdivisions (4)(a) and (5)(b) of this section, any person who violates this subsection is guilty of a Class IV felony. (2)(a) It is not unlawful under sections 86-271 to 86-295 for an employer on his, her, or its business premises, for an operator of a switchboard, or for an officer, employee, or agent of any provider, the facilities of which are used

	in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his, her, or its employment while engaged in any activity which is a necessary incident to the rendition of his, her, or its service or to the protection of the rights or property of the carrier or provider of such communication services. Such employers and providers shall not utilize service observing or random monitoring except for mechanical, service quality, or performance control checks as long as reasonable notice of the policy of random monitoring is provided to their employees. (b) It is not unlawful under sections 86-271 to 86-295 for a person acting under color of law to intercept a wire, electronic, or oral communication when such person is a party to the communication or one of the parties to the communication has given prior consent to such interception. (c) It is not unlawful under sections 86-271 to 86-295 for a person not acting under color of law to intercept a wire, electronic, or oral communication when such person is a party to the communication or when one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state. (d) It is not unlawful under sections 86-271 to 86-295: (i) To intercept or access an electronic communication made through an electronic communications system that is configured so that such electronic communication is readily accessible to the general public; (ii) To intercept any radio communication which is transmitted: (A) By any station for the use of the general public or that relates to ships, aircraft, vehicles, or persons in distress; (B) By any governmental, law enforcement, emergency management, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (C) By a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (D) By any marine or aeronautical communications system; (iii) To intercept or receive, or to assist in the interception or receipt of: (A) Any communications service offered over a cable system as provided in 47 U.S.C. 553, as such section existed on January 1, 2002; or (B) Any satellite cable programming for private viewing as provided in 47 U.S.C. 605, as such section existed on January 1, 2002; (iv) To intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment to the extent necessary to identify the source of such interference; or (v) For other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system if such communication is not scrambled or encrypted. (e) It is not unlawful under sections 86-271 to 86-295 and 86-298 to 86-2,101: (i) To use a pen register or a trap-and-trace device; or (ii) For a provider of an electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service from fraudulent, unlawful, or abusive use of such service. (3)(a) Except as provided in subsection (1) of this section and subdivision (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication, other than one to such person or entity or an agent thereof, while in transmission on such service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient. (b) A person or entity providing an electronic communication service to the public may divulge the contents of any such communication: (i) As otherwise authorized in subdivision (a) of this subsection or section 86-292; (ii) With the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) To a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or (iv) Which was inadvertently obtained by the provider and which appears to pertain to the commission of a crime if such divulgence is made to a law enforcement officer. (4)(a) If the offense is a first offense under subsection (1) of this section and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain and the wire or electronic communication with respect to the offense under subsection (1) of this section is a radio communication that is not scrambled or encrypted, then: (i) If the communication is not the radio portion of a cellular telephone communication, a public land mobile radio service communication, or a paging service communication and the conduct is not that described in subsection (5) of this section, the offense is a Class I misdemeanor; or (ii) If the communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication, or a paging service communication, the offense is a Class III misdemeanor.

	(b) Conduct, otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted: (i) To a broadcasting station for purposes of retransmission to the general public; or (ii) as an audio subcarrier intended for redistribution to facilities open to the public but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain. (5)(a) If the communication is: (i) A private satellite video communication that is not scrambled or encrypted and the conduct in violation of sections 86-271 to 86-295 is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or (ii) a radio communication that is transmitted on frequencies allocated for remote pickup broadcast stations under subpart D of 47 C.F.R. part 74, as such regulations existed on January 1, 2002, and that is not scrambled or encrypted and the conduct in violation of sections 86-271 to 86-295 is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the state in a court of competent jurisdiction. (b) In an action under this subsection: (i) If the violation is a first offense by the person under subsection (1) of this section and such person has not been found liable in a civil action under section 86-297, the state shall be entitled to appropriate injunctive relief; and (ii) If the violation is a second or subsequent offense under subsection (1) of this section or such person has been found liable in any prior civil action under section 86-297, the person shall be subject to a mandatory five-hundred-dollar civil fine. (c) The court may use any means within its authority to enforce an injunction issued under this subsection and shall impose a civil fine of not less than five hundred dollars for each violation of such an injunction. Laws 1969, c. 854, § 2, p. 3211; Laws 1977, LB 39, § 329; Laws 1988, LB 899, § 2; Laws 1996, LB 43, § 52; R.S. 1943, (1999), § 86-702; Laws 2002, LB 1105, § 152. Message intercepted by one who was not a party to the communication, nor acting under color of law or with prior consent, is not admissible in evidence. White v. Longo, 190 Neb. 703, 212 N.W.2d 84 (1973).
Nevada	**200.620 Interception and attempted interception of wire communication prohibited; exceptions.** 1. Except as otherwise provided in NRS 179.410 to 179.515, inclusive, 209.419 and 704.195, it is unlawful for any person to intercept or attempt to intercept any wire communication unless: (a) The interception or attempted interception is made with the prior consent of one of the parties to the communication; and (b) An emergency situation exists and it is impractical to obtain a court order as required by NRS 179.410 to 179.515, inclusive, before the interception, in which event the interception is subject to the requirements of subsection 3. If the application for ratification is denied, any use or disclosure of the information so intercepted is unlawful, and the person who made the interception shall notify the sender and the receiver of the communication that: (1) The communication was intercepted; and (2) Upon application to the court, ratification of the interception was denied. 2. This section does not apply to any person, or to the officers, employees or agents of any person, engaged in the business of providing service and facilities for wire communication where the interception or attempted interception is to construct, maintain, conduct or operate the service or facilities of that person. 3. Any person who has made an interception in an emergency situation as provided in paragraph (b) of subsection 1 shall, within 72 hours of the interception, make a written application to a justice of the Supreme Court or district judge for ratification of the interception. The interception must not be ratified unless the applicant shows that: (a) An emergency situation existed and it was impractical to obtain a court order before the interception; and (b) Except for the absence of a court order, the interception met the requirements of NRS 179.410 to 179.515, inclusive. 4. NRS 200.610 to 200.690, inclusive, do not prohibit the recording, and NRS 179.410 to 179.515, inclusive, do not prohibit the reception in evidence, of conversations on wire communications installed in the office of an official law enforcement or fire-fighting agency, or a public utility, if the equipment used for the recording is installed in a facility for wire communications or on a telephone with a number listed in a directory, on which emergency calls or requests by a person for response by the law enforcement or fire-fighting agency or public utility are likely to be received. In addition, those sections do not prohibit the recording or reception in evidence of conversations initiated by the law enforcement or fire-fighting agency or public utility from such a facility or telephone in connection with responding to the original call or request, if the agency or public utility informs the other party that the conversation is being recorded.

	704.285 Violation of law governing interception or disclosure of communications made by wire or radio: Investigation; hearing; orders to cease and desist. 1. The Commission, upon its own information or knowledge or upon a complaint by any person, firm, partnership or corporation that any public utility is acting in violation of the provisions of NRS 179.410 to 179.515, inclusive, or NRS 200.610 to 200.690, inclusive, or is knowingly allowing another person to violate those provisions, shall proceed without notice to make an investigation of the information or complaint. 2. If, after its investigation, the Commission determines that there is probable cause to believe that the utility is acting in violation of the provisions of NRS 179.410 to 179.515, inclusive, or NRS 200.610 to 200.690, inclusive, or allowing another to act in violation of those provisions, the Commission shall forthwith issue a cease and desist order to the utility. The order is permanent unless the utility, within 20 days after receipt of the order, files a written request for a hearing with the Commission. 3. When a written request for a hearing is filed pursuant to subsection 2, the Commission shall conduct the hearing pursuant to the provisions of NRS 703.320 to 703.370, inclusive. 4. If, as the result of a hearing, it is determined that the utility is acting in violation of the provisions of NRS 179.410 to 179.515, inclusive, or NRS 200.610 to 200.690, inclusive, or allowing another to act in violation of those provisions, the Commission shall issue a permanent cease and desist order and notify the district attorney of the county where the violation occurred of its determination. 5. This section is applicable whether or not the utility involved is required to have a certificate of public convenience and necessity from the Commission. **391.—.Teachers and other licensed personnel; Monitoring of employees arrested on matters that would be grounds for suspension or license revocation; Term "arrest" defined**—As used in sections 2 to 5, inclusive, of this act, "arrest" has the meaning ascribed to it in NRS 171.104. **391.—Teachers and other licensed personnel; Department of Education to adopt regulations to establish procedure for monitoring of employees arrested on matters that would be grounds for suspension or license revocation; Procedures; Notice requirements; Documentation and monitoring of status of employee; Personnel records**—1. The Department shall adopt regulations that establish a procedure for the notification, tracking and monitoring of the status of criminal cases involving persons who are licensed pursuant to chapter 391 of NRS. The procedure must include, without limitation: (a) A method by which the superintendent of schools of a school district and the administrative head of a charter school must notify the Department in a timely manner of the arrest of a person who is licensed pursuant to chapter 391 of NRS if: (1) The act for which the licensee is arrested: (I) May be a ground for the suspension or revocation of the person's license pursuant to NRS 391.330; and (II) Is not excluded by the Department from the notification requirements of this section; and (2) The school district or charter school has knowledge of that arrest. (b) A method by which the superintendent of schools of a school district and the administrative head of a charter school must notify the Department in a timely manner of: (1) Each action, if any, taken against the licensee by the school district or charter school after the arrest; and (2) The conviction of the licensee, if he is convicted of the act for which he was arrested. (c) The steps that the Department must follow in response to the receipt of notice pursuant to this section, including, without limitation, the preparation of a separate file on the licensee for the documentation and monitoring of the status of the case. 2. Each file that is maintained on a licensee pursuant to subsection 1 must include, without limitation: (a) The date on which the person was arrested and the date on which the Department received notice of the arrest from the school district or charter school; (b) The reason why the licensee was arrested; (c) The steps taken by the Department in response to all notices received by the Department from a school district or charter school pursuant to subsection 1; (d) An indication whether the case was referred to the Attorney General's office for review and the date of the referral, if any; (e) An indication whether the Superintendent of Public Instruction has presented the case to the State Board for action and the type of action recommended by the Superintendent, if any; (f) A description of any action taken by the State Board against the licensee and the reason for that action, or if no action is taken by the State Board, the reason for the inaction; and (g) The final resolution of the case and the date of resolution. 3. If the Department receives notice of a conviction of a licensee and the conviction is for an act which is a ground for the suspension or revocation of a license, the Superintendent of Public Instruction shall immediately recommend that the State Board proceed in accordance with the provisions of NRS 391.320 to 391.361, inclusive. 4. If the Department maintains a file on a licensee pursuant to this

	section and the State Board determines that there is not sufficient evidence to suspend or revoke the license, the file and any related documents must not be made a part of that licensee's permanent employment record. **391. Teachers and other licensed personnel; Monitoring of employees arrested on matters that would be grounds for suspension or license revocation; School superintendent of school district and administrative head of charter school to submit required information within set time frame**---The superintendent of schools of each school district and the administrative head of each charter school shall submit all information required by the Department pursuant to section 3 of this act within the time prescribed by the Department. **Nevada, United States of America, Plaintiff-Appellant v SDI Future Health, Inc et al, Defendants-Appellees., U.S. Court of Appeals, Ninth Circuit, 157, (Jan. 27, 2009) --Public Employees: Constitutional Rights: Workplace Searches.–** In order to establish standing for Fourth Amendment purposes to challenge the search of a workplace beyond an employee's internal office, the employee must show some personal connection to the places searched and the materials seized.
New Hampshire	**570-A:2 Interception and Disclosure of Telecommunication or Oral Communications Prohibited.** I. A person is guilty of a class B felony if, except as otherwise specifically provided in this chapter or without the consent of all parties to the communication, the person: (a) Wilfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any telecommunication or oral communication; (b) Wilfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when: (1) Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in telecommunication, or (2) Such device transmits communications by radio, or interferes with the transmission of such communication, or (3) Such use or endeavor to use (A) takes place on premises of any business or other commercial establishment, or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment; or (c) Wilfully discloses, or endeavors to disclose, to any other person the contents of any telecommunication or oral communication, knowing or having reason to know that the information was obtained through the interception of a telecommunication or oral communication in violation of this paragraph; or (d) Willfully uses, or endeavors to use, the contents of any telecommunication or oral communication, knowing or having reason to know that the information was obtained through the interception of a telecommunication or oral communication in violation of this paragraph. I-a. A person is guilty of a misdemeanor if, except as otherwise specifically provided in this chapter or without consent of all parties to the communication, the person knowingly intercepts a telecommunication or oral communication when the person is a party to the communication or with the prior consent of one of the parties to the communication, but without the approval required by RSA 570-A:2, II(d). II. It shall not be unlawful under this chapter for: (a) Any operator of a switchboard, or an officer, employee, or agent of any communication common carrier whose facilities are used in the transmission of a telecommunication, to intercept, disclose, or use that communication in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the carrier of such communication; provided, however, that said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks. (b) An officer, employee, or agent of any communication common carrier to provide information, facilities, or technical assistance to an investigative or law enforcement officer who, pursuant to this chapter, is authorized to intercept a telecommunication or oral communication. (c) Any law enforcement officer, when conducting investigations of or making arrests for offenses enumerated in this chapter, to carry on the person an electronic, mechanical or other device which intercepts oral communications and transmits such communications by radio. (d) An investigative or law enforcement officer in the ordinary course of the officer's duties pertaining to the conducting of investigations of organized crime, offenses enumerated in this chapter, solid waste violations under RSA 149-M:9, I and II, or harassing or obscene telephone calls to intercept a telecommunication or oral communication, when such person is a party to the communication or one of the parties to the communication has given prior consent to such interception; provided, however, that no such interception shall be made unless the attorney general, the deputy attorney general, or an assistant

	attorney general designated by the attorney general determines that there exists a reasonable suspicion that evidence of criminal conduct will be derived from such interception. Oral authorization for the interception may be given and a written memorandum of said determination and its basis shall be made within 72 hours thereafter. The memorandum shall be kept on file in the office of the attorney general. (e) Where the offense under investigation is defined in RSA 318-B, the attorney general to delegate authority under RSA 570-A:2, II(d) to a county attorney. The county attorney may exercise this authority only in the county where the county attorney serves. The attorney general shall, prior to the effective date of this subparagraph, adopt specific guidelines under which the county attorney may give authorization for such interceptions. Any county attorney may further delegate authority under this section to any assistant county attorney in the county attorney's office. (f) An officer, employee, or agent of the Federal Communications Commission, in the normal course of employment and in discharge of the monitoring responsibilities exercised by the commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a telecommunication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained. (g) Any law enforcement officer, when conducting investigations of or making arrests for offenses enumerated in this chapter, to carry on the person an electronic, mechanical or other device which intercepts oral communications and transmits such communications by radio. (h) Any municipal, county, or state fire or police department, the division of emergency services and communications as created by RSA 21-P:48-a, including the bureau of emergency communications as defined by RSA 106-H, or any independently owned emergency service, and their employees in the course of their employment, when receiving or responding to emergency calls, to intercept, record, disclose or use a telecommunication, while engaged in any activity which is a necessary incident to the rendition of service or the protection of life or property. (i) Any public utility regulated by the public utilities commission, and its employees in the course of employment, when receiving central dispatch calls or calls for emergency service, or when responding to central dispatch calls or calls for emergency service, to intercept, record, disclose or use a telecommunication, while engaged in any activity which is a necessary incident to the rendition of service, or the protection of life and property. Any public utility recording calls pursuant to this subparagraph shall provide an automatic tone warning device which automatically produces a distinct signal that is repeated at regular intervals during the conversation. The public utilities commission may adopt rules relative to the recording of emergency calls under RSA 541-A. (j) A uniformed law enforcement officer to make an audio recording in conjunction with a video recording of a routine stop performed in the ordinary course of patrol duties on any way as defined by RSA 259:125, provided that the officer shall first give notification of such recording to the party to the communication. (k)(1) The owner or operator of a school bus, as defined in RSA 259:96, to make an audio recording in conjunction with a video recording of the interior of the school bus while students are being transported to and from school or school activities, provided that the school board authorizes audio recording, the school district provides notification of such recording to the parents and students as part of the district's pupil safety and violence prevention policy required under RSA 193-F:3, I(b), and there is a sign informing the occupants of such recording prominently displayed on the school bus. (2) Prior to any audio recording, the school board shall hold a public hearing to determine whether audio recording should be authorized in school buses, and if authorized, the school board shall establish an administrative procedure to address the length of time which the recording is retained, ownership of the recording, limitations on who may listen to the recording, and provisions for erasing or destroying the recording. Such administrative procedure shall permit the parents or legal guardian of any student against whom a recording is being used as part of a disciplinary proceeding to listen to the recording. In no event, however, shall the recording be retained for longer than 10 school days unless the school district determines that the recording is relevant to a disciplinary proceeding, or a court orders that it be retained for a longer period of time. An audio recording shall only be reviewed if there has been a report of an incident or a complaint relative to conduct on the school bus, and only that portion of the audio recording which is relevant to the incident or complaint shall be reviewed. (*l*) A law enforcement officer in the ordinary course of the officer's duties using any device capable of making an audio or video recording, or both, and which is attached to and used in conjunction with a TASER or other similar electroshock device. Any person who is the subject of such recording shall be informed of the existence of the audio or video recording, or both, and shall be provided with a copy of such recording at his or her request.

	570-B:2 General Prohibition on Pen Register and Trap and Trace Devices. I. Except as otherwise provided in this chapter, a person is guilty of an offense if he installs or uses a pen register or a trap and trace device without first obtaining a court order under this chapter. II. The offense is a misdemeanor if the violation of this chapter is a first offense. If the violation of this chapter is a second or subsequent offense, the person shall be guilty of a class B felony. **644:9 Violation of Privacy.** I. A person is guilty of a class A misdemeanor if such person unlawfully and without the consent of the persons entitled to privacy therein, installs or uses: (a) Any device for the purpose of observing, photographing, recording, amplifying, broadcasting, or in any way transmitting images or sounds of the private body parts of a person including the genitalia, buttocks, or female breasts, or a person's body underneath that person's clothing; or (b) In any private place, any device for the purpose of observing, photographing, recording, amplifying or broadcasting, or in any way transmitting images or sounds in such place; or (c) Outside a private place, any device for the purpose of hearing, recording, amplifying, broadcasting, or in any way transmitting images or sounds originating in such place which would not ordinarily be audible or comprehensible outside such place. II. As used in this section, "private place" means a place where one may reasonably expect to be safe from surveillance including public restrooms, locker rooms, the interior of one's dwelling place, or any place where a person's private body parts including genitalia, buttocks, or female breasts may be exposed. III. A person is guilty of a class A misdemeanor if that person knowingly disseminates or causes the dissemination of any photograph or video recording of himself or herself engaging in sexual activity with another person without the express consent of the other person or persons who appear in the photograph or videotape. In this paragraph, "disseminate" and "sexual activity" shall have the same meaning as in RSA 649-A:2. III-a. A person is guilty of a misdemeanor if, for the purpose of arousing or gratifying the person's sexual desire, he or she knowingly views another person, without that person's knowledge or consent, in a place where one would have a reasonable expectation of privacy. For purposes of this paragraph, "views" means looking at another person with the unaided eye or any device intended to improve visual acuity. IV. A person is guilty of a misdemeanor if such person knowingly enters any residential curtilage, as defined in RSA 627:9, I, or any other private place as defined in paragraph II of this section, without lawful authority and looks into the residential structure thereon or other private place with no legitimate purpose. V. Paragraphs I and II shall not be construed to impair or limit any otherwise lawful activities of law enforcement personnel, nor are paragraphs I and II intended to limit employees of governmental agencies or other entities, public or private, who, in the course and scope of their employment and supported by articulable suspicion, attempt to capture any type of visual image, sound recording, or other physical impression of a person during an investigation, surveillance, or monitoring of conduct to obtain evidence of suspected illegal activity, the suspected violation of any administrative rule or regulation, a suspected fraudulent insurance claim, or any other suspected fraudulent conduct or activity involving a violation of law, or pattern of business practices adversely affecting the public health or safety.
New Jersey	**2A:156A-3. Interception, disclosure, use of wire, electronic, oral communication; violation** Except as otherwise specifically provided in this act, any person who: a. Purposely intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication; or b. Purposely discloses or endeavors to disclose to any other person the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or c. Purposely uses or endeavors to use the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the interception of a wire, electronic or oral communication; shall be guilty of a crime of the third degree. Subsections b. and c. of this section shall not apply to the contents of any wire, electronic or oral communication, or evidence derived therefrom, that has become common knowledge or public information.
New Mexico	**30-12-1. Interference with communications; exception.** Interference with communications consists of knowingly and without lawful authority: A. displacing, removing, injuring or destroying any radio station, television tower, antenna or cable, telegraph or telephone line, wire, cable, pole or conduit belonging to another, or the material or property appurtenant thereto; B. cutting, breaking, tapping or making any connection with any telegraph or telephone line, wire, cable or instrument belonging to or

	in the lawful possession or control of another, without the consent of such person owning, possessing or controlling such property; C. reading, interrupting, taking or copying any message, communication or report intended for another by telegraph or telephone without the consent of a sender or intended recipient thereof; D. preventing, obstructing or delaying the sending, transmitting, conveying or delivering in this state of any message, communication or report by or through telegraph or telephone; or E. using any apparatus to do or cause to be done any of the acts hereinbefore mentioned or to aid, agree with, comply or conspire with any person to do or permit or cause to be done any of the acts hereinbefore mentioned. Whoever commits interference with communications is guilty of a misdemeanor, unless such interference with communications is done: (1) under a court order as provided in Sections 30-12-2 through 30-12-11 NMSA 1978; or (2) by an operator of a switchboard or an officer, employee or agent of any communication common carrier in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his services or to the protection of rights or property of the carrier of such communication; or (3) by a person acting under color of law in the investigation of a crime, where such person is a party to the communication, or one of the parties to the communication has given prior consent to such interception, monitoring or recording of such communication.
New York	**250.05 Penal. Eavesdropping.** A person is guilty of eavesdropping when he unlawfully engages in wiretapping, mechanical overhearing of a conversation, or intercepting or accessing of an electronic communication. Eavesdropping is a class E felony. **250.25 Penal. Tampering with private communications.** A person is guilty of tampering with private communications when: 1. Knowing that he does not have the consent of the sender or receiver, he opens or reads a sealed letter or other sealed private communication; or 2. Knowing that a sealed letter or other sealed private communication has been opened or read in violation of subdivision one of this section, he divulges without the consent of the sender or receiver, the contents of such letter or communication, in whole or in part, or a resume of any portion of the contents thereof; or 3. Knowing that he does not have the consent of the sender or receiver, he obtains or attempts to obtain from an employee, officer or representative of a telephone or telegraph corporation, by connivance, deception, intimidation or in any other manner, information with respect to the contents or nature thereof of a telephonic or telegraphic communication; except that the provisions of this subdivision do not apply to a law enforcement officer who obtains information from a telephone or telegraph corporation pursuant to section 250.35; or 4. Knowing that he does not have the consent of the sender or receiver, and being an employee, officer or representative of a telephone or telegraph corporation, he knowingly divulges to another person the contents or nature thereof of a telephonic or telegraphic communication; except that the provisions of this subdivision do not apply to such person when he acts pursuant to section 250.35. Tampering with private communications is a class B misdemeanor. **700.10 Crim. Proc. Eavesdropping and video surveillance warrants; in general.** 1. Under circumstances prescribed in this article, a justice may issue an eavesdropping warrant or a video surveillance warrant upon ex parte application of an applicant who is authorized by law to investigate, prosecute or participate in the prosecution of the particular designated offense which is the subject of the application. 2. No eavesdropping or video surveillance warrant may authorize or approve the interception of any communication or the conducting of any video surveillance for any period longer than is necessary to achieve the objective of the authorization, or in any event longer than thirty days. Such thirty day period shall begin on the date designated in the warrant as the effective date, which date may be no later than ten days after the warrant is issued. **705.05 Crim. Proc. Pen register and trap and trace authorizations; in general.** Under circumstances prescribed in this article, a justice may issue an order authorizing the use of a pen register or a trap and trace device upon ex parte application of an applicant who is authorized by law to investigate, prosecute or participate in the prosecution of the designated crimes which are the subject of the application. **250.15 Penal. Failure to report wiretapping.** A telephone or telegraph corporation is guilty of failure to report wiretapping when, having knowledge of the occurrence of unlawful wiretapping, it does not report such matter to an appropriate law enforcement officer or agency. Failure to report wiretapping is a class B misdemeanor.

	203-c. Monitoring of employees; Employee protections; Privacy; Video recording of an employee in a restroom, locker room, or other room designated for changing clothes is prohibited; Exceptions—1. No employer may cause a video recording to be made of an employee in a restroom, locker room, or room designated by an employer for employees to change their clothes, unless authorized by court order. 2. No video recording made in violation of this section may be used by an employer for any purpose. 3. In any civil action alleging a violation of this section, the court may: (a) Award damages and reasonable attorneys' fees and costs to a prevailing plaintiff; and (b) Afford injunctive relief against any employer that commits or proposes to commit a violation of this section. 4. The rights and remedies provided herein shall be in addition to, and not supersede, any other rights and remedies provided by statute or common law. 5. The provisions of this section do not apply with respect to any law enforcement personnel engaged in the conduct of his or her authorized duties. **New York, U.S. Court of Appeals, Second Circuit, 144 LC (Sept. 26, 2001) 144 LC United States Court of Appeals, Second Circuit. No 00-9306. September 26, 2001, 266 F.3d 64).-- Privacy: Workplac Privacy: Search of Computer.–** Although a public employee had some expectation of privacy in the contents of his office computer, searches of his computer by his employing agency were reasonable in light of the agency's need to investigate allegations of misconduct as balanced against the intrusion caused by the searches. **Public Employees: Due Process Rights: Adverse Employment Action.–** An employee's due process rights were not violated by his loss of a provisional job appointment and his failure to receive a discretionary salary increase because neither involved property or liberty interests protected by the Fourteenth Amendment.
North Carolina	**15A-287. Interception and disclosure of wire, oral, or electronic communications prohibited.** (a) Except as otherwise specifically provided in this Article, a person is guilty of a Class H felony if, without the consent of at least one party to the communication, the person: (1) Willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication. (2) Willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when: a. The device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communications; or b. The device transmits communications by radio, or interferes with the transmission of such communications. (3) Willfully discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through violation of this Article; or (4) Willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this Article. (b) It is not unlawful under this Article for any person to: (1) Intercept or access an electronic communication made through an electronic communication system that is configured so that the electronic communication is readily accessible to the general public; (2) Intercept any radio communication which is transmitted: a. For use by the general public, or that relates to ships, aircraft, vehicles, or persons in distress; b. By any governmental, law enforcement, civil defense, private land mobile, or public safety communication system, including police and fire, readily available to the general public; c. By a station operating on any authorized band within the bands allocated to the amateur, citizens band, or general mobile radio services; or d. By any marine or aeronautical communication system; or (3) Intercept any communication in a manner otherwise allowed by Chapter 119 of the United States Code. (c) It is not unlawful under this Article for an operator of a switchboard, or an officer, employee, or agent of a provider of electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of employment while engaged in any activity that is a necessary incident to the rendition of his or her service or to the protection of the rights or property of the provider of that service, provided that a provider of wire or electronic communication service may not utilize service observing or random monitoring except for mechanical or service quality control checks. (d) It is not unlawful under this Article for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of Chapter 5 of Title 47 of the United States Code, to intercept a wire

	or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained. (e) Any person who, as a result of the person's official position or employment, has obtained knowledge of the contents of any wire, oral, or electronic communication lawfully intercepted pursuant to an electronic surveillance order or of the pendency or existence of or implementation of an electronic surveillance order who shall knowingly and willfully disclose such information for the purpose of hindering or thwarting any investigation or prosecution relating to the subject matter of the electronic surveillance order, except as is necessary for the proper and lawful performance of the duties of his position or employment or as shall be required or allowed by law, shall be guilty of a Class G felony. (f) Any person who shall, knowingly or with gross negligence, divulge the existence of or contents of any electronic surveillance order in a way likely to hinder or thwart any investigation or prosecution relating to the subject matter of the electronic surveillance order or anyone who shall, knowingly or with gross negligence, release the contents of any wire, oral, or electronic communication intercepted under an electronic surveillance order, except as is necessary for the proper and lawful performance of the duties of his position or employment or as is required or allowed by law, shall be guilty of a Class 1 misdemeanor. (g) Any public officer who shall violate subsection (a) or (d) of this section or who shall knowingly violate subsection (e) of this section shall be removed from any public office he may hold and shall thereafter be ineligible to hold any public office, whether elective or appointed. **15A-262. Application for order for pen register or trap and trace device.** (a) Application. — A law enforcement officer may make an application for an order or an extension of an order under G.S. 15A-263 authorizing or approving the installation and use of a pen register or a trap and trace device, in writing under oath or affirmation, to a superior court judge. (b) Contents of Application. — An application under subsection (a) of this section shall include: (1) The identity of the law enforcement officer making the application and the identity of the law enforcement agency conducting the investigation; and (2) A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency. **15A-261. Prohibition and exceptions.** (a) In General. — Except as provided in subsection (b) of this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order as provided in this Article. (b) Exception. — The prohibition of subsection (a) of this section does not apply to the use of a pen register or a trap and trace device by a provider of wire or electronic communication service: (1) Relating to the operation, maintenance, or testing of a wire or electronic communication service or to the protection of the rights or property of the provider, or to the protection of users of that service from abuse of service or unlawful use of service; or (2) To record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) With the consent of the user of that service. (c) Penalty. — A person who willfully and knowingly violates subsection (a) of this section is guilty of a Class 1 misdemeanor.
North Dakota	**12.1-15-02. Interception of wire or oral communications — Eavesdropping.** 1. A person is guilty of a class C felony if he: a. Intentionally intercepts any wire or oral communication by use of any electronic, mechanical, or other device; or b. Intentionally discloses to any other person or intentionally uses the contents of any wire or oral communication, knowing that the information was obtained through the interception of a wire or oral communication. 2. A person is guilty of a class A misdemeanor if he secretly loiters about any building with intent to overhear discourse or conversation therein and to repeat or publish the same with intent to vex, annoy, or injure others. 3. It is a defense to a prosecution under subsection 1 that: a. The actor was authorized by law to intercept, disclose, or use, as the case may be, the wire or oral communication. b. The actor was (1) a person acting under color of law to intercept a wire or oral communication, and (2) he was a party to the communication or one of the parties to the communication had given prior consent to such interception. c. (1) The actor was a party to the communication or one of the parties to the communication had given prior consent to such interception, and (2) such communication was not intercepted for the purpose of committing a crime or other unlawful harm. **29-29.3-02. Prohibition on pen register and trap and trace device use — Exception.** A person may not install or use a pen register or trap and trace device without first obtaining a court order under this

	chapter. The prohibition in this section does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service: 1. Relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; 2. To record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful, or abusive use of service; or 3. Where the consent of the user of that service has been obtained.
Ohio	**2933.52. (A) No person purposely shall do any of the following:** (A) No person purposely shall do any of the following: (1) Intercept, attempt to intercept, or procure another person to intercept or attempt to intercept a wire, oral, or electronic communication; (2) Use, attempt to use, or procure another person to use or attempt to use an interception device to intercept a wire, oral, or electronic communication, if either of the following applies: (a) The interception device is affixed to, or otherwise transmits a signal through, a wire, cable, satellite, microwave, or other similar method of connection used in wire communications; (b) The interception device transmits communications by radio, or interferes with the transmission of communications by radio. (3) Use, or attempt to use, the contents of a wire, oral, or electronic communication, knowing or having reason to know that the contents were obtained through the interception of a wire, oral, or electronic communication in violation of sections 2933.51 to 2933.66 of the Revised Code. (B) This section does not apply to any of the following: (1) The interception, disclosure, or use of the contents, or evidence derived from the contents, of an oral, wire, or electronic communication that is obtained through the use of an interception warrant issued pursuant to sections 2933.53 to 2933.56 of the Revised Code, that is obtained pursuant to an oral approval for an interception granted pursuant to section 2933.57 of the Revised Code, or that is obtained pursuant to an order that is issued or an interception that is made in accordance with section 802 of the "Omnibus Crime Control and Safe Streets Act of 1968," 82 Stat. 237, 254, 18 U.S.C. 2510 to 2520 (1968), as amended, the "Electronic Communications Privacy Act of 1986," 100 Stat. 1848-1857, 18 U.S.C. 2510-2521 (1986), as amended, or the "Foreign Intelligence Surveillance Act," 92 Stat. 1783, 50 U.S.C. 1801.11 (1978), as amended; (2) An operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication to intercept, disclose, or use that communication in the normal course of employment while engaged in an activity that is necessary to the rendition of service or to the protection of the rights or property of the provider of that service, except that a provider of wire or electronic communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks; (3) A law enforcement officer who intercepts a wire, oral, or electronic communication, if the officer is a party to the communication or if one of the parties to the communication has given prior consent to the interception by the officer; (4) A person who is not a law enforcement officer and who intercepts 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 the person prior consent to the interception, and if the communication is not intercepted for the purpose of committing a criminal offense or tortious act in violation of the laws or Constitution of the United States or this state or for the purpose of committing any other injurious act; (5) An officer, employee, or agent of a communications common carrier providing information, facilities, or technical assistance to an investigative officer who is authorized to intercept a wire, oral, or electronic communication pursuant to sections 2933.51 to 2933.66 of the Revised Code; (6) The use of a pen register in accordance with federal or state law; (7) The use of a trap and trace device in accordance with federal or state law; (8) A police, fire, or emergency communications system to intercept wire communications coming into and going out of the communications system of a police department, fire department, or emergency center, if both of the following apply: (a) The telephone, instrument, equipment, or facility is limited to the exclusive use of the communication system for administrative purposes; (b) At least one telephone, instrument, equipment, or facility that is not subject to interception is made available for public use at each police department, fire department, or emergency center. (9) The interception or accessing of an electronic communication made through an electronic communication system that is configured so that the electronic communication is readily accessible to the general public. (10) The interception of a radio communication that is transmitted by any of the following; (a) A station for the

	use of the general public; (b) A governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including a police or fire system, that is readily accessible to the general public; (c) A station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; (d) A marine or aeronautical communications system. (11) The interception of a radio communication that relates to a ship, aircraft, vehicle, or person in distress. (12) The interception of a wire or electronic communication the transmission of which is causing harmful interference to a lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of that interference. (13) Other users of the same frequency to intercept a radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of that system, if the communication is not scrambled or encrypted. (C) Whoever violates this section is guilty of interception of wire, oral, or electronic communications, a felony of the fourth degree. **4931.26. No person connected with a telegraph or messenger company, incorporated....** No person connected with a telegraph or messenger company, incorporated or unincorporated, operating a telegraph line or engaged in the business of receiving and delivering messages, shall willfully divulge the contents or the nature of the contents of a private communication entrusted to him for transmission or delivery, willfully refuse or neglect to transmit or deliver it, willfully delay its transmission or delivery, or willfully forge the name of the intended receiver to a receipt for such message, communication, or article of value entrusted to him by said company, with intent to injure, deceive, or defraud the sender or intended receiver thereof or such telegraph or messenger company, or to benefit himself or any other person. **4931.29. No person connected with a telephone company, incorporated or....** No person connected with a telephone company, incorporated or unincorporated, operating a telephone line or engaged in the business of transmitting to, from, through, or in this state, telephone messages, in any capacity, shall willfully divulge a private telephone message or the nature of such message, or a private conversation between persons communicating over the wires of such company, or willfully delay the transmission of a telephonic message or communication, with intent to injure, deceive, or defraud the sender or receiver thereof or any other person, or any such telephone company, or to benefit himself or any other person. **2933.52.1] § 2933.521. (A) Except as provided in division (B) of this section, no person....** (A) Except as provided in division (B) of this section, no person or entity that provides electronic communication service to the public shall purposely divulge the content of a communication, while it is in transmission on that service, to a person or entity other than an addressee or intended recipient of the communication or an agent of an addressee or intended recipient of the communication. (B)(1) Division (A) of this section does not apply to a communication being transmitted to the person or entity providing the electronic communication service or to an agent of that person or entity. (2) Notwithstanding division (A) of this section, a person or entity that provides electronic communication service to the public may divulge the content of a communication that is in transmission on that service in any of the following circumstances: (a) The divulgence is authorized by division (B)(2) of section 2933.52, by section 2933.581 [2933.58.11, by division (C) of section 2933.55, or by division (F) or (G) of section 2933.59 of the Revised Code or by a provision of the "Electronic Communications Privacy Act of 1986," 100 Stat. 1848-1857, 18 U.S.C. 2510-2521 (1986), as amended. (b) The originator or an addressee or intended recipient of the communication has lawfully consented to the divulgence. (c) The divulgence is made to a person who is employed or authorized, or whose facilities are used, to forward the communication to its destination. (d) The content of the communication divulged was inadvertently obtained by the provider of the service, the content appears to pertain to the commission of a crime, and the divulgence is made to a law enforcement agency. (C) Neither division (A) of this section nor any other provision of sections 2933.51 to 2933.66 of the Revised Code prohibits a provider of electronic communication service from recording the fact that a wire or electronic communication was initiated or completed, in order to protect the provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of the electronic communication service from fraudulent, unlawful, or abusive use of the electronic communication service.
Oklahoma	**13-176.3. Prohibited acts — Felonies — Penalties — Venue.** Except as otherwise specifically

	provided in this act, any person is guilty of a felony and upon conviction shall be punished by a fine of not less than Five Thousand Dollars ($5,000.00), or by imprisonment of not more than five (5) years, or by both who: 1. Willfully intercepts, endeavors to intercept or procures any other person to intercept or endeavor to intercept any wire, oral or electronic communication; 2. Willfully uses, endeavors to use or procures any other person to use or endeavor to use any electronic, mechanical or other device to intercept any oral communication; 3. Willfully discloses or endeavors to disclose to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained in violation of the provisions of the Security of Communications Act; 4. Willfully uses or endeavors to use the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained in violation of the provisions of the Security of Communications Act; 5. Willfully and maliciously, without legal authority, removes, injures or obstructs any telephone or telegraph line, or any part or appurtenances or apparatus connected thereto, or severs any wires thereof; 6. Sends through the mail or sends or carries any electronic, mechanical or other device with the intention of rendering the device primarily useful for the purpose of the illegal interception of wire, oral or electronic communications in violation of the provisions of the Security of Communications Act; 7. Manufactures, assembles, possesses or sells any electronic, mechanical or other device with the intention of rendering the device primarily useful for the purpose of the illegal interception of wire, oral or electronic communications in violation of the provisions of the Security of Communications Act; or 8. Willfully uses any communication facility in committing or in causing or facilitating the commission of any act or acts constituting one or more of the felonies enumerated in Section 176.7[13A-176.7] of this title. Each separate use of a communication facility to cause or facilitate such a felony shall be a separate offense. Venue for any violation of this section shall lie in the same county as venue for the underlying felony enumerated in Section 176.7[13A-176.7] of this title **13-177.2. Installation or use of pen register or trap and trace device without court order — Exceptions — Penalty** A. Except as otherwise provided in this section, no person shall install or use a pen register or a trap and trace device without first obtaining a court order as provided by Section 4 of this act. B. The prohibition of subsection A of this section shall not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service: 1. Relating to the operation, maintenance and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; 2. To record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication or a user of that service, from fraudulent, unlawful or abusive use of service; or 3. Where the consent of the user of that service has been obtained. C. Any person knowingly violating the provisions of subsection A of this section, upon conviction, shall be guilty of a misdemeanor and shall be punishable by a fine not exceeding One Thousand Dollars ($1,000.00) or by imprisonment of not more than one (1) year, or by both such fine and imprisonment. **Sec. 200.Employer searches of employee-owned vehicles limited to employer property**.— Employers of this state that conduct employee-owned vehicle searches of its employees shall conduct such search on the property of the employer only. Searches that are conducted on property not owned or rented by the employer shall require a search warrant issued according to law.
Oregon	**133.721 Definitions for ORS 41.910 and 133.721 to 133.739.** As used in ORS 41.910 and 133.721 to 133.739, unless the context requires otherwise: (1) "Aggrieved person" means a person who was a party to any wire, electronic or oral communication intercepted under ORS 133.724 or 133.726 or a person against whom the interception was directed and who alleges that the interception was unlawful. (2) "Contents," when used with respect to any wire, electronic or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport or meaning of that communication. (3) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a radio, electromagnetic, photoelectronic or photo-optical system, or transmitted in part by wire, but does not include: (a) Any oral communication or any communication that is completely by wire; or (b) Any communication made through a tone-only paging device. (4) "Electronic, mechanical

	or other device" means any device or apparatus that can be used to intercept a wire, electronic or oral communication other than: (a) Any telephone or telegraph instrument, equipment or facility, or any component thereof that is furnished to the subscriber or user by a telecommunications carrier in the ordinary course of its business and that is being used by the subscriber or user in the ordinary course of its business or being used by a telecommunications carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of official duties; or (b) A hearing aid or similar device being used to correct subnormal hearing to not better than normal. (5) "Intercept" means the acquisition, by listening or recording, of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device. (6) "Investigative or law enforcement officer" means an officer or other person employed by a county sheriff or municipal police department, the Oregon State Police, Attorney General, a district attorney or the Department of Corrections, and officers or other persons employed by law enforcement agencies of other states or the federal government, to investigate or enforce the law. (7) "Oral communication" means: (a) Any oral communication, other than a wire or electronic communication, uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation; or (b) An utterance by a person who is participating in a wire or electronic communication, if the utterance is audible to another person who, at the time the wire or electronic communication occurs, is in the immediate presence of the person participating in the communication. (8) "Telecommunications carrier" means: (a) A telecommunications utility as defined in ORS 759.005; or (b) A cooperative corporation organized under ORS chapter 62 that provides telecommunications services. (9) "Telecommunications service" has the meaning given that term in ORS 759.005. (10) "Wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection between the point of origin and the point of reception, whether furnished or operated by a public utility or privately owned or leased. **165.540 Obtaining contents of communications. **Update notice:** This section has been amended by Senate Bill 309 of 2009 (1) Except as otherwise provided in ORS 133.724 or 133.726 or subsections (2) to (7) of this section, a person may not: (a) Obtain or attempt to obtain the whole or any part of a telecommunication or a radio communication to which the person is not a participant, by means of any device, contrivance, machine or apparatus, whether electrical, mechanical, manual or otherwise, unless consent is given by at least one participant. (b) Tamper with the wires, connections, boxes, fuses, circuits, lines or any other equipment or facilities of a telecommunication or radio communication company over which messages are transmitted, with the intent to obtain unlawfully the contents of a telecommunication or radio communication to which the person is not a participant. (c) Obtain or attempt to obtain the whole or any part of a conversation by means of any device, contrivance, machine or apparatus, whether electrical, mechanical, manual or otherwise, if not all participants in the conversation are specifically informed that their conversation is being obtained. (d) Obtain the whole or any part of a conversation, telecommunication or radio communication from any person, while knowing or having good reason to believe that the conversation, telecommunication or radio communication was initially obtained in a manner prohibited by this section. (e) Use or attempt to use, or divulge to others, any conversation, telecommunication or radio communication obtained by any means prohibited by this section. (2)(a) The prohibitions in subsection (1)(a), (b) and (c) of this section do not apply to: (A) Officers, employees or agents of a telecommunication or radio communication company who perform the acts prohibited by subsection (1)(a), (b) and (c) of this section for the purpose of construction, maintenance or conducting of their telecommunication or radio communication service, facilities or equipment. (B) Public officials in charge of and at jails, police premises, sheriffs' offices, Department of Corrections institutions and other penal or correctional institutions, except as to communications or conversations between an attorney and the client of the attorney. (b) Officers, employees or agents of a telecommunication or radio communication company who obtain information under paragraph (a) of this subsection may not use or attempt to use, or divulge to others, the information except for the purpose of construction, maintenance, or conducting of their telecommunication or radio communication service, facilities or equipment. (3) The prohibitions in subsection (1)(a), (b) or (c) of this section do not apply to subscribers or members of their family who perform the acts prohibited in subsection (1) of this section in their homes. (4) The prohibitions in subsection (1)(a) of this section do not apply to the

	receiving or obtaining of the contents of any radio or television broadcast transmitted for the use of the general public. (5) The prohibitions in subsection (1)(c) of this section do not apply to: (a) A person who records a conversation during a felony that endangers human life; (b) A law enforcement officer who is in uniform and displaying a badge and who is operating a vehicle-mounted video camera that records the scene in front of, within or surrounding a police vehicle, unless the officer has reasonable opportunity to inform participants in the conversation that the conversation is being obtained; or (c) A law enforcement officer who, acting in the officer's official capacity, deploys an Electro-Muscular Disruption Technology device that contains a built-in monitoring system capable of recording audio or video, for the duration of that deployment. (6) The prohibitions in subsection (1)(c) of this section do not apply to persons who intercept or attempt to intercept with an unconcealed recording device the oral communications that are part of any of the following proceedings: (a) Public or semipublic meetings such as hearings before governmental or quasi-governmental bodies, trials, press conferences, public speeches, rallies and sporting or other events; (b) Regularly scheduled classes or similar educational activities in public or private institutions; or (c) Private meetings or conferences if all others involved knew or reasonably should have known that the recording was being made. (7) The prohibitions in subsection (1)(a), (c), (d) and (e) of this section do not apply to any: (a) Radio communication that is transmitted by a station operating on an authorized frequency within the amateur or citizens bands; or (b) Person who intercepts a radio communication that is transmitted by any governmental, law enforcement, civil defense or public safety communications system, including police and fire, readily accessible to the general public provided that the interception is not for purposes of illegal activity. (8) Violation of subsection (1) or (2)(b) of this section is a Class A misdemeanor. (9) As used in this section: (a) "Electro-Muscular Disruption Technology device" means a device that uses a high-voltage, low power charge of electricity to induce involuntary muscle contractions intended to cause temporary incapacitation. "Electro-Muscular Disruption Technology device" includes devices commonly known as tasers. (b) "Law enforcement officer" has the meaning given that term in ORS 133.726. **165.515 Bribery of telegraph company agents to disclose contents of message.** (1) Any person who, by the payment or promise of any bribe, inducement or reward, procures or attempts to procure any telegraphic agent, operator or employee to disclose any private message, or the contents, purport, substance of meaning thereof, or who offers to any such person any bribe, compensation or reward for the disclosure of any private information received by such person by reason of trust, or who uses or attempts to use information so obtained, shall be punished upon conviction by a fine not to exceed $1,000, or imprisonment not to exceed one year, or both. (2) Any person violating this section shall be liable in a civil suit for all damages occasioned thereby.
Pennsylvania	**18 Pa.C.S.A. § 5703. Interception, disclosure or use of wire, electronic or oral communications** Except as otherwise provided in this chapter, a person is guilty of a felony of the third degree if he: (1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication; (2) intentionally discloses or endeavors to disclose to any other person the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or (3) intentionally uses or endeavors to use the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the interception of a wire, electronic or oral communication. **18 Pa.C.S.A. § 5771. General prohibition on use of certain devices and exception (a) General rule. —** Except as provided in this section, no person may install or use a pen register or a trap and trace device or a telecommunication identification interception device without first obtaining a court order under section 5773 (relating to issuance of an order for use of certain devices). **(b) Exception. —** The prohibition of subsection (a) does not apply with respect to the use of a pen register, a trap and trace device or a telecommunication identification interception device by a provider of electronic or wire communication service: (1) relating to the operation, maintenance and testing of a wire or electronic communication service or to the protection of the rights or property of the provider, or to the protection of users of the service from abuse of service or unlawful use of service; (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect the

	provider, another provider furnishing service toward the completion of the wire communication or a user of the service from fraudulent, unlawful or abusive use of service; or (3) with the consent of the user of the service. **(b.1) Limitation. —** A government agency authorized to install and use a pen register under this chapter shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing. **(c) Penalty. —** Whoever intentionally and knowingly violates subsection (a) is guilty of a misdemeanor of the third degree.
Rhode Island	**11-35-21. Unauthorized interception, disclosure or use of wire, electronic, or oral communication. —** (a) Except as otherwise specifically provided in chapter 5.1 of title 12, any person: (1) who willfully intercepts, attempts to intercept, or procures any other person to intercept or attempt to intercept, any wire, electronic, or oral communication; (2) who willfully discloses or attempts to disclose to any person the contents of any wire, electronic, or oral communication, knowing, or having reason to know that the information was obtained through interception of a wire, electronic, or oral communication in violation of this section; or (3) who willfully uses or attempts to use the contents of any wire, electronic, or oral communication, knowing, or having reason to know, that the information was obtained through interception of a wire, electronic, or oral communication in violation of this section; shall be imprisoned for not more than five (5) years. (b) The provisions of subdivisions (a)(2) and (3) of this section shall not apply to the contents of any wire, electronic, or oral communication, or evidence derived from those contents, which has become common knowledge or public information. (c) It shall not be unlawful under this chapter for: (1) An operator of a switchboard, or an officer, agent, or employee of a communication common carrier, whose facilities are used in the transmission of a wire, electronic, or oral communication, to intercept, disclose, or use that communication in the normal course of his or her employment while engaged in any activity which is a necessary incident to the rendition of his or her service or to the protection of the rights or property of the carrier of the communication. No communication common carrier shall utilize service observing or random monitoring except for mechanical or service quality control checks; (2) A person acting under color of law to intercept a wire, electronic, or oral communication, where that person is a party to the communication, or where one of the parties to the communication has given prior consent to the interception; or (3) A person not acting under color of law to intercept a wire, electronic, or oral communication, where the person is a party to the communication, or one of the parties to the communication has given prior consent to the interception unless the communication is intercepted for the purpose of committing any criminal or tortious act in the violation of the constitution or laws of the United States or of any state or for the purpose of committing any other injurious act. **12-5.1-2. Application for orders. —** (a) The attorney general, or an assistant attorney general specially designated by the attorney general, may apply ex parte to the presiding justice of the superior court of competent jurisdiction for an order authorizing the interception of any wire, electronic, or oral communications. Each application ex parte for an order must be in writing, subscribed and sworn to by the applicant. (b) The application must contain: (1) The identity of the officer making the application; (2) A full and complete statement of the facts and circumstances relied upon by the applicant to justify his or her belief that an order should be issued, including: (i) Details as to the particular designated offense that has been, is being, or is about to be committed; (ii) A particular description of the nature and location of the facilities from which, or the place where, the communication is to be intercepted; (iii) A particular description of the type of communications sought to be intercepted; and (iv) The identity of the person, if known, committing the offense and whose communications are to be intercepted; (3) A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous; (4) A statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization of interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur after the described type of communication has been first obtained; (5) A full and complete statement of the facts concerning all previous applications, known to the individual making the application, made to the presiding justice of the superior court for authorization to intercept wire, electronic, or oral communications involving any

	of the same persons, facilities or places specified in the application, and the action taken by the presiding justice of the superior court on each application; and (6) Where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain the results. (c) The presiding justice of the superior court may require the applicant to furnish additional testimony or documentary evidence in support of the application. (d) Allegations of fact in the application may be based either upon the personal knowledge of the applicant or upon information and belief. If the applicant personally knows the fact alleged, it must be so stated. If the facts establishing reasonable cause are derived in whole or in part from the statements of persons other than the applicant, the sources of the information and belief must be either disclosed or described, and the application must contain facts establishing the existence and reliability of the informant, or the reliability of the information supplied by the informant. The application must also state, so far as possible, the basis of the informant's knowledge or belief. If the applicant's information and belief is derived from tangible evidence or recorded oral evidence, a copy or detailed description of the evidence should be annexed to or included in the application. Affidavits of persons other than the applicant must be submitted in conjunction with the application if they tend to support any fact or conclusion alleged in the application. Accompanying affidavits may be based either on personal knowledge of the affiant, or information and belief with the source of the information and reason for the belief specified. **12-5.2-2. Application for an order for a pen register or a trap and trace device. —** (a) The attorney general or an assistant attorney general designated by the attorney general may make application for an order or an extension of an order pursuant to the provisions of § 12-5.2-3 authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to the presiding justice of the superior court or his or her designee in order to obtain information regarding a designated offense. (2) Any law enforcement officer set forth in § 12-5-3 may make application for an order or an extension of an order under § 12-5.2-3 authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation to the presiding justice of the superior court or his or her designee. (b) An application pursuant to subsection (a) of this section shall include: (1) The identity of the attorney general, assistant attorney general, or the law enforcement officer making the application and the identity of the law enforcement agency conducting the investigation; and (2) A certification by the applicant that the information likely to be obtained is relevant and necessary to an ongoing criminal investigation, that other investigative procedures have been or are being initiated or conducted, and that the request for the issuance of the pen register and/or trap and trace device is necessary to further an ongoing criminal investigation being conducted by that agency. **11-35-23. Failure to report to law enforcement officers. —** An employee of any communication common carrier who has knowledge obtained during the course of that employment of any violation of this chapter and willfully fails to report that knowledge within seven (7) days to the attorney general shall be guilty of a misdemeanor punishable by imprisonment for not more than one year, or by a fine of not more than five hundred dollars ($500), or both. **28-6.12-1. Privacy in the workplace; Employee privacy protection; Employers are prohibited from causing a video or audio tape to be made of employees in a restroom, locker room, or other room designated for changing clothes unless by court order; Use of recordings prohibited; Civil remedies**—No employer may cause an audio or video recording to be made of an employee in a restroom, locker room, or room designated by an employer for employees to change their clothes, unless authorized by court order. (b) No recording made in violation of this section may be used by an employer for any purpose. (c) In any civil action alleging a violation of this chapter, the court may: (1) award damages and reasonable attorneys' fees and cost to a prevailing plaintiff; and (2) afford injunctive relief against any employer that commits or proposes to commit a violation of this chapter. (d) The rights and remedies provided herein shall be in addition to, and not supersede, any other rights and remedies provided by statute or common law.
South Carolina	**17-30-20. Prohibited acts.** Except as otherwise specifically provided in this chapter, a person who commits any of the following acts is guilty of a felony and, upon conviction, must be punished as provided in Section 17-30-50 of this chapter: (1) intentionally intercepts, attempts to intercept, or

	procures any other person to intercept or attempt to intercept any wire, oral, or electronic communication; (2) intentionally uses, attempts to use, or procures any other person to use or attempt to use any electronic, mechanical, or other device to intercept any oral communication when: (a) the device is affixed to or otherwise transmits a signal through a wire, cable, or other like connection used in wire communication; or (b) the device transmits communications by radio or interferes with the transmission of the communication; (3) intentionally discloses or attempts to disclose to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; (4) intentionally uses or attempts to use the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or (5) intentionally discloses or attempts to disclose to any other person the contents of any wire, oral, or electronic communication intercepted by means authorized by Section 17-30-70 or Section 17-30-95 when that person knows or has reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation and the disclosure is not otherwise authorized under this chapter. **17-29-20. Installation of pen register or trap and trace device prohibited.** (A) Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under Section 17-29-40. (B) The prohibition of subsection (A) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service: (1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of the provider, or to the protection of users of that service from abuse of service or unlawful use of service; or (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful, or abusive use of service; or (3) where the consent of the user of that service has been obtained. (C) Any person violating the provisions of subsection (A) of this section is guilty of a misdemeanor and upon conviction must be punished by a fine of not more than one thousand dollars or by imprisonment for a term of not more than one year, or both. **16-17-470. Eavesdropping, peeping, voyeurism.** (A) It is unlawful for a person to be an eavesdropper or a peeping tom on or about the premises of another or to go upon the premises of another for the purpose of becoming an eavesdropper or a peeping tom. The term "peeping tom", as used in this section, is defined as a person who peeps through windows, doors, or other like places, on or about the premises of another, for the purpose of spying upon or invading the privacy of the persons spied upon and any other conduct of a similar nature, that tends to invade the privacy of others. The term "peeping tom" also includes any person who employs the use of video or audio equipment for the purposes set forth in this section. A person who violates the provisions of this section is guilty of a misdemeanor and, upon conviction, must be fined not more than five hundred dollars or imprisoned not more than three years, or both. (B) A person commits the crime of voyeurism if, for the purpose of arousing or gratifying sexual desire of any person, he or she knowingly views, photographs, audio records, video records, produces, or creates a digital electronic file, or films another person, without that person's knowledge and consent, while the person is in a place where he or she would have a reasonable expectation of privacy. A person who violates the provisions of this subsection: (1) for a first offense, is guilty of a misdemeanor and, upon conviction, must be fined not more than five hundred dollars or imprisoned not more than three years, or both; or (2) for a second or subsequent offense, is guilty of a felony and, upon conviction, must be fined not less than five hundred dollars or more than five thousand dollars or imprisoned not more than five years, or both. (C) A person commits the crime of aggravated voyeurism if he or she knowingly sells or distributes any photograph, audio recording, video recording, digital electronic file, or film of another person taken or made in violation of this section. A person who violates the provisions of this subsection is guilty of a felony and, upon conviction, must be fined not less than five hundred dollars or more than five thousand dollars or imprisoned not more than ten years, or both. (D) As used in this section: (1) "Place where a person would have a reasonable expectation of privacy" means: (a) a place where a reasonable person would believe that he or she could disrobe in privacy, without being concerned that his or her

	undressing was being photographed, filmed, or videotaped by another; or (b) a place where one would reasonably expect to be safe from hostile intrusion or surveillance. (2) "Surveillance" means secret observation of the activities of another person for the purpose of spying upon and invading the privacy of the person. (3) "View" means the intentional looking upon of another person for more than a brief period of time, in other than a casual or cursory manner, with the unaided eye or with a device designed or intended to improve visual acuity. (E) The provisions of subsection (A) do not apply to: (1) viewing, photographing, videotaping, or filming by personnel of the Department of Corrections or of a county, municipal, or local jail or detention center or correctional facility for security purposes or during investigation of alleged misconduct by a person in the custody of the Department of Corrections or a county, municipal, or local jail or detention center or correctional facility; (2) security surveillance for the purposes of decreasing or prosecuting theft, shoplifting, or other security surveillance measures in bona fide business establishments; (3) any official law enforcement activities conducted pursuant to Section 16-17-480; (4) private detectives and investigators conducting surveillance in the ordinary course of business; or (5) any bona fide news gathering activities. (F) In addition to any other punishment prescribed by this section or other provision of law, a person procuring photographs, audio recordings, video recordings, digital electronic files, or films in violation of this section shall immediately forfeit all items. These items must be destroyed when no longer required for evidentiary purposes.
South Dakota	**23A-35A-20.** Except as provided in § 23A-35A-21, a person is guilty of a Class 5 felony who being: (1) Not a sender or receiver of a telephone or telegraph communication, intentionally and by means of an eavesdropping device overhears or records a telephone or telegraph communication, or aids, authorizes, employs, procures, or permits another to so do, without the consent of either a sender or receiver thereof; (2) Not present during a conversation or discussion, intentionally and by means of an eavesdropping device overhears or records such conversation or discussion, or aids, authorizes, employs, procures, or permits another to so do, without the consent of a party to such conversation or discussion; or (3) Not a member of a jury, intentionally records or listens to by means of an eavesdropping device the deliberations of the jury or aids, authorizes, employs, procures, or permits another to so do.
Tennessee	**39-13-601. Wiretapping and electronic surveillance — Prohibited acts — Exceptions. —** (a)(1) Except as otherwise specifically provided in §§ 39-13-601 — 39-13-603 and title 40, chapter 6, part 3, a person commits an offense who: (A) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (B) Intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when: (i) The device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or (ii) The device transmits communications by radio, or interferes with the transmission of the communication; (C) Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection (a); or (D) Intentionally uses, or endeavors to use, the contents of any wire, oral or electronic communication, knowing or having reason to know, that the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection (a). (2) A violation of subdivision (a)(1) shall be punished as provided in § 39-13-602 and shall be subject to suit as provided in § 39-13-603. (b)(1) It is lawful under §§ 39-13-601 — 39-13-603 and title 40, chapter 6, part 3 for an officer, employee, or agent of a provider of wire or electronic communications service, or a telecommunications company, whose facilities are used in the transmission of a wire communication, to intercept, disclose or use that communication in the normal course of employment while engaged in any activity that is necessary to the rendition of service or to the protection of the rights or property of the provider of that service. Nothing in §§ 39-13-601 — 39-13-603 and title 40, chapter 6, part 3 shall be construed to prohibit a telecommunications or other company from engaging in service observing for the purpose of maintaining service quality standards for the benefit of consumers. (2) Notwithstanding any other law, providers of wire or electronic communications service, their officers, employees, or agents, landlords, custodians, or other persons are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications, if the provider, its officers, employees, or agents, landlord, custodian or other specified person has been provided with a court order signed by the

	authorizing judge of competent jurisdiction that: (A) Directs the assistance; (B) Sets forth a period of time during which the provision of the information, facilities, or technical assistance is authorized; and (C) Specifies the information, facilities, or technical assistance required. (3) No provider of wire or electronic communications service, officer, employee, or agent thereof, or landlord, custodian or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order, except as may otherwise be required by legal process, and then only after prior notification to the attorney general and reporter or to the district attorney general or any political subdivision of a district, as may be appropriate. Any such disclosure shall render the person liable for the civil damages provided for in § 39-13-603. No cause of action shall lie in any court against any provider of wire or electronic communications service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order under §§ 39-13-601 — 39-13-603 and title 40, chapter 6, part 3. (4) It is lawful under §§ 39-13-601 — 39-13-603 and title 40, chapter 6, part 3 for a person acting under the color of law to intercept a wire, oral or electronic communication, where the person is a party to the communication or one of the parties to the communication has given prior consent to such interception. (5) It is lawful under §§ 39-13-601 — 39-13-603 and title 40, chapter 6, part 3 for a person not acting under color of law to intercept a wire, oral, or electronic communication, where the person is a party to the communication or where one of the parties to the communication has given prior consent to the interception, unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the state of Tennessee. (6) It is unlawful to intercept any wire, oral, or electronic communication for the purpose of committing a criminal act. (7) It is lawful, unless otherwise prohibited by state or federal law, for any person: (A) To intercept or access an electronic communication made through an electronic communication system that is configured so that the electronic communication is readily accessible to the general public; (B) To intercept any radio communication that is transmitted by: (i) Any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (ii) Any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (iii) Any station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (iv) Any marine or aeronautical communications system; (C) To intercept any wire or electronic communication, the transmission of which is causing harmful interference with any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or (D) For other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted. (c)(1) Except as provided in subdivision (c)(2), a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication, other than one to such person or entity, or an agent thereof, while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient. (2) A person or entity providing electronic communication service to the public may divulge the contents of any such communication: (A) As otherwise authorized in subdivisions (b)(1)-(3) or § 40-6-306; (B) With the lawful consent of the originator or any addressee or intended recipient of such communication; (C) To a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or (D) That were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if the divulgence is made to a law enforcement agency **40-6-304. Order for electronic surveillance — Application — Required findings — Expiration of order — Recordings — Evidence — Motions to suppress. —** (a) Each application for an order authorizing the interception of a wire, oral or electronic communication shall be made in writing upon oath or affirmation to a judge of competent jurisdiction in the district where the interception of a wire, oral or electronic communication is to occur, or in any district where jurisdiction exists to prosecute the underlying offense to support an intercept order under § 40-6-305. The application shall state the investigative or law enforcement officer's authority to make the application and shall include the following information: (1) Identity of the investigative or law enforcement officer making the

	application, and the district attorney general authorizing the application; (2) A full and complete statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that an order should be issued, including: (A) Details as to the particular offense that has been, is being, or is about to be committed; (B) A particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted; (C) A particular description of the type of communications sought to be intercepted; and (D) The identity of all persons, if known, committing the offense and whose communications are to be or may be intercepted; (3) A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous; (4) A statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; (5) A full and complete statement of the facts concerning all previous applications known to the individuals authorizing and making the application, made to any judge for authorization to intercept wire, oral or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each application; and (6) Where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain results. (b) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application. (c) Upon an application the judge may enter an ex parte order, as requested or as modified, authorizing interception of wire, oral or electronic communications within the district in which the judge is sitting, and outside that district but within the state of Tennessee in the case of a mobile interception device, if the judge determines on the basis of the facts submitted by the applicant that: (1) There is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in § 40-6-305; (2) There is probable cause for belief that particular communications concerning that offense will be obtained through the interception; (3) Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and (4) There is probable cause for belief that the facilities from which, or the place where, the wire, oral or electronic communications are to be intercepted are being used, or about to be used, in connection with the commission of the offense, or are leased to, listed in the name of, or commonly used by the person. (d)(1) Each order authorizing the interception of any wire, oral or electronic communication under this part or §§ 39-13-601 — 39-13-603 shall specify: (A) The identity of all persons, if known, whose communications are to be or may be intercepted; (B) The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted; (C) A particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (D) The identity of the agency authorized to intercept the communications, and the identity of the person authorizing the application; and (E) The period of time during which the interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained. (2) An order authorizing the interception of a wire, oral or electronic communication under this part or §§ 39-13-601 — 39-13-603 shall, upon the request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish the applicant with all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that the service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian, or other person furnishing facilities or technical assistance shall be compensated by the applicant for reasonable expenses incurred in providing the facilities or assistance. (e) No order entered under this section may authorize or approve the interception of any wire, oral or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty (30) days. The thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten (10) days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (a) and the court making the findings required by subsection (c). The period of extension shall be no longer than the authorizing judge

	deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty (30) days. Every order and extension of an order shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in a way as to minimize the interception of communications not otherwise subject to interception under this part or §§ 39-13-601 — 39-13-603, and must terminate upon attainment of the authorized objective, or in any event in thirty (30) days. In the event the intercepted communication is in a code or foreign language, and an expert in that code or foreign language is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this part or §§ 39-13-601 — 39-13-603 may be conducted in whole or in part by state personnel, or by an individual operating under a contract with the state, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception. (f)(1) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this part or §§ 39-13-601 — 39-13-603 shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral or electronic communication under this subsection (f) shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under the judge's direction. All recordings of wire, oral, or electronic communications shall be treated as confidential and shall not be open for inspection by members of the public. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing judge and in any event shall be kept for ten (10) years; provided, that upon the agreement of the person whose communications were intercepted, or such person's counsel, and the appropriate district attorney general, the issuing judge may order the destruction of all such recordings at any time. Duplicate recordings may be made for use or disclosure pursuant to the provisions of § 40-6-306(a) and (b) for investigations, upon an order of the issuing judge. All duplicate recordings or written transcripts shall be treated as confidential and shall not be open for inspection by members of the public. Upon an order of the issuing judge, the contents of any wire, oral, or electronic communication may be unsealed and used while giving testimony, pursuant to the provisions under § 40-6-306(c). The presence of the seal provided for by this subsection (f), or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral or electronic communication or evidence derived therefrom under § 40-6-306(c). All wire, oral, or electronic communications that are not disclosed while giving testimony retain their confidential character and shall not be open for inspection by members of the public. Immediately following duplication or use while giving testimony, the recordings shall be returned to the judge issuing the order and resealed under the judge's direction. (2) Applications made and orders granted under this section shall be treated as confidential and shall not be open for inspection by members of the public. Applications and orders shall be sealed by the judge and custody shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge and in any event shall be kept for ten (10) years. Upon the agreement of the person named in the order or application, or such person's counsel, and the appropriate district attorney general, the issuing judge may order the destruction of all such applications and orders at any time. (3) Any violation of the provisions of this subsection (f) may be punished as contempt of the issuing or denying judge. (4) Within a reasonable time, but not later than ninety (90) days after the termination of an order of approval under (c) and (d), or an order authorizing an extension under subsection (e), or the denial of an order under subsection (c), the issuing or denying judge shall cause to be served on the persons named in the order or application and such other parties to intercepted communications as the judge may determine in the judge's discretion that is in the interest of justice, an inventory which shall include notice of: (A) The fact of entry of the order or the application; (B) The date of the entry and the period of authorized interception, or the denial of the application; and (C) The fact that during the period wire, oral, or electronic communications were or were not intercepted. The judge, upon the filing of a motion, may, in the judge's discretion, make available to such person or the person's counsel for inspection such portions of the intercepted communications, applications, and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction, the serving of the inventory required by this subsection (f) may be postponed for ninety (90) days. At the end of this period, the judge may allow additional ninety-day extensions, but only on further showing of good cause. (g) The contents of any intercepted wire, oral, or electronic

	communication or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a state court unless each party, not less than ten (10) days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized. This ten-day period may be waived by the judge if the judge finds that it was not possible to furnish the party with such information ten (10) days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information. (h)(1) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the state of Tennessee or a political subdivision of the state may move to suppress the contents of any intercepted wire, oral, or electronic communication, or evidence derived therefrom, on the grounds that: (A) The communication was unlawfully intercepted; (B) The order of authorization under which it was intercepted is insufficient on its face; or (C) The interception was not made in conformity with the order of authorization. Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire, oral or electronic communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this part or §§ 39-13-601 — 39-13-603. The judge, upon the filing of such motion by the aggrieved person, may in the judge's discretion make available such portions of the intercepted communication, or evidence derived therefrom, as the judge determines to be in the interest of justice. (2) In addition to any other right to appeal, the state has the right to appeal from an order granting a motion to suppress made under subdivision (h)(1), or the denial of an application for an order of approval, if the district attorney general certifies to the judge or other official granting the motion or denying the application that the appeal is not taken for purposes of delay. The appeal shall be taken within thirty (30) days after the date the order was entered and shall be diligently prosecuted.
Texas	**16.02 PENAL Unlawful Interception, Use, or Disclosure of Wire, Oral, or Electronic Communications** (a) In this section, "computer trespasser," "covert entry," "communication common carrier," "contents," "electronic communication," "electronic, mechanical, or other device," "immediate life-threatening situation," "intercept," "investigative or law enforcement officer," "member of a law enforcement unit specially trained to respond to and deal with life-threatening situations," "oral communication," "protected computer," "readily accessible to the general public," and "wire communication" have the meanings given those terms in Article 18.20, Code of Criminal Procedure. (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 electronic, mechanical, or other 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 Article 18.20, 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) 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 electronic, mechanical, or other 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 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 electronic, mechanical, or other 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 electronic, mechanical, or other 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 electronic, mechanical, or other 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 provider acting in the normal course of the provider's or communication 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. (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. **18.20 CODE CRIM. P. Interception and use of wire, oral, or electronic communications Definitions** Sec. 1. In this article: (1) "Wire communication" means an aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception, including the use of such a connection in a switching station, furnished or operated by a person authorized to engage in providing or operating the facilities for the transmission of communications as a communications common carrier. The term includes the electronic storage of a wire communication. (2) "Oral communication" means an oral communication uttered by a person exhibiting an expectation that the communication is not subject to interception under circumstances justifying that expectation. The term does not include an electronic communication. (3) "Intercept" means the aural or other acquisition of the contents of a wire, oral, or electronic communication through the use of an electronic, mechanical, or other device. (4) "Electronic, mechanical, or other device" means a device that may be used for the nonconsensual interception of wire, oral, or electronic communications. The term does not include a telephone or telegraph instrument, the equipment or a facility used for the transmission of electronic communications, or a component of the equipment or a facility used for the transmission of electronic communications if the instrument, equipment, facility, or component is: (A) furnished to the subscriber or user by a provider of wire or electronic communications service in the ordinary course of the provider's business and being used by the subscriber or user in the ordinary course of its business; (B) furnished by a subscriber or user for connection to the facilities of a wire or electronic communications service for use in the ordinary course of the subscriber's or user's business; (C) being used by a communications common carrier in the ordinary course of its business; or (D) being used by an investigative or law enforcement officer in the ordinary course of the officer's duties. (5) "Investigative or law enforcement officer" means an officer of this state or of a political subdivision of this state who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in Section 4 of this article or an attorney authorized by law to prosecute or participate in the prosecution of the enumerated offenses. (6) "Contents," when used with respect to a wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. (7) "Judge of competent jurisdiction" means a judge from the panel of nine active district judges with criminal jurisdiction appointed by the presiding judge of the court of criminal appeals as provided by Section 3 of this article. (8) "Prosecutor" means a district attorney, criminal district attorney, or county attorney performing the duties of a district attorney, with jurisdiction in the county within an administrative judicial district described by Section 3(b). (9) "Director" means the director of the Department of Public Safety or, if the director is absent or unable to serve, the assistant director of the Department of Public Safety. (10) "Communication common carrier" means a person engaged as a common carrier for hire in the transmission of wire or electronic communications. (11) "Aggrieved person" means a person who was a party to an intercepted wire, oral, or electronic communication or a person against whom the interception was directed. (12) "Covert entry" means any entry into or onto premises which if made without a court order allowing such an entry under this Act, would be a violation of the Penal Code. (13) "Residence" means a structure or the portion of a structure used as a person's home or fixed place of habitation to which the person indicates an intent to return after any temporary absence. (14) "Pen register," "ESN reader," "trap and trace device," and "mobile tracking device" have the meanings assigned by Article 18.21. (15) "Electronic communication" means a transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-

	optical system. The term does not include: (A) a wire or oral communication; (B) a communication made through a tone-only paging device; or (C) a communication from a tracking device. (16) "User" means a person who uses an electronic communications service and is authorized by the provider of the service to use the service. (17) "Electronic communications system" means a wire, radio, electromagnetic, photo-optical or photoelectronic facility for the transmission of wire or electronic communications, and any computer facility or related electronic equipment for the electronic storage of those communications. (18) "Electronic communications service" means a service that provides to users of the service the ability to send or receive wire or electronic communications. (19) "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. (20) "Electronic storage" means: (A) a temporary, intermediate storage of a wire or electronic communication that is incidental to the electronic transmission of the communication; or (B) storage of a wire or electronic communication by an electronic communications service for purposes of backup protection of the communication. (21) "Aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception. (22) "Immediate life-threatening situation" means a hostage, barricade, or other emergency situation in which a person unlawfully and directly: (A) threatens another with death; or (B) exposes another to a substantial risk of serious bodily injury. (23) "Member of a law enforcement unit specially trained to respond to and deal with life-threatening situations" means a peace officer who, as evidenced by the submission of appropriate documentation to the Commission on Law Enforcement Officer Standards and Education: (A) receives a minimum of 40 hours a year of training in hostage and barricade suspect situations; or (B) has received a minimum of 24 hours of training on kidnapping investigations and is: (i) the sheriff of a county with a population of 3.3 million or more or the sheriff's designee; or (ii) the police chief of a police department in a municipality with a population of 500,000 or more or the police chief's designee. (24) "Access," "computer," "computer network," "computer system," and "effective consent" have the meanings assigned by Section 33.01, Penal Code. (25) "Computer trespasser" means a person who: (A) is accessing a protected computer without effective consent of the owner; and (B) has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer. The term does not include a person who accesses the computer under an existing contractual relationship with the owner or operator of the protected computer. (26) "Protected computer" means a computer, computer network, or computer system that is: (A) owned by a financial institution or governmental entity; or (B) used by or for a financial institution or governmental entity and conduct constituting an offense affects that use. **Prohibition of Use as Evidence of Intercepted Communications** Sec. 2. (a) The contents of an intercepted communication and evidence derived from an intercepted communication may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States or of this state or a political subdivision of this state unless: (1) the communication was intercepted in violation of this article, Section 16.02, Penal Code, or federal law; or (2) the disclosure of the contents of the intercepted communication or evidence derived from the communication would be in violation of this article, Section 16.02, Penal Code, or federal law. (b) The contents of an intercepted communication and evidence derived from an intercepted communication may be received in a civil trial, hearing, or other proceeding only if the civil trial, hearing, or other proceeding arises out of a violation of a penal law. (c) This section does not prohibit the use or admissibility of the contents of a communication or evidence derived from the communication if the communication was intercepted in a jurisdiction outside this state in compliance with the law of that jurisdiction. **Judges Authorized to Consider Interception Applications** Sec. 3. (a) The presiding judge of the court of criminal appeals, by order filed with the clerk of that court, shall appoint one district judge from each of the administrative judicial districts of this state to serve at

	his pleasure as the judge of competent jurisdiction within that administrative judicial district. The presiding judge shall fill vacancies, as they occur, in the same manner. (b) Except as provided by Subsection (c), a judge appointed under Subsection (a) may act on an application for authorization to intercept wire, oral, or electronic communications if the judge is appointed as the judge of competent jurisdiction within the administrative judicial district in which the following is located: (1) the site of: (A) the proposed interception; or (B) the interception device to be installed or monitored; (2) the communication device to be intercepted; (3) the billing, residential, or business address of the subscriber to the electronic communications service to be intercepted; (4) the headquarters of the law enforcement agency that makes a request for or executes an order authorizing an interception; or (5) the headquarters of the service provider. (c) If the judge of competent jurisdiction for an administrative judicial district is absent or unable to serve or if exigent circumstances exist, the application may be made to the judge of competent jurisdiction in an adjacent administrative judicial district. Exigent circumstances does not include a denial of a previous application on the same facts and circumstances. To be valid, the application must fully explain the circumstances justifying application under this subsection. **Offenses for which Interceptions may be Authorized** Sec. 4. A judge of competent jurisdiction may issue an order authorizing interception of wire, oral, or electronic communications only if the prosecutor applying for the order shows probable cause to believe that the interception will provide evidence of the commission of: (1) a felony under Section 19.02, 19.03, or 43.26, Penal Code; (2) a felony under: (A) Chapter 481, Health and Safety Code, other than felony possession of marihuana; (B) Section 485.033, Health and Safety Code; or (C) Chapter 483, Health and Safety Code; (3) an offense under Section 20.03 or 20.04, Penal Code; (4) an offense under Chapter 20A, Penal Code; (5) an offense under Chapter 34, Penal Code, if the criminal activity giving rise to the proceeds involves the commission of an offense under Title 5, Penal Code, or an offense under federal law or the laws of another state containing elements that are substantially similar to the elements of an offense under Title 5; or (6) an attempt, conspiracy, or solicitation to commit an offense listed in this section. **Control of Intercepting Devices** Sec. 5. (a) Except as provided by Section 8A, only the Department of Public Safety is authorized by this article to own, possess, install, operate, or monitor an electronic, mechanical, or other device. The Department of Public Safety may be assisted by an investigative or law enforcement officer or other person in the operation and monitoring of an interception of wire, oral, or electronic communications, provided that the officer or other person: (1) is designated by the director for that purpose; and (2) acts in the presence and under the direction of a commissioned officer of the Department of Public Safety. (b) The director shall designate in writing the commissioned officers of the Department of Public Safety who are responsible for the possession, installation, operation, and monitoring of electronic, mechanical, or other devices for the department. **Request for Application for Interception** Sec. 6. (a) The director may, based on written affidavits, request in writing that a prosecutor apply for an order authorizing interception of wire, oral, or electronic communications. (b) The head of a local law enforcement agency or, if the head of the local law enforcement agency is absent or unable to serve, the acting head of the local law enforcement agency may, based on written affidavits, request in writing that a prosecutor apply for an order authorizing interception of wire, oral, or electronic communications. Prior to the requesting of an application under this subsection, the head of a local law enforcement agency must submit the request and supporting affidavits to the director, who shall make a finding in writing whether the request and supporting affidavits establish that other investigative procedures have been tried and failed or they reasonably appear unlikely to succeed or to be too dangerous if tried, is feasible, is justifiable, and whether the Department of Public Safety has the necessary resources available. The prosecutor may file the application only after a written positive finding on all the above requirements by the director. **Authorization for Disclosure and Use of Intercepted Communications** Sec. 7. (a) An investigative or law enforcement officer who, by any means authorized by this article, obtains knowledge of the contents of a wire, oral, or electronic communication or evidence derived from the communication may disclose the contents or evidence to another investigative or law enforcement officer, including a federal law enforcement officer or agent or a law enforcement officer or agent of another state, to the extent that the disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure. (b) An investigative or law enforcement officer who, by any means authorized by this article, obtains knowledge of the contents of a wire, oral, or electronic communication or evidence derived from the communication may use the contents or evidence to the extent the use is appropriate to the proper

	performance of his official duties. (c) A person who receives, by any means authorized by this article, information concerning a wire, oral, or electronic communication or evidence derived from a communication intercepted in accordance with the provisions of this article may disclose the contents of that communication or the derivative evidence while giving testimony under oath in any proceeding held under the authority of the United States, of this state, or of a political subdivision of this state. (d) An otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this article does not lose its privileged character and any evidence derived from such privileged communication against the party to the privileged communication shall be considered privileged also. (e) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in a manner authorized by this article, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization, the contents of and evidence derived from the communication may be disclosed or used as provided by Subsections (a) and (b) of this section. Such contents and any evidence derived therefrom may be used under Subsection (c) of this section when authorized by a judge of competent jurisdiction where the judge finds, on subsequent application, that the contents were otherwise intercepted in accordance with the provisions of this article. The application shall be made as soon as practicable. **Application for Interception Authorization** Sec. 8. (a) To be valid, an application for an order authorizing the interception of a wire, oral, or electronic communication must be made in writing under oath to a judge of competent jurisdiction and must state the applicant's authority to make the application. An applicant must include the following information in the application: (1) the identity of the prosecutor making the application and of the officer requesting the application; (2) a full and complete statement of the facts and circumstances relied on by the applicant to justify his belief that an order should be issued, including: (A) details about the particular offense that has been, is being, or is about to be committed; (B) a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted; (C) a particular description of the type of communication sought to be intercepted; and (D) the identity of the person, if known, committing the offense and whose communications are to be intercepted; (3) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed or to be too dangerous if tried; (4) a statement of the period of time for which the interception is required to be maintained and, if the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication is first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur after the described type of communication is obtained; (5) a statement whether a covert entry will be necessary to properly and safely install the wiretapping or electronic surveillance or eavesdropping equipment and, if a covert entry is requested, a statement as to why such an entry is necessary and proper under the facts of the particular investigation, including a full and complete statement as to whether other investigative techniques have been tried and have failed or why they reasonably appear to be unlikely to succeed or to be too dangerous if tried or are not feasible under the circumstances or exigencies of time; (6) a full and complete statement of the facts concerning all applications known to the prosecutor making the application that have been previously made to a judge for authorization to intercept wire, oral, or electronic communications involving any of the persons, facilities, or places specified in the application and of the action taken by the judge on each application; and (7) if the application is for the extension of an order, a statement setting forth the results already obtained from the interception or a reasonable explanation of the failure to obtain results. (b) The judge may, in an ex parte hearing in chambers, require additional testimony or documentary evidence in support of the application, and such testimony or documentary evidence shall be preserved as part of the application. **Emergency Installation and Use of Intercepting Device** Sec. 8A. (a) The prosecutor in a county in which an electronic, mechanical, or other device is to be installed or used to intercept wire, oral, or electronic communications shall designate in writing each peace officer in the county, other than a commissioned officer of the Department of Public Safety, who: (1) is a member of a law enforcement unit specially trained to respond to and deal with life-threatening situations; and (2) is authorized to possess such a device and responsible for the installation, operation, and monitoring of the device in an immediate life-threatening situation. (b) A peace officer designated under Subsection (a) or under Section 5(b) may possess, install, operate, or monitor an electronic, mechanical, or other device to intercept wire, oral, or electronic communications if the officer: (1) reasonably believes an immediate life-threatening

	situation exists that: (A) is within the territorial jurisdiction of the officer or another officer the officer is assisting; and (B) requires interception of communications before an order authorizing the interception can, with due diligence, be obtained under this section; (2) reasonably believes there are sufficient grounds under this section on which to obtain an order authorizing the interception; and (3) obtains oral or written consent to the interception before beginning the interception from: (A) a district judge for the county in which the device will be installed or used; or (B) a judge or justice of a court of appeals or of a higher court. (c) An official described in Subsection (b)(3) may give oral or written consent to the interception of communications under this section to provide evidence of the commission of a felony, or of a threat, attempt, or conspiracy to commit a felony, in an immediate life-threatening situation. Oral or written consent given under this section expires 48 hours after the grant of consent or at the conclusion of the emergency justifying the interception, whichever occurs first. (d) If an officer installs or uses a device under Subsection (b), the officer shall: (1) promptly report the installation or use to the prosecutor in the county in which the device is installed or used; and (2) within 48 hours after the installation is complete or the interception begins, whichever occurs first, obtain a written order from a judge of competent jurisdiction authorizing the interception. (e) A judge of competent jurisdiction under Section 3 or under Subsection (b) may issue a written order authorizing interception of communications under this section during the 48-hour period prescribed by Subsection (d)(2). A written order under this section expires on the 30th day after execution of the order or at the conclusion of the emergency that initially justified the interception, whichever occurs first. If an order is denied or is not issued within the 48-hour period, the officer shall terminate use of and remove the device promptly on the earlier of: (1) the denial; (2) the end of the emergency that initially justified the interception; or (3) the expiration of 48 hours. (f) The state may not use as evidence in a criminal proceeding any information gained through the use of a device installed under this section if authorization for the device is not sought or is sought but not obtained. (g) A peace officer may certify to a communications common carrier that the officer is acting lawfully under this section. **Action on Application for Interception Order** Sec. 9. (a) On receipt of an application, the judge may enter an ex parte order, as requested or as modified, authorizing interception of wire, oral, or electronic communications if the judge determines from the evidence submitted by the applicant that: (1) there is probable cause to believe that a person is committing, has committed, or is about to commit a particular offense enumerated in Section 4 of this article; (2) there is probable cause to believe that particular communications concerning that offense will be obtained through the interception; (3) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed or to be too dangerous if tried; (4) there is probable cause to believe that the facilities from which or the place where the wire, oral, or electronic communications are to be intercepted are being used or are about to be used in connection with the commission of an offense or are leased to, listed in the name of, or commonly used by the person; and (5) a covert entry is or is not necessary to properly and safely install the wiretapping or electronic surveillance or eavesdropping equipment. (b) An order authorizing the interception of a wire, oral, or electronic communication must specify: (1) the identity of the person, if known, whose communications are to be intercepted; (2) the nature and location of the communications facilities as to which or the place where authority to intercept is granted; (3) a particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates; (4) the identity of the officer making the request and the identity of the prosecutor; (5) the time during which the interception is authorized, including a statement of whether or not the interception will automatically terminate when the described communication is first obtained; and (6) whether or not a covert entry or surreptitious entry is necessary to properly and safely install wiretapping, electronic surveillance, or eavesdropping equipment. (c) On request of the applicant for an order authorizing the interception of a wire, oral, or electronic communication, the judge may issue a separate order directing that a provider of wire or electronic communications service, a communication common carrier, landlord, custodian, or other person furnish the applicant all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that the provider, carrier, landlord, custodian, or other person is providing the person whose communications are to be intercepted. Any provider of wire or electronic communications service, communication common carrier, landlord, custodian, or other person furnishing facilities or technical assistance is entitled to compensation by the applicant for reasonable expenses incurred in providing the facilities or assistance at the prevailing rates. The interception order may include an order to: (1)

	install or use a pen register, ESN reader, trap and trace device, or mobile tracking device, or similar equipment that combines the function of a pen register and trap and trace device; (2) disclose a stored communication, information subject to an administrative subpoena, or information subject to access under Article 18.21, Code of Criminal Procedure. (d) An order entered pursuant to this section may not authorize the interception of a wire, oral, or electronic communication for longer than is necessary to achieve the objective of the authorization and in no event may it authorize interception for more than 30 days. The issuing judge may grant extensions of an order, but only on application for an extension made in accordance with Section 8 and the court making the findings required by Subsection (a). The period of extension may not be longer than the authorizing judge deems necessary to achieve the purposes for which it is granted and in no event may the extension be for more than 30 days. To be valid, each order and extension of an order must provide that the authorization to intercept be executed as soon as practicable, be conducted in a way that minimizes the interception of communications not otherwise subject to interception under this article, and terminate on obtaining the authorized objective or within 30 days, whichever occurs sooner. If the intercepted communication is in code or a foreign language and an expert in that code or language is not reasonably available during the period of interception, minimization may be accomplished as soon as practicable after the interception. (e) An order entered pursuant to this section may not authorize a covert entry into a residence solely for the purpose of intercepting a wire or electronic communication. (f) An order entered pursuant to this section may not authorize a covert entry into or onto a premises for the purpose of intercepting an oral communication unless: (1) the judge, in addition to making the determinations required under Subsection (a) of this section, determines that: (A)(i) the premises into or onto which the covert entry is authorized or the person whose communications are to be obtained has been the subject of a pen register previously authorized in connection with the same investigation; (ii) the premises into or onto which the covert entry is authorized or the person whose communications are to be obtained has been the subject of an interception of wire or electronic communications previously authorized in connection with the same investigation; and (iii) that such procedures have failed; or (B) that the procedures enumerated in Paragraph (A) reasonably appear to be unlikely to succeed or to be too dangerous if tried or are not feasible under the circumstances or exigencies of time; and (2) the order, in addition to the matters required to be specified under Subsection (b) of this section, specifies that the covert entry is for the purpose of intercepting oral communications of two or more persons and that there is probable cause to believe they are committing, have committed, or are about to commit a particular offense enumerated in Section 4 of this article. (g) Whenever an order authorizing interception is entered pursuant to this article, the order may require reports to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Reports shall be made at any interval the judge requires. (h) A judge who issues an order authorizing the interception of a wire, oral, or electronic communication may not hear a criminal prosecution in which evidence derived from the interception may be used or in which the order may be an issue. **Procedure for Preserving Intercepted Communications** Sec. 10. (a) The contents of a wire, oral, or electronic communication intercepted by means authorized by this article shall be recorded on tape, wire, or other comparable device. The recording of the contents of a wire, oral, or electronic communication under this subsection shall be done in a way that protects the recording from editing or other alterations. (b) Immediately on the expiration of the period of the order and all extensions, if any, the recordings shall be made available to the judge issuing the order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. The recordings may not be destroyed until at least 10 years after the date of expiration of the order and the last extension, if any. A recording may be destroyed only by order of the judge of competent jurisdiction for the administrative judicial district in which the interception was authorized. (c) Duplicate recordings may be made for use or disclosure pursuant to Subsections (a) and (b), Section 7, of this article for investigations. (d) The presence of the seal required by Subsection (b) of this section or a satisfactory explanation of its absence is a prerequisite for the use or disclosure of the contents of a wire, oral, or electronic communication or evidence derived from the communication under Subsection (c), Section 7, of this article. **Sealing of Orders and Applications** Sec. 11. The judge shall seal each application made and order granted under this article. Custody of the applications and orders shall be wherever the judge directs. An application or order may be disclosed only on a showing of good cause before a judge of competent jurisdiction and may not be destroyed until at least 10 years after the date it is sealed. An application or order may be destroyed

	only by order of the judge of competent jurisdiction for the administrative judicial district in which it was made or granted. **Contempt** Sec. 12. A violation of Section 10 or 11 of this article may be punished as contempt of court. **Notice and Disclosure of Interception to a Party** Sec. 13. (a) Within a reasonable time but not later than 90 days after the date an application for an order is denied or after the date an order or the last extension, if any, expires, the judge who granted or denied the application shall cause to be served on the persons named in the order or the application and any other parties to intercepted communications, if any, an inventory, which must include notice: (1) of the entry of the order or the application; (2) of the date of the entry and the period of authorized interception or the date of denial of the application; and (3) that during the authorized period wire, oral, or electronic communications were or were not intercepted. (b) The judge, on motion, may in his discretion make available to a person or his counsel for inspection any portion of an intercepted communication, application, or order that the judge determines, in the interest of justice, to disclose to that person. (c) On an ex parte showing of good cause to the judge, the serving of the inventory required by this section may be postponed, but in no event may any evidence derived from an order under this article be disclosed in any trial, until after such inventory has been served. **Preconditions to Use as Evidence** Sec. 14. (a) The contents of an intercepted wire, oral, or electronic communication or evidence derived from the communication may not be received in evidence or otherwise disclosed in a trial, hearing, or other proceeding in a federal or state court unless each party, not later than the 10th day before the date of the trial, hearing, or other proceeding, has been furnished with a copy of the court order and application under which the interception was authorized or approved. This 10-day period may be waived by the judge if he finds that it is not possible to furnish the party with the information 10 days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving the information. (b) An aggrieved person charged with an offense in a trial, hearing, or proceeding in or before a court, department, officer, agency, regulatory body, or other authority of the United States or of this state or a political subdivision of this state may move to suppress the contents of an intercepted wire, oral, or electronic communication or evidence derived from the communication on the ground that: (1) the communication was unlawfully intercepted; (2) the order authorizing the interception is insufficient on its face; or (3) the interception was not made in conformity with the order. (c) A person identified by a party to an intercepted wire, oral, or electronic communication during the course of that communication may move to suppress the contents of the communication on the grounds provided in Subsection (b) of this section or on the ground that the harm to the person resulting from his identification in court exceeds the value to the prosecution of the disclosure of the contents. (d) The motion to suppress must be made before the trial, hearing, or proceeding unless there was no opportunity to make the motion or the person was not aware of the grounds of the motion. The hearing on the motion shall be held in camera upon the written request of the aggrieved person. If the motion is granted, the contents of the intercepted wire, oral, or electronic communication and evidence derived from the communication shall be treated as having been obtained in violation of this article. The judge, on the filing of the motion by the aggrieved person, shall make available to the aggrieved person or his counsel for inspection any portion of the intercepted communication or evidence derived from the communication that the judge determines, in the interest of justice, to make available. (e) Any judge of this state, upon hearing a pretrial motion regarding conversations intercepted by wire pursuant to this article, or who otherwise becomes informed that there exists on such intercepted wire, oral, or electronic communication identification of a specific individual who is not a party or suspect to the subject of interception: (1) shall give notice and an opportunity to be heard on the matter of suppression of references to that person if identification is sufficient so as to give notice; or (2) shall suppress references to that person if identification is sufficient to potentially cause embarrassment or harm which outweighs the probative value, if any, of the mention of such person, but insufficient to require the notice provided for in Subdivision (1), above. **Reports concerning intercepted wire, oral, or electronic communications** Sec. 15. (a) Within 30 days after the date an order or the last extension, if any, expires or after the denial of an order, the issuing or denying judge shall report to the Administrative Office of the United States Courts: (1) the: fact that an order or extension was applied for; (2) the kind of order or extension applied for; (3) the fact that the order or extension was granted as applied for, was modified, or was denied; (4) the period of interceptions authorized by the order and the number and duration of any extensions of the order; (5) the offense specified in the order or application or extension; (6) the identity of the officer making the request and the prosecutor; and (7) the nature of the facilities from

	which or the place where communications were to be intercepted. (b) In January of each year each prosecutor shall report to the Administrative Office of the United Slates Courts the following information for the preceding calendar year: (1) the information required by Subsection (a) of this section with respect to each application for an order or extension made; (2) a general description of the interceptions made under each order or extension, including the approximate nature and frequency of incriminating communications intercepted, the approximate nature and frequency of other communications intercepted, the approximate number of persons whose communications were intercepted, and the approximate nature, amount, and cost of the manpower and other resources used in the interceptions; (3) the number of arrests resulting from interceptions made under each order or extension and the offenses for which arrests were made; (4) the number of trials resulting from interceptions; (5) the number of motions to suppress made with respect to interceptions and the number granted or denied; (6) the number of convictions resulting from interceptions, the offenses for which the convictions were obtained, and a general assessment of the importance of the interceptions; and (7) the information required by Subdivisions (2) through (6) of this subsection with respect to orders or extensions obtained. (c) Any judge or prosecutor required to file a report with the Administrative Office of the United States Courts shall forward a copy of such report to the director of the Department of Public Safety. On or before March 1 of each year, the director shall submit to the governor; lieutenant governor; speaker of the house of representatives; chairman, senate jurisprudence committee; and chairman, house of representatives criminal jurisprudence committee a report of all intercepts as defined herein conducted pursuant to this article and terminated during the preceding calendar year. Such report shall include: (1) the reports of judges and prosecuting attorneys forwarded to the director as required in this section; (2) the number of Department of Public Safety personnel authorized to possess, install, or operate electronic, mechanical, or other devices; (3) the number of Department of Public Safety and other law enforcement personnel who participated or engaged in the seizure of intercepts pursuant to this article during the preceding calendar year; and (4) the total cost to the Department of Public Safety of all activities and procedures relating to the seizure of intercepts during the preceding calendar year, including costs of equipment, manpower, and expenses incurred as compensation for use of facilities or technical assistance provided to the department. **Recovery of Civil Damages Authorized** Sec. 16. (a) A person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of this article, or in violation of Chapter 16, Penal Code, has a civil cause of action against any person who intercepts, discloses, or uses or solicits another person to intercept, disclose, or use the communication and is entitled to recover from the person: (1) actual damages but not less than liquidated damages computed at a rate of $100 a day for each day of violation or $1,000, whichever is higher; (2) punitive damages; and (3) a reasonable attorney's fee and other litigation costs reasonably incurred. (b) A good faith reliance on a court order or legislative authorization constitutes a complete defense to an action brought under this section. (c) A person is subject to suit by the federal or state government in a court of competent jurisdiction for appropriate injunctive relief if the person engages in conduct that: (1) constitutes an offense under Section 16.05, Penal Code, but is not for a tortious or illegal purpose or for the purpose of direct or indirect commercial advantage or private commercial gain; and (2) involves a radio communication that is: (A) transmitted on frequencies allocated under Subpart D of Part 74 of the rules of the Federal Communications Commission; and (B) not scrambled or encrypted. (d) A defendant is liable for a civil penalty of $500 if it is shown at the trial of the civil suit brought under Subsection (c) that the defendant: (1) has been convicted of an offense under Section 16.05, Penal Code; or (2) is found liable in a civil action brought under Subsection (a). (e) Each violation of an injunction ordered under Subsection (c) is punishable by a fine of $500. (f) The attorney general, or the county or district attorney of the county in which the conduct, as described by Subsection (c), is occurring, may file suit under Subsection (c) on behalf of the state. (g) A computer trespasser or a user, aggrieved person, subscriber, or customer of a communications common carrier or electronic communications service does not have a cause of action against the carrier or service, its officers, employees, or agents, or other specified persons for providing information, facilities, or assistance as required by a good faith reliance on: (1) legislative authority; or (2) a court order, warrant, subpoena, or certification under this article. **Nonapplicability** Sec. 17. This article does not apply to conduct described as an affirmative defense under Section 16.02(c), Penal Code. Sec. 18. Repealed by Acts 2005, 79th Leg., ch. 889, § 2.
Utah	**76-9-402. Privacy violation.** (1) A person is guilty of privacy violation if, except as authorized by

	law, he: (a) Trespasses on property with intent to subject anyone to eavesdropping or other surveillance in a private place; or (b) Installs in any private place, without the consent of the person or persons entitled to privacy there, any device for observing, photographing, recording, amplifying, or broadcasting sounds or events in the place or uses any such unauthorized installation; or (c) Installs or uses outside of a private place any device for hearing, recording, amplifying, or broadcasting sounds originating in the place which would not ordinarily be audible or comprehensible outside, without the consent of the person or persons entitled to privacy there. (2) Privacy violation is a class B misdemeanor. **76-9-403. Communication Abuse.** (1) A person commits communication abuse if, except as authorized by law, he: (a) Intercepts, without the consent of the sender or receiver, a message by telephone, telegraph, letter, or other means of communicating privately; this paragraph does not extend to: (i) Overhearing of messages through a regularly installed instrument on a telephone party line or on an extension; or (ii) Interception by the telephone company or subscriber incident to enforcement of regulations limiting use of the facilities or to other normal operation and use; or (b) Divulges without consent of the sender or receiver the existence or contents of any such message if the actor knows that the message was illegally intercepted or if he learned of the message in the course of employment with an agency engaged in transmitting it. (2) Communication abuse is a class B misdemeanor. **77-23a-4. Offenses — Criminal and civil — Lawful interception.** (1)(a) Except as otherwise specifically provided in this chapter, any person who violates Subsection (1)(b) is guilty of an offense and is subject to punishment under Subsection (10), or when applicable, the person is subject to civil action under Subsection (11). (b) A person commits a violation of this subsection who: (i) intentionally or knowingly intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic, or oral communication; (ii) intentionally or knowingly uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication, when the device is affixed to, or otherwise transmits a signal through a wire, cable, or other like connection used in wire communication or when the device transmits communications by radio, or interferes with the transmission of the communication; (iii) intentionally or knowingly discloses or endeavors to disclose to any other person the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this section; or (iv) intentionally or knowingly uses or endeavors to use the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this section. (2) The operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service whose facilities are used in the transmission of a wire communication may intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service. However, a provider of wire communications service to the public may not utilize service observing or random monitoring except for mechanical or service quality control checks. (3)(a) Providers of wire or electronic communications service, their officers, employees, or agents, and any landlords, custodians, or other persons may provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance if the provider and its officers, employees, or agents, and any landlords, custodians, or other specified persons have been provided with: (i) a court order directing the assistance signed by the authorizing judge; or (ii) a certification in writing by a person specified in Subsection 77-23a-10 (7), or by the attorney general or an assistant attorney general, or by a county attorney or district attorney or his deputy that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required. (b) The order or certification under this subsection shall set the period of time during which the provision of the information, facilities, or technical assistance is authorized and shall specify the information, facilities, or technical assistance required. (4)(a) The providers of wire or electronic communications service, their officers, employees, or agents, and any landlords, custodians, or other specified persons may not disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance regarding which the person has been

	furnished an order or certification under this section except as is otherwise required by legal process, and then only after prior notification to the attorney general or to the county attorney or district attorney of the county in which the interception was conducted, as is appropriate. (b) Any disclosure in violation of this subsection renders the person liable for civil damages under Section 77-23a-11. (5) A cause of action does not lie in any court against any provider of wire or electronic communications service, its officers, employees, or agents, or any landlords, custodians, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter. (6) Subsections (3), (4), and (5) supersede any law to the contrary. (7)(a) A person acting under color of law may intercept a wire, electronic, or oral communication if that person is a party to the communication or one of the parties to the communication has given prior consent to the interception. (b) A person not acting under color of law may intercept a wire, electronic, or oral communication if that person is a party to the communication or one of the parties to the communication has given prior consent to the interception, unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of state or federal laws. (c) An employee of a telephone company may intercept a wire communication for the sole purpose of tracing the origin of the communication when the interception is requested by the recipient of the communication and the recipient alleges that the communication is obscene, harassing, or threatening in nature. The telephone company and its officers, employees, and agents shall release the results of the interception, made under this subsection, upon request of the local law enforcement authorities. (8) A person may: (a) intercept or access an electronic communication made through an electronic communications system that is configured so that the electronic communication is readily accessible to the general public; (b) intercept any radio communication transmitted by: (i) any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (ii) any government, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (iii) a station operating on an authorized frequency within the bands allocated to the amateur, citizens' band, or general mobile radio services; or (iv) by a marine or aeronautics communications system; (c) intercept any wire or electronic communication, the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of the interference; or (d) as one of a group of users of the same frequency, intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of the system, if the communication is not scrambled or encrypted. (9)(a) Except under Subsection (b), a person or entity providing an electronic communications service to the public may not intentionally divulge the contents of any communication, while in transmission of that service, to any person or entity other than an addressee or intended recipient of the communication or his agent. (b) A person or entity providing electronic communications service to the public may divulge the contents of any communication: (i) as otherwise authorized under this section or Section 77-23a-9; (ii) with lawful consent of the originator or any addressee or intended recipient of the communication; (iii) to a person employed or authorized or whose facilities are used to forward the communication to its destination; or (iv) that is inadvertently obtained by the service provider and appears to pertain to the commission of a crime, if the divulgence is made to a law enforcement agency. (10) (a) Except under Subsection (b) or Subsection (11), a violation of Subsection (1) is a third degree felony. (b) If the offense is a first offense under this section and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication regarding which the offense was committed is a radio communication that is not scrambled or encrypted: (i) if the communication is not the radio portion of a cellular telephone communication, a public land mobile radio service communication, or paging service communication, and the conduct is not under Subsection (11), the offense is a class A misdemeanor; and (ii) if the communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication, or a paging service communication, the offense is a class B misdemeanor. (c) Conduct otherwise an offense under this section is not an offense if the conduct was not done for the purpose of direct or indirect commercial advantage or private financial gain, and consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled, and is either transmitted: (i) to a broadcasting station for purposes of retransmission to the general public; or (ii) as an audio subcarrier intended for redistribution to facilities open to the public, but in any event not including data transmissions or

	telephone calls. (11) (a) A person is subject to civil suit initiated by the state in a court of competent jurisdiction when his conduct is prohibited under Subsection (1) and the conduct involves a: (i) private satellite video communication that is not scrambled or encrypted, and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or (ii) radio communication that is transmitted on frequencies allocated under Subpart D, Part 74, Rules of the Federal Communication Commission, that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain. (b) In an action under Subsection (a): (i) if the violation of this chapter is a first offense under this section and the person is not found liable in a civil action under Section 77-23a-11, the state may seek appropriate injunctive relief; (ii) if the violation of this chapter is a second or subsequent offense under this section, or the person has been found liable in any prior civil action under Section 77-23a-11, the person is subject to a mandatory $500 civil penalty. (c) The court may use any means within its authority to enforce an injunction issued under Subsection (b)(i), and shall impose a civil fine of not less than $500 for each violation of the injunction.
Vermont	Vermont does not have a wiretapping and eavesdropping law.
Virginia	**19.2-62. Interception, disclosure, etc., of wire, electronic or oral communications unlawful; penalties; exceptions.** A. Except as otherwise specifically provided in this chapter any person who: 1. Intentionally intercepts, endeavors to intercept or procures any other person to intercept or endeavor to intercept, any wire, electronic or oral communication; 2. Intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical or other device to intercept any oral communication; 3. Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, electronic or oral communication knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or 4. Intentionally uses, or endeavors to use, the contents of any wire, electronic or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; shall be guilty of a Class 6 felony. B. 1. It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee or agent of a provider of wire or electronic communications service, whose facilities are used in the transmission of a wire communication, to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service. However, a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks. It shall not be a criminal offense under this chapter for providers of wire or electronic communications service, their officers, employees and agents, landlords, custodians, or other persons pursuant to a court order under this chapter, to provide information facilities or technical assistance to an investigative or law-enforcement officer, who, pursuant to this chapter, is authorized to intercept a wire, electronic or oral communication. 2. It shall not be a criminal offense under this chapter for a person to intercept a wire, electronic or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception. 3. It shall not be a criminal offense under this chapter for any person: (a) To intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public; (b) To intercept any radio communication which is transmitted (i) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress, (ii) by any governmental, law-enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public, (iii) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (iv) by any marine or aeronautical communications system; (c) To intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; (d) Using the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted; (e) To use a pen register or a trap and trace device pursuant to §§ 19.2-

	70.1 and 19.2-70.2; or (f) Who is a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service. C. A person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication, other than one to such person or entity or an agent thereof, while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of the addressee or intended recipient. However, a person or entity providing electronic communication service to the public may divulge the contents of any such communication: 1. As authorized in subdivision B 1 of this section or § 19.2-67; 2. With the lawful consent of the originator or any addressee or intended recipient of such communication; 3. To a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or 4. Which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, to a law-enforcement agency. Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted (i) to a broadcasting station for purposes of retransmission to the general public, or (ii) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this section unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain. Further, private viewing of a satellite video communication that is not scrambled or encrypted and interception of a radio communication that is transmitted on frequencies allocated under subpart D of Part 74 of the Rules of the Federal Communications Commission that is not scrambled or encrypted when the viewing or interception is not done for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, shall not be offenses under this chapter. Violation of this subsection shall be punishable as a Class 1 misdemeanor. **18.2-164. Unlawful use of, or injury to, telephone and telegraph lines; copying or obstructing messages; penalty.** A. If any person commits any of the following acts, he is guilty of a Class 2 misdemeanor: 1. Maliciously injure, molest, cut down, or destroy any telephone or telegraph line, wire, cable, pole, tower, or the material or property belonging thereto; 2. Maliciously cut, break, tap, or make any connection with any telephone or telegraph line, wire, cable, or instrument of any telegraph or telephone company which has legally acquired the right-of-way by purchase, condemnation, or otherwise; 3. Maliciously copy in any unauthorized manner any message, either social, business, or otherwise, passing over any telephone or telegraph line, wire, cable, or wireless telephone transmission in the Commonwealth; 4. Willfully or maliciously prevent, obstruct, or delay by any means or contrivance whatsoever the sending, conveyance, or delivery in the Commonwealth of any authorized communication by or through any telephone or telegraph line, wire, cable, or wireless transmission device under the control of any telephone or telegraph company doing business in the Commonwealth; 5. Maliciously aid, agree with, employ, or conspire with any unauthorized person or persons unlawfully to do or cause to be done any of the acts hereinbefore mentioned. B. If any person, with the intent to prevent another person from summoning law-enforcement, fire, or rescue services: 1. Commits any act set forth in subsection A; or 2. Maliciously prevents or interferes with telephone or telegraph communication by disabling or destroying any device that enables such communication, whether wired or wireless, he is guilty of a Class 1 misdemeanor. **18.2-167.1. Interception or monitoring of customer telephone calls; penalty. —** It shall be unlawful for any person, firm or corporation to intercept or monitor, or attempt to intercept or monitor, the transmission of a message, signal or other communication by telephone between an employee or other agent of such person, firm or corporation and a customer of such person, firm or corporation. The provisions of this section shall not apply if the person, firm or corporation gives notice to such employee or agent that such monitoring may occur at any time during the course of such employment. Any person, firm or corporation violating the provisions of this section shall be guilty of a Class 4 misdemeanor. The provisions of this section shall not apply to any wiretap or other interception of any communication authorized pursuant to Chapter 6 of Title 19.2 (§ 19.2-61 et seq.).
Washington	**RCW 9.73.030** (1) Except as otherwise provided in this chapter, it shall be unlawful.... (1) Except as otherwise provided in this chapter, it shall be unlawful for any individual, partnership, corporation,

	association, or the state of Washington, its agencies, and political subdivisions to intercept, or record any: (a) Private communication transmitted by telephone, telegraph, radio, or other device between two or more individuals between points within or without the state by any device electronic or otherwise designed to record and/or transmit said communication regardless how such device is powered or actuated, without first obtaining the consent of all the participants in the communication; (b) Private conversation, by any device electronic or otherwise designed to record or transmit such conversation regardless how the device is powered or actuated without first obtaining the consent of all the persons engaged in the conversation. (2) Notwithstanding subsection (1) of this section, wire communications or conversations (a) of an emergency nature, such as the reporting of a fire, medical emergency, crime, or disaster, or (b) which convey threats of extortion, blackmail, bodily harm, or other unlawful requests or demands, or (c) which occur anonymously or repeatedly or at an extremely inconvenient hour, or (d) which relate to communications by a hostage holder or barricaded person as defined in RCW 70.85.100, whether or not conversation ensues, may be recorded with the consent of one party to the conversation. (3) Where consent by all parties is needed pursuant to this chapter, consent shall be considered obtained whenever one party has announced to all other parties engaged in the communication or conversation, in any reasonably effective manner, that such communication or conversation is about to be recorded or transmitted: PROVIDED, That if the conversation is to be recorded that said announcement shall also be recorded. (4) An employee of any regularly published newspaper, magazine, wire service, radio station, or television station acting in the course of bona fide news gathering duties on a full-time or contractual or part-time basis, shall be deemed to have consent to record and divulge communications or conversations otherwise prohibited by this chapter if the consent is expressly given or if the recording or transmitting device is readily apparent or obvious to the speakers. Withdrawal of the consent after the communication has been made shall not prohibit any such employee of a newspaper, magazine, wire service, or radio or television station from divulging the communication or conversation. **NOTES:** This section was amended by 1985 chap. 260 sec. 2 and by 1986 chap. 38 sec. 1, each without reference to the other. Both amendments are incorporated in the publication of this section under Wash. Rev. Code 1.12.025(2). For rule of construction, see Wash. Rev. Code 1.12.025(1). **Severability — 1967 Ex.Sess. chap. 93:** "If any provision of this act, or its application to any person or circumstance is held invalid, the remainder of the act, or the application of the provision to other persons or circumstances is not affected." [1967 Ex.Sess. chap. 93 sec. 7.]
West Virginia	**62-1D-3. Interception of communications generally.** (a) Except as otherwise specifically provided in this article it is unlawful for any person to: (1) Intentionally intercept, attempt to intercept or procure any other person to intercept or attempt to intercept, any wire, oral or electronic communication; or (2) Intentionally disclose or intentionally attempt to disclose to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of this article; and (3) Intentionally use or disclose or intentionally attempt to use or disclose the contents of any wire, oral or electronic communication or the identity of any party thereto, knowing or having reason to know that such information was obtained through the interception of a wire, oral or electronic communication in violation of this article. (b) Any person who violates subsection (a) of this section is guilty of a felony, and, upon conviction thereof, shall be imprisoned in the penitentiary for not more than five years or fined not more than ten thousand dollars or both fined and imprisoned. (c) It is lawful under this article for an operator of a switchboard or an officer, employee, or provider of any wire or electronic communication service whose facilities are used in the transmission of a wire communication to intercept, disclose or use that communication or the identity of any party to that communication in the normal course of his or her employment while engaged in any activity which is a necessary incident to the rendition of his or her service or to the protection of the rights or property of the carrier of the communication. Providers of wire or electronic communication services may not utilize service observing or random monitoring except for mechanical or service quality control checks. (d) Notwithstanding any other law, any provider of wire or electronic communications services, or the directors, officers, employees, agents, landlords or custodians of any such provider, are authorized to provide information, facilities or technical assistance to persons authorized by this article to intercept wire, oral or electronic communication if such provider or its directors, officers, employees, agents, landlords or custodians has been provided with a duly certified copy of a court order directing such assistance and setting forth the period of time

	during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities or assistance required. No cause of action shall lie in any court against any such provider of wire or electronic communication services, its directors, officers, agents, landlords or custodians for providing information facilities or assistance in accordance with the terms of any such order. (e) It is lawful under this article for a person to intercept a wire, oral or electronic communication where the person is a party to the communication or where one of the parties to the communication has given prior consent to the interception unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the United States or the constitution or laws of this State: (f) notwithstanding the provisions of this article or any other provision of law, an electronic interception as defined by section one, article one-f of this chapter, is regulated solely by the provisions of article one-f of this chapter, and no penalties or other requirements of this article are applicable. **61-3-24c. Intercepting or monitoring customer telephone calls; penalty.** (a) It is unlawful for any person, firm or corporation to intercept or monitor, or to attempt to intercept or monitor, the transmission of a message, signal or other communication by telephone between an employee or similar agent of such person, firm or corporation and a customer of such person, firm or corporation unless such person, firm or corporation does all of the following: (1) Notifies each employee or agent subject to interception or monitoring that their telephone messages are subject to interception or monitoring. (2) Provides telephone instruments for employee's personal use which are not subject to intercepting or monitoring. Any person, firm or corporation violating the provisions of this section is guilty of a misdemeanor, and, upon conviction thereof, shall be fined not less than fifty nor more than two hundred dollars, or imprisoned in the county jail not more than one year, or both fined and imprisoned. (b) Nothing contained in this section shall require marking of telephone instruments nor require consent to interception or monitoring, in the case of a wiretap or other form of monitoring which is engaged in for the sole purpose of law enforcement and which is lawful in all other respects. (c) The public service commission shall not issue any rule or regulation requiring or suggesting the monitoring of any message, signal or other communication by telephone to or from any telephone utility customer so as to obtain the content or substance of any such communication. **21-3-20. Use of video and other electronic surveillance devices by employers prohibited.** (a) It is unlawful for any employer or the agent or representative of an employer, whether public or private, to operate any electronic surveillance device or system, including, but not limited to, the use of a closed circuit television system, a video-recording device, or any combination of those or other electronic devices for the purpose of recording or monitoring the activities of the employees in areas designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as rest rooms, shower rooms, locker rooms, dressing rooms and employee lounges. (b) Any employer or agent thereof who violates any provision of this section is guilty of a misdemeanor and, if convicted, shall be fined five hundred dollars for the first offense. An employer or agent thereof convicted a second time under this provision shall be fined one thousand dollars. For the third and any subsequent offense, the penalty shall be two thousand dollars. **62-1F-2. Electronic interception of conduct or oral communications in the home authorized.** (a) Prior to engaging in electronic interception, as defined in section one of this article, an investigative or law-enforcement officer shall, in accordance with this article, first obtain from a magistrate or a judge of a circuit court within the county wherein the non-consenting party's home is located an order authorizing said interception. The order shall be based upon an affidavit by the investigative or law-enforcement officer or an informant that establishes probable cause that the interception would provide evidence of the commission of a crime under the laws of this State or the United States. (b) The Legislature hereby requests the Supreme Court of Appeals to promptly undertake all necessary actions and promulgate any requisite rules to assure a magistrate or circuit judge is available after normal business hours to authorize warrants. **21-3-20. Electronic surveillance; Use prohibited in certain areas; Penalty for violations—** (a) It is unlawful for any employer or the agent or representative of an employer, whether public or private, to operate any electronic surveillance device or system, including, but not limited to, the use of a closed circuit television system, a video-recording device, or any combination of those or other electronic devices for the purpose of recording or monitoring the activities of the employees in areas

	designed for the health or personal comfort of the employees or for safeguarding of their possessions, such as rest rooms, shower rooms, locker rooms, dressing rooms and employee lounges. (b) Any employer or agent thereof who violates any provision of this section is guilty of a misdemeanor and, if convicted, shall be fined five hundred dollars for the first offense. An employer or agent thereof convicted a second time under this provision shall be fined one thousand dollars. For the third and any subsequent offense, the penalty shall be two thousand dollars.
Wisconsin	**968.31 Interception and disclosure of wire, electronic or oral communications prohibited.** (1) Except as otherwise specifically provided in ss. 196.63 or 968.28 to 968.30, whoever commits any of the acts enumerated in this section is guilty of a Class H felony: (a) Intentionally intercepts, attempts to intercept or procures any other person to intercept or attempt to intercept, any wire, electronic or oral communication. (b) Intentionally uses, attempts to use or procures any other person to use or attempt to use any electronic, mechanical or other device to intercept any oral communication. (c) Discloses, or attempts to disclose, to any other person the contents of any wire, electronic or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication in violation of this section or under circumstances constituting violation of this section. (d) Uses, or attempts to use, the contents of any wire, electronic or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication in violation of this section or under circumstances constituting violation of this section. (e) Intentionally discloses the contents of any oral, electronic or wire communication obtained by authority of ss. 968.28, 968.29 and 968.30, except as therein provided. (f) Intentionally alters any wire, electronic or oral communication intercepted on tape, wire or other device. (2) It is not unlawful under ss. 968.28 to 968.37: (a) For an operator of a switchboard, or an officer, employee or agent of any provider of a wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication to intercept, disclose or use that communication in the normal course of his or her employment while engaged in any activity which is a necessary incident to the rendition of his or her service or to the protection of the rights or property of the provider of that service, except that a provider of a wire or electronic communication service shall not utilize service observing or random monitoring except for mechanical or service quality control checks. (b) For a person acting under color of law to intercept a wire, electronic or oral communication, where the person is a party to the communication or one of the parties to the communication has given prior consent to the interception. (c) For a person not acting under color of law to intercept a wire, electronic or oral communication where the person is a party to the communication or where one of the parties to the communication has given prior consent to the interception unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the United States or of any state or for the purpose of committing any other injurious act. (d) For any person to intercept or access an electronic communication made through an electronic communication system that is configured so that the electronic communication is readily accessible to the general public. (e) For any person to intercept any radio communication that is transmitted: 1. By any station for the use of the general public, or that relates to ships, aircraft, vehicles or persons in distress; 2. By any governmental, law enforcement, civil defense, private land mobile or public safety communications system, including police and fire, readily accessible to the general public; 3. By a station operating on an authorized frequency within the bands allocated to the amateur, citizens band or general mobile radio services; or 4. By any marine or aeronautical communications system. (f) For any person to engage in any conduct that: 1. Is prohibited by section 633 of the communications act of 1934; or 2. Is excepted from the application of section 705 (a) of the communications act of 1934 by section 705 (b) of that act. (g) For any person to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of the interference. (h) For users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of the system, if the communication is not scrambled or encrypted. (i) To use a pen register or a trap and trace device as authorized under ss. 968.34 to 968.37; or (j) For a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of the service. (2m) Any person whose wire, electronic or oral

	communication is intercepted, disclosed or used in violation of ss. 968.28 to 968.37 shall have a civil cause of action against any person who intercepts, discloses or uses, or procures any other person to intercept, disclose, or use, the communication, and shall be entitled to recover from any such person: (a) Actual damages, but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher; (b) Punitive damages; and (c) A reasonable attorney's fee and other litigation costs reasonably incurred. (3) Good faith reliance on a court order or on s. 968.30 (7) shall constitute a complete defense to any civil or criminal action brought under ss. 968.28 to 968.37. History: 1971 c. 40 ss. 92, 93; 1977 c. 272; 1985 a. 297; 1987 a. 399; 1989 a. 56; 1991 a. 294; 1997 a. 283; 2001 a. 109. The testimony of an undercover police officer who was carrying a concealed eavesdropping device under sub. (2) is not the product of the eavesdropping and is admissible even assuming the eavesdropping was unconstitutional. State v. Smith, 72 Wis.2d 711, 242 N.W.2d 184 (1976). An individual, who volunteers to aid the authorities in a lawful, albeit surreptitious, investigation does not commit an injury against the investigated party under sub. (2) (c) simply by participation. Undercover informants must surely realize that evidence they receive may be potentially harmful to the target of the investigation, but this is not the type of injurious act contemplated by the statute. State v. Maloney, 2005 WI 74, 281 Wis.2d 595, 698 N.W.2d 583, 03-2180. Consent under sub. (2) (b) may be express or implied in fact from surrounding circumstances indicating that the person knowingly agreed to the surveillance. In the prison setting, an inmate has given implied consent to electronic surveillance when he or she has meaningful notice that a telephone call is subject to monitoring and recording and nonetheless proceeds with the call. State v. Riley, 2005 WI App 203, 287 Wis.2d 244, 704 N.W.2d 635, 04-2321. The use of the "called party control device" by the communications common carrier to trace bomb scares and other harassing telephone calls would not violate any law if used with the consent of the receiving party. 60 Atty. Gen. 90.
Wyoming	**7-3-702. Prohibition against interception or disclosure of wire, oral or electronic communications; exceptions; penalties.** (a) Except as provided in subsection (b) of this section, no person shall intentionally: (i) Intercept, attempt to intercept, or procure any other person to intercept or attempt to intercept any wire, oral or electronic communication; (ii) Use, attempt to use, or procure any other person to use or attempt to use any electronic, mechanical or other device to intercept any oral communication when: (A) Such device is affixed to, or otherwise transmits a signal through, a wire, cable or other like connection used in wire communication; or (B) Such device transmits communications by radio or interferes with the transmission of such communication. (iii) Disclose or attempt to disclose to another person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of this section; (iv) Use or attempt to use the contents of any wire, oral or electronic communication knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of this section; (v) Disclose, or attempt to disclose, to any other person the contents of any wire, oral or electronic communication, intercepted by means authorized by this act: (A) Knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation; (B) Having obtained or received the information in connection with a criminal investigation; and (C) With intent to improperly obstruct, impede or interfere with a duly authorized criminal investigation. (b) Nothing in subsection (a) of this section prohibits: (i) An operator of a switchboard, or an officer, employee or agent of a wire or electronic communication service whose facilities are used in the transmission of a wire communication from intercepting, disclosing or using a wire or electronic communication intercepted in the normal course of that person's employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks; (ii) An officer, employee or agent of any provider of wire or electronic communications service, landlords, custodians or other persons from providing information, facilities or technical assistance to a peace officer who is authorized pursuant to this act to intercept a wire, oral or electronic communication if any such person has been provided with a court order directing such assistance. No provider of wire or electronic communication service, officer, employee or agent thereof, or landlord, custodian or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court

	order under this act, except as may otherwise be required by legal process and then only after prior notification to the attorney general. Any such disclosure, shall render such person liable for the civil damages provided for in W.S. 7-3-710. No criminal or civil cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees or agents, landlord, custodian or other specified person for providing information, facilities or assistance in accordance with the terms of a court order under this act; (iii) An officer, employee or agent of the federal communications commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the commission in the enforcement of 47 U.S.C. § 151 et seq., from intercepting a wire or electronic communication, or oral communication transmitted by radio, or disclosing or using the information thereby obtained; (iv) Any person from intercepting an oral, wire or electronic communication where the person is a party to the communication or where one (1) of the parties to the communication has given prior consent to the interception unless the communication is intercepted for the purpose of committing any criminal or tortious act; (v) A peace officer from intercepting, using or disclosing to another peace officer in the course of his official duties any wire, oral or electronic communication pursuant to an order permitting the interception under this act; (vi) An employee of a telephone company from intercepting a wire communication for the sole purpose of tracing the origin of the communication upon request by the recipient of the communication who alleges that the communication is obscene, harassing or threatening in nature. The person conducting the interception shall notify local law enforcement authorities of the interception within forty-eight (48) hours; (vii) A person from intercepting or accessing an electronic communication made through an electronic communication system that is configured so that the electronic communication is readily accessible to the general public; (viii) A person from intercepting any radio communication which is transmitted: (A) By any station for the use of the general public, or that relates to ships, aircraft, vehicles or persons in distress; (B) By any governmental, law enforcement, civil defense, private land mobile or public safety communications system, including police and fire, readily accessible to the general public; (C) By a station operating on an authorized frequency within the bands allocated to the amateur, citizens band or general mobile radio services; or (D) By any marine or aeronautical communications system. (ix) A person from intercepting any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; (x) Other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of the system, if the communication is not scrambled or encrypted; or (xi) Conduct described in this paragraph unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain. Conduct that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted: (A) To a broadcasting station for purposes of retransmission to the general public; or (B) As an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls. (c) It shall not be unlawful under this act: (i) To use a pen register or a trap and trace device authorized by article 8 of this chapter; or (ii) For a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service. (d) Except as provided in subsection (e) of this section, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient. (e) A person or entity providing electronic communication service to the public may divulge the contents of any such communication: (i) As otherwise authorized in W.S. 7-3-702(b)(i), (ii) or 7-3-706; (ii) With the lawful consent of the originator or any addressee or intended recipient of such communication; (iii) To a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or (iv) Which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency. (f) Except as otherwise provided in this subsection, any person who violates this section is guilty of a felony punishable by a fine of not more than one thousand dollars ($1,000.00), imprisonment for not more than five (5) years, or both. If the intercepted communication is the radio

	portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless handset and the base unit, a public land mobile radio service communication or a paging service communication, a violation of this section is a misdemeanor punishable by a fine of not more than seven hundred fifty dollars ($750.00), imprisonment for not more than six (6) months, or both. **7-3-802. General prohibition on pen register and trap and trace device use; exception.** (a) Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under W.S. 7-3-804. (b) The prohibition of subsection (a) of this section does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service: (i) Relating to the operation, maintenance and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; (ii) To record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (iii) Where the consent of the user of that service has been obtained. (c) A state or local agency authorized to install and use a pen register under this act shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing. (d) Whoever knowingly violates subsection (a) of this section shall be fined not more than one thousand dollars ($1,000.00), imprisoned not more than one (1) year, or both.