## Chapter 9.73 RCW PRIVACY, VIOLATING RIGHT OF

## Sections

9.73.010 9.73.020	Divulging telegram. Opening sealed letter.
9.73.030	Intercepting, recording, or divulging private communication —Consent required—Exceptions.
9.73.040	Intercepting private communication—Court order permitting interception—Grounds for issuance—Duration—Renewal.
9.73.050 9.73.060	Admissibility of intercepted communication in evidence. Violating right of privacy—Civil action—Liability for damages.
9.73.070 9.73.080	Persons and activities excepted from chapter. Penalties.
9.73.090	Certain emergency response personnel exempted from RCW 9.73.030 through 9.73.080—Standards—Court authorizations—Admissibility.
9.73.095	Intercepting, recording, or divulging offender conversations—Conditions—Notice.
9.73.100	Recordings available to defense counsel.
9.73.110	Intercepting, recording, or disclosing private communications—Not unlawful for building owner— Conditions.
9.73.130	Recording private communications—Authorization— Application for, contents.
9.73.140	Recording private communications—Authorization of or application for—Inventory, contents, service— Availability of recording, applications, and orders.
9.73.200	Intercepting, transmitting, or recording conversations concerning controlled substances—Findings.
9.73.210	Intercepting, transmitting, or recording conversations concerning controlled substances or commercial sexual abuse of a minor—Authorization—Monthly report— Admissibility—Destruction of information.
9.73.220	Judicial authorizations-Availability of judge required.
9.73.230	Intercepting, transmitting, or recording conversations concerning controlled substances or commercial sexual abuse of a minor—Conditions—Written reports required— Judicial review—Notice—Admissibility—Penalties.
9.73.240	Intercepting, transmitting, or recording conversations concerning controlled substances—Concurrent power of attorney general to investigate and prosecute.
9.73.260	Pen registers, trap and trace devices, cell site simulator devices.
9.73.270	Collecting, using electronic data or metadata—Cell site

simulator devices-Requirements.

**RCW 9.73.010 Divulging telegram.** Every person who shall wrongfully obtain or attempt to obtain, any knowledge of a telegraphic message, by connivance with the clerk, operator, messenger, or other employee of a telegraph company, and every clerk, operator, messenger, or other employee of such company who shall willfully divulge to any but the person for whom it was intended, any telegraphic message or

dispatch intrusted to him or her for transmission or delivery, or the nature or contents thereof, or shall willfully refuse, neglect, or delay duly to transmit or deliver the same, shall be guilty of a misdemeanor. [2011 c 336 § 323; 1909 c 249 § 410; Code 1881 § 2342; RRS § 2662.]

Intercepting, delaying telegram: RCW 9A.48.070, 9A.48.080.

RCW 9.73.020 Opening sealed letter. Every person who shall wilfully open or read, or cause to be opened or read, any sealed message, letter or telegram intended for another person, or publish the whole or any portion of such a message, letter or telegram, knowing it to have been opened or read without authority, shall be guilty of a misdemeanor. [1909 c 249 § 411; RRS § 2663.]

RCW 9.73.030 Intercepting, recording, or divulging private communication—Consent required—Exceptions. (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.

(5) This section does not apply to the recording of custodial interrogations pursuant to RCW 10.122.040. [2021 c 329 § 21. Prior: 1986 c 38 § 1; 1985 c 260 § 2; 1977 ex.s. c 363 § 1; 1967 ex.s. c 93 § 1.1

Severability-1967 ex.s. c 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.s. c 93 § 7.]

RCW 9.73.040 Intercepting private communication—Court order permitting interception—Grounds for issuance—Duration—Renewal. (1) An ex parte order for the interception of any communication or conversation listed in RCW 9.73.030 may be issued by any superior court judge in the state upon verified application of either the state attorney general or any county prosecuting attorney setting forth fully facts and circumstances upon which the application is based and stating that:

(a) There are reasonable grounds to believe that national security is endangered, that a human life is in danger, that arson is about to be committed, or that a riot is about to be committed, and

(b) There are reasonable grounds to believe that evidence will be obtained essential to the protection of national security, the preservation of human life, or the prevention of arson or a riot, and

(c) There are no other means readily available for obtaining such information.

(2) Any application pursuant to this section that seeks communications or conversations related to an investigation that alleges criminal liability for the provision, receipt, attempted provision or receipt, assistance in the provision or receipt, or attempted assistance in the provision or receipt of protected health care services as defined in RCW 7.115.010 that are lawful in the state of Washington shall include an attestation, made under penalty of perjury, stating that the application seeks information related to the provision, receipt, attempted provision or receipt, assistance in the provision or receipt, or attempted assistance in the provision or receipt of protected health care services as defined in RCW 7.115.010 that are lawful in the state of Washington.

(3) Where statements are solely upon the information and belief of the applicant, the grounds for the belief must be given.

(4) The applicant must state whether any prior application has been made to obtain such communications on the same instrument or for the same person and if such prior application exists the applicant shall disclose the current status thereof.

(5) The application and any order issued under RCW 9.73.030 through 9.73.080 shall identify as fully as possible the particular equipment, lines or location from which the information is to be obtained and the purpose thereof.

(6) The court may examine upon oath or affirmation the applicant and any witness the applicant desires to produce or the court requires to be produced.

(7) Orders issued under this section shall be effective for fifteen days, after which period the court which issued the order may upon application of the officer who secured the original order renew or continue the order for an additional period not to exceed fifteen days.

(8) No order issued under this section shall authorize or purport to authorize any activity which would violate any laws of the United States.

(9) The court shall not issue an order for the interception of any communication or conversation for the purpose of investigating or recovering evidence that relates to an investigation that alleges criminal liability for the provision, receipt, attempted provision or receipt, assistance in the provision or receipt, or attempted assistance in the provision or receipt of protected health care services as defined in RCW 7.115.010 that are lawful in the state of Washington. [2023 c 193 § 5; 1967 ex.s. c 93 § 2.]

Effective date-2023 c 193: See note following RCW 7.115.020.

Severability-1967 ex.s. c 93: See note following RCW 9.73.030.

RCW 9.73.050 Admissibility of intercepted communication in evidence. Any information obtained in violation of RCW 9.73.030 or pursuant to any order issued under the provisions of RCW 9.73.040 shall be inadmissible in any civil or criminal case in all courts of general or limited jurisdiction in this state, except with the permission of the person whose rights have been violated in an action brought for damages under the provisions of RCW 9.73.030 through 9.73.080, or in a criminal action in which the defendant is charged with a crime, the commission of which would jeopardize national security. [1967 ex.s. c 93 § 3.]

Severability-1967 ex.s. c 93: See note following RCW 9.73.030.

RCW 9.73.060 Violating right of privacy—Civil action—Liability for damages. Any person who, directly or by means of a detective agency or any other agent, violates the provisions of this chapter shall be subject to legal action for damages, to be brought by any other person claiming that a violation of this statute has injured his or her business, his or her person, or his or her reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured by him or her on account of violation of the provisions of this chapter, or liquidated damages computed at the rate of one hundred dollars a day for each day of violation, not to exceed one thousand dollars, and a reasonable attorney's fee and other costs of litigation. [2011 c 336 § 324; 1977 ex.s. c 363 § 2; 1967 ex.s. c 93 § 4.]

Severability-1967 ex.s. c 93: See note following RCW 9.73.030.

**RCW 9.73.070 Persons and activities excepted from chapter.** (1) The provisions of this chapter shall not apply to any activity in connection with services provided by a common carrier pursuant to its

tariffs on file with the Washington utilities and transportation commission or the Federal Communication Commission and any activity of any officer, agent or employee of a common carrier who performs any act otherwise prohibited by this law in the construction, maintenance, repair and operations of the common carrier's communications services, facilities, or equipment or incident to the use of such services, facilities or equipment. Common carrier as used in this section means any person engaged as a common carrier or public service company for hire in intrastate, interstate or foreign communication by wire or radio or in intrastate, interstate or foreign radio transmission of energy.

(2) The provisions of this chapter shall not apply to:

(a) Any common carrier automatic number, caller, or location identification service that has been approved by the Washington utilities and transportation commission; or

(b) A 911 or enhanced 911 emergency service as defined in RCW 82.14B.020, for purposes of aiding public health or public safety agencies to respond to calls placed for emergency assistance. [1994 c 49 § 1. Prior: 1991 c 329 § 8; 1991 c 312 § 1; 1967 ex.s. c 93 § 5.]

Severability-1967 ex.s. c 93: See note following RCW 9.73.030.

RCW 9.73.080 Penalties. (1) Except as otherwise provided in this chapter, any person who violates RCW 9.73.030 is guilty of a gross misdemeanor.

(2) Any person who knowingly alters, erases, or wrongfully discloses any recording in violation of RCW 9.73.090(1)(c) is guilty of a gross misdemeanor. [2000 c 195 § 3; 1989 c 271 § 209; 1967 ex.s. c 93 § 6.1

Intent-2000 c 195: See note following RCW 9.73.090.

Severability-1989 c 271: See note following RCW 9.94A.510.

Severability-1967 ex.s. c 93: See note following RCW 9.73.030.

RCW 9.73.090 Certain emergency response personnel exempted from RCW 9.73.030 through 9.73.080—Standards—Court authorizations— Admissibility. (1) The provisions of RCW 9.73.030 through 9.73.080 shall not apply to police, fire, emergency medical service, emergency communication center, and poison center personnel in the following instances:

(a) Recording incoming telephone calls to police and fire stations, licensed emergency medical service providers, emergency communication centers, and poison centers;

(b) Video and/or sound recordings may be made of arrested persons by police officers responsible for making arrests or holding persons in custody before their first appearance in court. Such video and/or sound recordings shall conform strictly to the following:

(i) The arrested person shall be informed that such recording is being made and the statement so informing him or her shall be included in the recording;

(ii) The recording shall commence with an indication of the time of the beginning thereof and terminate with an indication of the time thereof;

(iii) At the commencement of the recording the arrested person shall be fully informed of his or her constitutional rights, and such statements informing him or her shall be included in the recording;

(iv) The recordings shall only be used for valid police or court activities;

(c) Sound recordings that correspond to video images recorded by video cameras mounted in law enforcement vehicles. All law enforcement officers wearing a sound recording device that makes recordings corresponding to videos recorded by video cameras mounted in law enforcement vehicles must be in uniform. A sound recording device that makes a recording pursuant to this subsection (1) (c) must be operated simultaneously with the video camera when the operating system has been activated for an event. No sound recording device may be intentionally turned off by the law enforcement officer during the recording of an event. Once the event has been captured, the officer may turn off the audio recording and place the system back into "preevent" mode.

No sound or video recording made under this subsection (1)(c) may be duplicated and made available to the public by a law enforcement agency subject to this section until final disposition of any criminal or civil litigation which arises from the event or events which were recorded. Such sound recordings shall not be divulged or used by any law enforcement agency for any commercial purpose.

A law enforcement officer shall inform any person being recorded by sound under this subsection (1)(c) that a sound recording is being made and the statement so informing the person shall be included in the sound recording, except that the law enforcement officer is not required to inform the person being recorded if the person is being recorded under exigent circumstances. A law enforcement officer is not required to inform a person being recorded by video under this subsection (1)(c) that the person is being recorded by video.

(2) It shall not be unlawful for a law enforcement officer acting in the performance of the officer's official duties to intercept, record, or disclose an oral communication or conversation where the officer is a party to the communication or conversation or one of the parties to the communication or conversation has given prior consent to the interception, recording, or disclosure: PROVIDED, That prior to the interception, transmission, or recording the officer shall obtain written or telephonic authorization from a judge or magistrate, who shall approve the interception, recording, or disclosure of communications or conversations with a nonconsenting party for a reasonable and specified period of time, if there is probable cause to believe that the nonconsenting party has committed, is engaged in, or is about to commit a felony: PROVIDED HOWEVER, That if such authorization is given by telephone the authorization and officer's statement justifying such authorization must be electronically recorded by the judge or magistrate on a recording device in the custody of the judge or magistrate at the time transmitted and the recording shall be retained in the court records and reduced to writing as soon as possible thereafter.

Any recording or interception of a communication or conversation incident to a lawfully recorded or intercepted communication or conversation pursuant to this subsection shall be lawful and may be divulged. All recordings of communications or conversations made pursuant to this subsection shall be retained for as long as any crime may be charged based on the events or communications or conversations recorded.

(3) Communications or conversations authorized to be intercepted, recorded, or disclosed by this section shall not be inadmissible under RCW 9.73.050.

(4) Authorizations issued under subsection (2) of this section shall be effective for not more than seven days, after which period the issuing authority may renew or continue the authorization for additional periods not to exceed seven days.

(5) If the judge or magistrate determines that there is probable cause to believe that the communication or conversation concerns the unlawful manufacture, delivery, sale, or possession with intent to manufacture, deliver, or sell, controlled substances as defined in chapter 69.50 RCW, or legend drugs as defined in chapter 69.41 RCW, or imitation controlled substances as defined in chapter 69.52 RCW, the judge or magistrate may authorize the interception, transmission, recording, or disclosure of communications or conversations under subsection (2) of this section even though the true name of the nonconsenting party, or the particular time and place for the interception, transmission, recording, or disclosure, is not known at the time of the request, if the authorization describes the nonconsenting party and subject matter of the communication or conversation with reasonable certainty under the circumstances. Any such communication or conversation may be intercepted, transmitted, recorded, or disclosed as authorized notwithstanding a change in the time or location of the communication or conversation after the authorization has been obtained or the presence of or participation in the communication or conversation by any additional party not named in the authorization.

Authorizations issued under this subsection shall be effective for not more than fourteen days, after which period the issuing authority may renew or continue the authorization for an additional period not to exceed fourteen days. [2011 c 336 § 325; 2006 c 38 § 1; 2000 c 195 § 2; 1989 c 271 § 205; 1986 c 38 § 2; 1977 ex.s. c 363 § 3; 1970 ex.s. c 48 § 1.]

Intent-2000 c 195: "The legislature intends, by the enactment of this act, to provide a very limited exception to the restrictions on disclosure of intercepted communications." [2000 c 195 § 1.]

Severability-1989 c 271: See note following RCW 9.94A.510.

Severability—1970 ex.s. c 48: "If a court of competent jurisdiction shall adjudge to be invalid or unconstitutional any clause, sentence, paragraph, section or part of this act, such judgment or decree shall not affect, impair, invalidate or nullify the remainder of this act, but the effect thereof shall be confined to the clause, sentence, paragraph, section or part of this chapter so adjudged to be invalid or unconstitutional." [1970 ex.s. c 48 § 3.]

RCW 9.73.095 Intercepting, recording, or divulging offender conversations—Conditions—Notice. (1) RCW 9.73.030 through 9.73.080 and 9.73.260 shall not apply to employees of the department of corrections in the following instances: Intercepting, recording, or divulging any telephone calls from an offender or resident of a state correctional facility; or intercepting, recording, or divulging any monitored nontelephonic conversations in offender living units, cells, rooms, dormitories, and common spaces where offenders may be present. For the purposes of this section, "state correctional facility" means a facility that is under the control and authority of the department of corrections, and used for the incarceration, treatment, or rehabilitation of convicted felons.

(2) (a) All personal calls made by offenders shall be made using a calling system approved by the secretary of corrections which is at least as secure as the system it replaces. In approving one or more calling systems, the secretary of corrections shall consider the safety of the public, the ability to reduce telephone fraud, and the ability of offender families to select a low-cost option.

(b) The calls shall be "operator announcement" type calls. The operator shall notify the receiver of the call that the call is coming from a prison offender, and that it will be recorded and may be monitored.

(3) The department of corrections shall adhere to the following procedures and restrictions when intercepting, recording, or divulging any telephone calls from an offender or resident of a state correctional facility as provided for by this section. The department shall also adhere to the following procedures and restrictions when intercepting, recording, or divulging any monitored nontelephonic conversations in offender living units, cells, rooms, dormitories, and common spaces where offenders may be present:

(a) Unless otherwise provided for in this section, after intercepting or recording any conversation, only the superintendent and his or her designee shall have access to that recording.

(b) The contents of any intercepted and recorded conversation shall be divulged only as is necessary to safeguard the orderly operation of the correctional facility, in response to a court order, or in the prosecution or investigation of any crime.

(c) All conversations that are recorded under this section, unless being used in the ongoing investigation or prosecution of a crime, or as is necessary to assure the orderly operation of the correctional facility, shall be destroyed one year after the intercepting and recording.

(4) So as to safeguard the sanctity of the attorney-client privilege, the department of corrections shall not intercept, record, or divulge any conversation between an offender or resident and an attorney. The department shall develop policies and procedures to implement this section. The department's policies and procedures implemented under this section shall also recognize the privileged nature of confessions made by an offender to a member of the clergy or a priest in his or her professional character, in the course of discipline enjoined by the church to which he or she belongs as provided in RCW 5.60.060(3).

(5) The department shall notify in writing all offenders, residents, and personnel of state correctional facilities that their nontelephonic conversations may be intercepted, recorded, or divulged in accordance with the provisions of this section.

(6) The department shall notify all visitors to state correctional facilities who may enter offender living units, cells, rooms, dormitories, or common spaces where offenders may be present, that their conversations may intercepted, recorded, or divulged in accordance with the provisions of this section. The notice required under this subsection shall be accomplished through a means no less conspicuous than a general posting in a location likely to be seen by visitors entering the facility. [2004 c 13 § 2; 1998 c 217 § 2; 1996 c 197 § 1; 1989 c 271 § 210.]

Findings—Intent—2004 c 13: "The legislature finds that the current telephone service for offender calls from department of corrections facilities is based on outdated technology that provides neither the most secure nor the most accountable system available and is provided at a high cost to the offenders' families. The legislature, in budget provisions, has required the secretary of corrections to investigate other systems as offender telephone service contracts came due for renewal. The legislature now finds that the current statute prevents the secretary of corrections from using systems that provide greater security, more offender accountability, and lower costs. Therefore, the legislature intends to remove this barrier while retaining the intent of the statute to provide safe, accountable, and affordable telephone services." [2004 c 13 § 1.]

Effective dates—1996 c 197: "(1) Sections 1 and 3 of this act shall take effect August 1, 1996.

(2) Section 2 of this act is necessary for the immediate preservation of the public peace, health, or safety, or support of the state government and its existing public institutions, and shall take effect immediately [March 28, 1996]." [1996 c 197 § 4.]

Severability-1989 c 271: See note following RCW 9.94A.510.

Local government reimbursement claims: RCW 4.92.280.

RCW 9.73.100 Recordings available to defense counsel. Video and/or sound recordings obtained by police personnel under the authority of RCW 9.73.090 and 9.73.100 shall be made available for hearing and/or viewing by defense counsel at the request of defense counsel whenever a criminal charge has been filed against the subject of the video and/or sound recordings. [1970 ex.s. c 48 § 2.]

Severability-1970 ex.s. c 48: See note following RCW 9.73.090.

RCW 9.73.110 Intercepting, recording, or disclosing private communications—Not unlawful for building owner—Conditions. It shall not be unlawful for the owner or person entitled to use and possession of a building, as defined in RCW 9A.04.110(5), or the agent of such person, to intercept, record, or disclose communications or conversations which occur within such building if the persons engaged in such communication or conversation are engaged in a criminal act at the time of such communication or conversation by virtue of unlawful entry or remaining unlawfully in such building. [1977 ex.s. c 363 § 4.]

RCW 9.73.130 Recording private communications—Authorization— Application for, contents. Each application for an authorization to record communications or conversations pursuant to RCW 9.73.090 as now or hereafter amended shall be made in writing upon oath or affirmation and shall state:

(1) The authority of the applicant to make such application;

(2) The identity and qualifications of the investigative or law enforcement officers or agency for whom the authority to record a communication or conversation is sought and the identity of whoever authorized the application;

(3) A particular statement of the facts relied upon by the applicant to justify his or her belief that an authorization should be issued, including:

(a) The identity of the particular person, if known, committing the offense and whose communications or conversations are to be recorded;

(b) The details as to the particular offense that has been, is being, or is about to be committed;

(c) The particular type of communication or conversation to be recorded and a showing that there is probable cause to believe such communication will be communicated on the wire communication facility involved or at the particular place where the oral communication is to be recorded;

(d) The character and location of the particular wire communication facilities involved or the particular place where the oral communication is to be recorded;

(e) A statement of the period of time for which the recording is required to be maintained, if the character of the investigation is such that the authorization for recording should not automatically terminate when the described type of communication or conversation has been first obtained, a particular statement of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(f) A particular statement of facts showing that other normal investigative procedures with respect to the offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ;

(4) Where the application is for the renewal or extension of an authorization, a particular statement of facts showing the results thus far obtained from the recording, or a reasonable explanation of the failure to obtain such results;

(5) A complete statement of the facts concerning all previous applications, known to the individual authorizing and to the individual making the application, made to any court for authorization to record a wire or oral communication involving any of the same facilities or places specified in the application or involving any person whose communication is to be intercepted, and the action taken by the court on each application; and

(6) Such additional testimony or documentary evidence in support of the application as the judge may require. [2011 c 336 § 326; 1977 ex.s. c 363 § 6.]

RCW 9.73.140 Recording private communications—Authorization of or application for—Inventory, contents, service—Availability of recording, applications, and orders. Within a reasonable time but not later than thirty days after the termination of the period of the authorization or of extensions or renewals thereof, or the date of the denial of an authorization applied for under RCW 9.73.090 as now or hereafter amended, the issuing authority shall cause to be served on the person named in the authorization or application for an authorization, and such other parties to the recorded communications as the judge may in his or her discretion determine to be in the interest of justice, an inventory which shall include:

(1) Notice of the entry of the authorization or the application for an authorization which has been denied under RCW 9.73.090 as now or hereafter amended;

(2) The date of the entry of the authorization or the denial of an authorization applied for under RCW 9.73.090 as now or hereafter amended;

(3) The period of authorized or disapproved recording; and

(4) The fact that during the period wire or oral communications were or were not recorded.

The issuing authority, upon the filing of a motion, may in its discretion make available to such person or his or her attorney for inspection such portions of the recorded communications, applications and orders as the court determines to be in the interest of justice. On an ex parte showing of good cause to the court the serving of the inventory required by this section may be postponed or dispensed with. [2011 c 336 § 327; 1977 ex.s. c 363 § 7.]

RCW 9.73.200 Intercepting, transmitting, or recording conversations concerning controlled substances—Findings. The legislature finds that the unlawful manufacturing, selling, and distributing of controlled substances is becoming increasingly prevalent and violent. Attempts by law enforcement officers to prevent the manufacture, sale, and distribution of drugs is resulting in numerous life-threatening situations since drug dealers are using sophisticated weapons and modern technological devices to deter the efforts of law enforcement officials to enforce the controlled substance statutes. Dealers of unlawful drugs are employing a wide variety of violent methods to realize the enormous profits of the drug trade.

Therefore, the legislature finds that conversations regarding illegal drug operations should be intercepted, transmitted, and recorded in certain circumstances without prior judicial approval in order to protect the life and safety of law enforcement personnel and to enhance prosecution of drug offenses, and that that interception and transmission can be done without violating the constitutional guarantees of privacy. [1989 c 271 § 201.]

Severability-1989 c 271: See note following RCW 9.94A.510.

RCW 9.73.210 Intercepting, transmitting, or recording conversations concerning controlled substances or commercial sexual abuse of a minor—Authorization—Monthly report—Admissibility— Destruction of information. (1) If a police commander or officer above the rank of first line supervisor has reasonable suspicion that the safety of the consenting party is in danger, law enforcement personnel may, for the sole purpose of protecting the safety of the consenting party, intercept, transmit, or record a private conversation or communication concerning:

(a) The unlawful manufacture, delivery, sale, or possession with intent to manufacture, deliver, or sell, controlled substances as defined in chapter 69.50 RCW, or legend drugs as defined in chapter 69.41 RCW, or imitation controlled substances as defined in chapter 69.52 RCW; or

(b) Person(s) engaging in the commercial sexual abuse of a minor under RCW 9.68A.100, or promoting commercial sexual abuse of a minor under RCW 9.68A.101, or promoting travel for commercial sexual abuse of a minor under RCW 9.68A.102.

(2) Before any interception, transmission, or recording of a private conversation or communication pursuant to this section, the police commander or officer making the determination required by subsection (1) of this section shall complete a written authorization which shall include (a) the date and time the authorization is given; (b) the persons, including the consenting party, expected to participate in the conversation or communication, to the extent known; (c) the expected date, location, and approximate time of the conversation or communication; and (d) the reasons for believing the consenting party's safety will be in danger.

(3) A monthly report shall be filed by the law enforcement agency with the administrator for the courts indicating the number of authorizations made under this section, the date and time of each authorization, and whether an interception, transmission, or recording was made with respect to each authorization.

(4) Any information obtained pursuant to this section is inadmissible in any civil or criminal case in all courts of general or limited jurisdiction in this state, except:

(a) With the permission of the person whose communication or conversation was intercepted, transmitted, or recorded without his or her knowledge;

(b) In a civil action for personal injury or wrongful death arising out of the same incident, where the cause of action is based upon an act of physical violence against the consenting party; or

(c) In a criminal prosecution, arising out of the same incident for a serious violent offense as defined in RCW 9.94A.030 in which a party who consented to the interception, transmission, or recording was a victim of the offense.

(5) Nothing in this section bars the admission of testimony of a participant in the communication or conversation unaided by information obtained pursuant to this section.

(6) The authorizing agency shall immediately destroy any written, transcribed, or recorded information obtained from an interception, transmission, or recording authorized under this section unless the agency determines there has been a personal injury or death or a serious violent offense which may give rise to a civil action or criminal prosecution in which the information may be admissible under subsection (4)(b) or (c) of this section.

(7) Nothing in this section authorizes the interception, recording, or transmission of a telephonic communication or conversation. [2011 c 241 § 3; 1989 c 271 § 202.]

Findings-Effective date-2011 c 241: See notes following RCW 9.73.230.

Severability-1989 c 271: See note following RCW 9.94A.510.

RCW 9.73.220 Judicial authorizations—Availability of judge required. In each superior court judicial district in a county with a population of two hundred ten thousand or more there shall be available twenty-four hours a day at least one superior court or district court judge or magistrate designated to receive telephonic requests for authorizations that may be issued pursuant to this chapter. The presiding judge of each such superior court in conjunction with the district court judges in that superior court judicial district shall establish a coordinated schedule of rotation for all of the superior and district court judges and magistrates in the superior court judicial district for purposes of ensuring the availability of at least one judge or magistrate at all times. During the period that each judge or magistrate is designated, he or she shall be equipped with an electronic paging device when not present at his or her usual telephone. It shall be the designated judge's or magistrate's responsibility to ensure that all attempts to reach him or her for purposes of requesting authorization pursuant to this chapter are forwarded to the electronic page number when the judge or magistrate leaves the place where he or she would normally receive such calls. [1991 c 363 § 9; 1989 c 271 § 203.]

Purpose-Captions not law-1991 c 363: See notes following RCW 2.32.180.

Severability-1989 c 271: See note following RCW 9.94A.510.

RCW 9.73.230 Intercepting, transmitting, or recording conversations concerning controlled substances or commercial sexual abuse of a minor-Conditions-Written reports required-Judicial review -Notice-Admissibility-Penalties. (1) As part of a bona fide criminal investigation, the chief law enforcement officer of a law enforcement agency or his or her designee above the rank of first line supervisor may authorize the interception, transmission, or recording of a conversation or communication by officers under the following circumstances:

(a) At least one party to the conversation or communication has consented to the interception, transmission, or recording;

(b) Probable cause exists to believe that the conversation or communication involves:

(i) The unlawful manufacture, delivery, sale, or possession with intent to manufacture, deliver, or sell, controlled substances as defined in chapter 69.50 RCW, or legend drugs as defined in chapter 69.41 RCW, or imitation controlled substances as defined in chapter 69.52 RCW; or

(ii) A party engaging in the commercial sexual abuse of a minor under RCW 9.68A.100, or promoting commercial sexual abuse of a minor under RCW 9.68A.101, or promoting travel for commercial sexual abuse of a minor under RCW 9.68A.102; and

(c) A written report has been completed as required by subsection (2) of this section.

(2) The agency's chief officer or designee authorizing an interception, transmission, or recording under subsection (1) of this section, shall prepare and sign a written report at the time of authorization indicating:

(a) The circumstances that meet the requirements of subsection(1) of this section;

(b) The names of the authorizing and consenting parties, except that in those cases where the consenting party is a confidential informant, the name of the confidential informant need not be divulged;

(c) The names of the officers authorized to intercept, transmit, and record the conversation or communication;

(d) The identity of the particular person or persons, if known, who may have committed or may commit the offense;

(e) The details of the particular offense or offenses that may have been or may be committed and the expected date, location, and approximate time of the conversation or communication; and

(f) Whether there was an attempt to obtain authorization pursuant to RCW 9.73.090(2) and, if there was such an attempt, the outcome of the attempt.

(3) An authorization under this section is valid in all jurisdictions within Washington state and for the interception of communications from additional persons if the persons are brought into the conversation or transaction by the nonconsenting party or if the nonconsenting party or such additional persons cause or invite the consenting party to enter another jurisdiction.

(4) The recording of any conversation or communication under this section shall be done in such a manner that protects the recording from editing or other alterations.

(5) An authorization made under this section is valid for no more than twenty-four hours from the time it is signed by the authorizing officer, and each authorization shall independently meet all of the requirements of this section. The authorizing officer shall sign the written report required under subsection (2) of this section, certifying the exact date and time of his or her signature. An authorization under this section may be extended not more than twice for an additional consecutive twenty-four hour period based upon the same probable cause regarding the same suspected transaction. Each such extension shall be signed by the authorizing officer.

(6) Within fifteen days after the signing of an authorization that results in any interception, transmission, or recording of a conversation or communication pursuant to this section, the law enforcement agency which made the interception, transmission, or recording shall submit a report including the original authorization under subsection (2) of this section to a judge of a court having jurisdiction which report shall identify (a) the persons, including the consenting party, who participated in the conversation, and (b) the date, location, and approximate time of the conversation.

In those cases where the consenting party is a confidential informant, the name of the confidential informant need not be divulged.

A monthly report shall be filed by the law enforcement agency with the administrator for the courts indicating the number of authorizations granted, the date and time of each authorization, interceptions made, arrests resulting from an interception, and subsequent invalidations.

(7) (a) Within two judicial days of receipt of a report under subsection (6) of this section, the court shall make an ex parte review of the authorization and shall make a determination whether the requirements of subsection (1) of this section were met. Evidence obtained as a result of the interception, transmission, or recording need not be submitted to the court. If the court determines that any of the requirements of subsection (1) of this section were not met, the court shall order that any recording and any copies or transcriptions of the conversation or communication be destroyed. Destruction of recordings, copies, or transcriptions shall be stayed pending any appeal of a finding that the requirements of subsection (1) of this section were not met.

(b) Absent a continuation under (c) of this subsection, six months following a determination under (a) of this subsection that probable cause did not exist, the court shall cause a notice to be mailed to the last known address of any nonconsenting party to the conversation or communication that was the subject of the authorization. The notice shall indicate the date, time, and place of any interception, transmission, or recording made pursuant to the authorization. The notice shall also identify the agency that sought the authorization and shall indicate that a review under (a) of this subsection resulted in a determination that the authorization was made in violation of this section provided that, if the confidential informant was a minor at the time of the recording or an alleged victim of commercial child sexual abuse under RCW 9.68A.100 through 9.68A.102 or 9[A].40.100, no such notice shall be given.

(c) An authorizing agency may obtain six-month extensions to the notice requirement of (b) of this subsection in cases of active, ongoing criminal investigations that might be jeopardized by sending the notice.

(8) In any subsequent judicial proceeding, evidence obtained through the interception or recording of a conversation or communication pursuant to this section shall be admissible only if:

(a) The court finds that the requirements of subsection (1) of this section were met and the evidence is used in prosecuting an offense listed in subsection (1)(b) of this section; or

(b) The evidence is admitted with the permission of the person whose communication or conversation was intercepted, transmitted, or recorded; or

(c) The evidence is admitted in a prosecution for a "serious violent offense" as defined in RCW 9.94A.030 in which a party who consented to the interception, transmission, or recording was a victim of the offense; or

(d) The evidence is admitted in a civil suit for personal injury or wrongful death arising out of the same incident, in which a party who consented to the interception, transmission, or recording was a victim of a serious violent offense as defined in RCW 9.94A.030.

Nothing in this subsection bars the admission of testimony of a party or eyewitness to the intercepted, transmitted, or recorded conversation or communication when that testimony is unaided by information obtained solely by violation of RCW 9.73.030.

(9) Any determination of invalidity of an authorization under this section shall be reported by the court to the administrative office of the courts.

(10) Any person who intentionally intercepts, transmits, or records or who intentionally authorizes the interception, transmission, or recording of a conversation or communication in violation of this section, is guilty of a class C felony punishable according to chapter 9A.20 RCW.

(11) An authorizing agency is liable for twenty-five thousand dollars in exemplary damages, in addition to any other damages authorized by this chapter or by other law, to a person whose

conversation or communication was intercepted, transmitted, or recorded pursuant to an authorization under this section if:

(a) In a review under subsection (7) of this section, or in a suppression of evidence proceeding, it has been determined that the authorization was made without the probable cause required by subsection (1) (b) of this section; and

(b) The authorization was also made without a reasonable suspicion that the conversation or communication would involve the unlawful acts identified in subsection (1)(b) of this section. [2011 c 241 § 2; 2005 c 282 § 17; 1989 c 271 § 204.]

Findings-2011 c 241: "The legislature finds increasing incidents of commercial sexual exploitation of children in our state, and further protection of victims require giving law enforcement agencies the tool to have a unified victim-centered police investigation approach to further protect victims by ensuring their safety by prosecuting traffickers. The one-party consent provision permitted for drug trafficking investigation passed in the comprehensive bill to facilitate police investigation and prosecution of drug trafficking crimes is a helpful tool to this end. The legislature also finds that exceptions should be allowed for minors employed for investigation when the minor is a victim and involves only electronic communication with the defendant." [2011 c 241 § 1.]

Effective date-2011 c 241: "This act takes effect August 1, 2011." [2011 c 241 § 5.]

Severability-1989 c 271: See note following RCW 9.94A.510.

RCW 9.73.240 Intercepting, transmitting, or recording conversations concerning controlled substances-Concurrent power of attorney general to investigate and prosecute. (1) The attorney general shall have concurrent authority and power with the prosecuting attorneys to investigate violations of RCW 9.73.200 through 9.73.230 or RCW 9.73.090 and initiate and conduct prosecutions of any violations upon request of any of the following:

(a) The person who was the nonconsenting party to the intercepted, transmitted, or recorded conversation or communication; or

(b) The county prosecuting attorney of the jurisdiction in which the offense has occurred.

(2) The request shall be communicated in writing to the attorney [1989 c 271 § 206.] general.

Severability-1989 c 271: See note following RCW 9.94A.510.

## RCW 9.73.260 Pen registers, trap and trace devices, cell site simulator devices. (1) As used in this section:

(a) "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, and such term includes any electronic storage of such communication.

(b) "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:

(i) Any wire or oral communication;

(ii) Any communication made through a tone-only paging device; or

(iii) Any communication from a tracking device, but solely to the extent the tracking device is owned by the applicable law enforcement agency.

(c) "Electronic communication service" means any service that provides to users thereof the ability to send or receive wire or electronic communications.

(d) "Pen register" means a device that records or decodes electronic or other impulses that identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

(e) "Trap and trace device" means a device that captures the incoming electronic or other impulses that identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

(f) "Cell site simulator device" means a device that transmits or receives radio waves for the purpose of conducting one or more of the following operations: (i) Identifying, locating, or tracking the movements of a communications device; (ii) intercepting, obtaining, accessing, or forwarding the communications, stored data, or metadata of a communications device; (iii) affecting the hardware or software operations or functions of a communications device; (iv) forcing transmissions from or connections to a communications device; (v) denying a communications device access to other communications devices, communications protocols, or services; or (vi) spoofing or simulating a communications device, cell tower, cell site, or service including, but not limited to, an international mobile subscriber identity catcher or other invasive cell phone or telephone surveillance or eavesdropping device that mimics a cell phone tower and sends out signals to cause cell phones in the area to transmit their locations, identifying information, and communications content, or a passive interception device or digital analyzer that does not send signals to a communications device under surveillance. A cell site simulator device does not include any device used or installed by an electric utility, as defined in RCW 19.280.020, solely to the extent such device is used by that utility to measure electrical usage, to provide services to customers, or to operate the electric grid.

(2) No person may install or use a pen register, trap and trace device, or cell site simulator device without a prior court order issued under this section except as provided under subsection (6) of this section or RCW 9.73.070.

(3) A law enforcement officer may apply for and the superior court may issue orders and extensions of orders authorizing the installation and use of pen registers, trap and trace devices, and

cell site simulator devices as provided in this section. The application shall be under oath and shall include the identity of the officer making the application and the identity of the law enforcement agency conducting the investigation. The applicant must certify that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

(4) If the court finds that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation and finds that there is probable cause to believe that the pen register, trap and trace device, or cell site simulator device will lead to obtaining evidence of a crime, contraband, fruits of crime, things criminally possessed, weapons, or other things by means of which a crime has been committed or reasonably appears about to be committed, or will lead to learning the location of a person who is unlawfully restrained or reasonably believed to be a witness in a criminal investigation or for whose arrest there is probable cause, the court shall enter an ex parte order authorizing the installation and use of a pen register, trap and trace device, or cell site simulator device. The order shall specify:

(a) (i) In the case of a pen register or trap and trace device, the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached; or

(ii) In the case of a cell site simulator device, the identity, if known, of (A) the person to whom is subscribed or in whose name is subscribed the electronic communications service utilized by the device to which the cell site simulator device is to be used and (B) the person who possesses the device to which the cell site simulator device is to be used;

(b) The identity, if known, of the person who is the subject of the criminal investigation;

(c) (i) In the case of a pen register or trap and trace device, the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; or

(ii) In the case of a cell site simulator device: (A) The telephone number or other unique subscriber account number identifying the wire or electronic communications service account used by the device to which the cell site simulator device is to be attached or used; (B) if known, the physical location of the device to which the cell site simulator device is to be attached or used; (C) the type of device, and the communications protocols being used by the device, to which the cell site simulator device is to be attached or used; (D) the geographic area that will be covered by the cell site simulator device; (E) all categories of metadata, data, or information to be collected by the cell site simulator device from the targeted device including, but not limited to, call records and geolocation information; (F) whether or not the cell site simulator device will incidentally collect metadata, data, or information from any parties or devices not specified in the court order, and if so, what categories of information or metadata will be collected; and (G) any disruptions to access or use of a communications or internet access network that may be created by use of the device; and

(d) A statement of the offense to which the information likely to be obtained by the pen register, trap and trace device, or cell site simulator device relates.

The order shall direct, if the applicant has requested, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register, trap and trace device, or cell site simulator device. An order issued under this section shall authorize the installation and use of a: (i) Pen register or a trap and trace device for a period not to exceed sixty days; and (ii) cell site simulator device for sixty days. An extension of the original order may only be granted upon: A new application for an order under subsection (3) of this section; and a showing that there is a probability that the information or items sought under this subsection are more likely to be obtained under the extension than under the original order. No extension beyond the first extension shall be granted unless: There is a showing that there is a high probability that the information or items sought under this subsection are much more likely to be obtained under the second or subsequent extension than under the original order; and there are extraordinary circumstances such as a direct and immediate danger of death or serious bodily injury to a law enforcement officer. The period of extension shall be for a period not to exceed sixty days.

An order authorizing or approving the installation and use of a pen register, trap and trace device, or cell site simulator device shall direct that the order be sealed until otherwise ordered by the court and that the person owning or leasing the line to which the pen register, trap and trace device, and cell site simulator device is attached or used, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register, trap and trace device, or cell site simulator device or the existence of the investigation to the listed subscriber or to any other person, unless or until otherwise ordered by the court.

(5) Upon the presentation of an order, entered under subsection (4) of this section, by an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish such law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in subsection (4) of this section.

Upon the request of an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line and shall furnish such law enforcement officer all additional information, facilities, and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in subsection (4) of this section. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this subsection shall be reasonably compensated by the law enforcement agency that requests the facilities or assistance for such reasonable expenses incurred in providing such facilities and assistance.

No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order under this section. A good faith reliance on a court order under this section, a request pursuant to this section, a legislative authorization, or a statutory authorization is a complete defense against any civil or criminal action brought under this chapter or any other law.

(6) (a) Notwithstanding any other provision of this chapter, a law enforcement officer and a prosecuting attorney or deputy prosecuting attorney who jointly and reasonably determine that there is probable cause to believe that an emergency situation exists that involves immediate danger of death or serious bodily injury to any person that requires the installation and use of a pen register, trap and trace device, or cell site simulator device before an order authorizing such installation and use can, with due diligence, be obtained, and there are grounds upon which an order could be entered under this chapter to authorize such installation and use, may have installed and use a pen register, trap and trace device, or cell site simulator device if, within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with subsection (4) of this section. In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register, trap and trace device, or cell site simulator device, whichever is earlier. If an order approving the installation or use is not obtained within forty-eight hours, any information obtained is not admissible as evidence in any legal proceeding. The knowing installation or use by any law enforcement officer of a pen register, trap and trace device, or cell site simulator device pursuant to this subsection without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter and be punishable as a gross misdemeanor. A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this subsection shall be reasonably compensated by the law enforcement agency that requests the facilities or assistance for such reasonable expenses incurred in providing such facilities and assistance.

(b) A law enforcement agency that authorizes the installation of a pen register, trap and trace device, or cell site simulator device under this subsection (6) shall file a monthly report with the administrator for the courts. The report shall indicate the number of authorizations made, the date and time of each authorization, whether a court authorization was sought within forty-eight hours, and whether a subsequent court authorization was granted.

(c) A law enforcement agency authorized to use a cell site simulator device in accordance with this section must: (i) Take all steps necessary to limit the collection of any information or metadata to the target specified in the applicable court order; (ii) take all steps necessary to permanently delete any information or metadata collected from any party not specified in the applicable court order immediately following such collection and must not transmit, use, or retain such information or metadata for any purpose whatsoever; and (iii) delete any information or metadata collected from the target specified in the court order within thirty days if there is no longer probable cause to support the belief that such information or metadata is evidence of a crime.

(7) (a) If an application for the installation and use of a pen register, trap and trace device, or cell site simulator device is for the purpose of investigating or recovering evidence that relates to an investigation that alleges criminal liability for the provision, receipt, attempted provision or receipt, assistance in the provision or receipt, or attempted assistance in the provision or receipt of protected health care services as defined in RCW 7.115.010 that are lawful in the state of Washington, the applicant shall include an attestation, made under penalty of perjury, stating that the application seeks information related to the provision, receipt, attempted provision or receipt, assistance in the provision or receipt, or attempted assistance in the provision or receipt of protected health care services as defined in RCW 7.115.010 that are lawful in the state of Washington.

(b) The court shall not issue an order for the installation and use of pen registers, trap and trace devices, and cell site simulator devices for the purpose of investigating or recovering evidence that relates to an investigation that alleges criminal liability for the provision, receipt, attempted provision or receipt, assistance in the provision or receipt, or attempted assistance in the provision or receipt of protected health care services as defined in RCW 7.115.010 that are lawful in the state of Washington. [2023 c 193 § 6; 2015 c 222 § 2; 1998 c 217 § 1.]

Effective date-2023 c 193: See note following RCW 7.115.020.

Effective date-2015 c 222: See note following RCW 9.73.270.

Local government reimbursement claims: RCW 4.92.280.

RCW 9.73.270 Collecting, using electronic data or metadata—Cell site simulator devices-Requirements. The state and its political subdivisions shall not, by means of a cell site simulator device, collect or use a person's electronic data or metadata without (1) that person's informed consent, (2) a warrant, based upon probable cause, that describes with particularity the person, place, or thing to be searched or seized, or (3) acting in accordance with a legally recognized exception to the warrant requirements. [2015 c 222 § 1.]

Effective date-2015 c 222: "This act is necessary for the immediate preservation of the public peace, health, or safety, or support of the state government and its existing public institutions, and takes effect immediately [May 11, 2015]." [2015 c 222 § 4.]