Chapter 23a
Interception of Communications Act

77-23a-1 Short title.

This act shall be known and may be cited as the "Interception of Communications Act."

Enacted by Chapter 15, 1980 General Session

77-23a-2 Legislative findings.

The Legislature finds and determines that:

(1) Wire communications are normally conducted through facilities which form part of an interstate network. The same facilities are used for interstate and intrastate communications.

(2) In order to protect effectively the privacy of wire and oral communications, to protect the integrity of court and administrative proceedings, and to prevent the obstruction of intrastate commerce, it is necessary for the legislature to define the circumstances and conditions under which the interception of wire and oral communications may be authorized and to prohibit any unauthorized interception of these communications and the use of the contents thereof in evidence in courts and administrative proceedings.

(3) Organized criminals make extensive use of wire and oral communications in their criminal activities. The interception of such communications to obtain evidence of the commission of crimes or to prevent their commission is an indispensable aid to law enforcement and the administration of justice.

(4) To safeguard the privacy of innocent persons, the interception of wire or oral communications when none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurance that the interception is justified and that the information obtained thereby will not be misused.

Enacted by Chapter 15, 1980 General Session

77-23a-3 Definitions.

As used in this chapter:

(1) "Aggrieved person" means a person who was a party to any intercepted wire, electronic, or oral communication, or a person against whom the interception was directed.

(2) "Aural transfer" means any transfer containing the human voice at any point between and including the point of origin and the point of reception.

(3) "Communications common carrier" means any person engaged as a common carrier for hire in intrastate, interstate, or foreign communication by wire or radio, including a provider of electronic communication service. However, a person engaged in radio broadcasting is not, when that person is so engaged, a communications common carrier.

(4) "Contents" when used with respect to any wire, electronic, or oral communication includes any information concerning the substance, purport, or meaning of that communication.

(5) "Electronic communication" means any transfer of signs, signals, writings, 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) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;
(b) any wire or oral communications;
(c) any communication made through a tone-only paging device; or
(d) any communication from an electronic or mechanical device that permits the tracking of the movement of a person or object.

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

(7) "Electronic communications system" means any wire, radio, electromagnetic, photoelectronic, or photo-optical facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of the communication.

(8) "Electronic, mechanical, or other device" means any device or apparatus that may be used to intercept a wire, electronic, or oral communication other than:
(a) any telephone or telegraph instrument, equipment or facility, or a component of any of them:
(i) furnished by the provider of wire or electronic communications service or by the subscriber or user, and being used by the subscriber or user in the ordinary course of its business; or
(ii) being used by a provider of wire or electronic communications 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.

(9) "Electronic storage" means:
(a) any temporary intermediate storage of a wire or electronic communication incident to the electronic transmission of it; and
(b) any storage of the communication by an electronic communications service for the purposes of backup protection of the communication.

(10) "Intercept" means the acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.

(11) "Investigative or law enforcement officer" means any officer of the state or of a political subdivision, who by law may conduct investigations of or make arrests for offenses enumerated in this chapter, or any federal officer as defined in Section 53-13-106, and any attorney authorized by law to prosecute or participate in the prosecution of these offenses.

(12) "Judge of competent jurisdiction" means a judge of a district court of the state.

(13) "Oral communication" means any oral communication uttered by a person exhibiting an expectation that the communication is not subject to interception, under circumstances justifying that expectation, but does not include any electronic communication.

(14) "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 the device is attached. "Pen register" 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 the provider, or any device used by a provider or customer of a wire communications service for cost accounting or other like purposes in the ordinary course of its business.

(15) "Person" means any employee or agent of the state or a political subdivision, and any individual, partnership, association, joint stock company, trust, or corporation.

(16) "Readily accessible to the general public" means, regarding a radio communication, that the communication is not:
(a) scrambled or encrypted;

(b) transmitted using modulation techniques with essential parameters that have been withheld from the public with the intention of preserving the privacy of the communication;
(c) carried on a subcarrier or signal subsidiary to a radio transmission;
(d) transmitted over a communications 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, 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.
(17) "Trap and trace device" means a device, process, or procedure 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 is transmitted.
(18) "User" means any person or entity who:
(a) uses an electronic communications service; and
(b) is authorized by the provider of the service to engage in the use.
(19)
(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 the connection in a switching station, furnished or operated by any person engaged as a common carrier in providing or operating these facilities for the transmission of intrastate, interstate, or foreign communications.
(b) "Wire communication" includes the electronic storage of the communication, but does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit.

Amended by Chapter 302, 2025 General Session

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 (9)(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 (10)(b) or (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 (11)(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; or

(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 (11)(b)(i), and shall impose a civil fine of not less than $500 for each violation of the injunction.

Amended by Chapter 340, 2011 General Session

77-23a-4.5 Implanting an electronic identification device -- Penalties.

(1) A person may not require, coerce, or compel any other individual to undergo or submit to the subcutaneous implanting of a radio frequency identification tag.

(2) Any person who violates Subsection (1) is guilty of a class A misdemeanor.

(3)

(a) A person who is implanted with a subcutaneous identification device in violation of Subsection (1) may bring a civil action in any court of competent jurisdiction for actual damages, compensatory damages, punitive damages, injunctive relief, or any combination of these.

(b) The initial civil penalty may not be more than $10,000, and no more than $1,000 for each day the violation continues until the electronic identification device is removed or disabled.

Enacted by Chapter 168, 2011 General Session

77-23a-5 Traffic in intercepting devices -- Offenses -- Lawful activities.

(1) Except as otherwise specifically provided in this chapter, any person is guilty of a third degree felony who intentionally:
  (a) sends through the mail, or sends or carries in intrastate, interstate, or foreign commerce any electronic, mechanical, or other device, knowing or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious interception of wire, electronic, or oral communications;
  (b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious interception of wire, electronic, or oral communications; or
  (c) 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 the 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 the advertisement promotes the use of the device for the purpose of the surreptitious interception of wire, electronic, or oral communications.
(2) The following persons may send through the mail, send or carry in intrastate, interstate, or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of the device renders it primarily useful for the purpose of surreptitious interception of wire, electronic, or oral communication:
  (a) 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, in the normal course of the activities of the United States, a state, or a political subdivision.

Amended by Chapter 122, 1989 General Session

77-23a-6 Seizure and forfeiture of intercepting devices.

Any electronic, mechanical or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of Sections 77-23a-4 and 77-23a-5, may be seized and forfeited to the State of Utah.

Enacted by Chapter 15, 1980 General Session

77-23a-7 Evidence -- Exclusionary rule.

When any wire, electronic, or oral communication has been intercepted, no part of the contents of the communication and no evidence derived from it 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 state, or a political subdivision of the state, if the disclosure of that information would be in violation of this chapter.

Amended by Chapter 251, 1988 General Session

77-23a-8 Court order to authorize or approve interception -- Procedure.

(1) The attorney general of the state, any assistant attorney general specially designated by the attorney general, any county attorney, district attorney, deputy county attorney, or deputy district attorney specially designated by the county attorney or by the district attorney, may

authorize an application to a judge of competent jurisdiction for an order for an interception of wire, electronic, or oral communications by any law enforcement agency of the state, the federal government or of any political subdivision of the state that is responsible for investigating the type of offense for which the application is made.

(2) The judge may grant the order in conformity with the required procedures when the interception sought may provide or has provided evidence of the commission of:

(a) an act:

(i) prohibited by the criminal provisions of:

(A) Title 58, Chapter 37, Utah Controlled Substances Act;

(B) Title 58, Chapter 37c, Utah Controlled Substance Precursor Act; or

(C) Title 58, Chapter 37d, Clandestine Drug Lab Act; and

(ii) punishable by a term of imprisonment of more than one year;

(b) an act prohibited by the criminal provisions under Title 61, Chapter 1, Utah Uniform Securities Act, and punishable by a term of imprisonment of more than one year;

(c) an offense:

(i) of:

(A) attempt under Section 76-4-101;

(B) conspiracy under Section 76-4-201;

(C) criminal solicitation of an adult, Section 76-4-203; or

(D) criminal solicitation of a minor, Section 76-4-205; and

(ii) punishable by a term of imprisonment of more than one year;

(d) a threat of terrorism offense punishable by a maximum term of imprisonment of more than one year under Section 76-5-107.3;

(e)

(i) aggravated murder under Section 76-5-202;

(ii) murder under Section 76-5-203; or

(iii) manslaughter under Section 76-5-205;

(f)

(i) kidnapping under Section 76-5-301;

(ii) child kidnapping under Section 76-5-301.1;

(iii) aggravated kidnapping under Section 76-5-302;

(iv) human trafficking for labor under Section 76-5-308;

(v) human trafficking for sexual exploitation under Section 76-5-308.1;

(vi) human trafficking of a child under Section 76-5-308.5;

(vii) human smuggling under Section 76-5-308.3;

(viii) aggravated human trafficking under Section 76-5-310; or

(ix) aggravated human smuggling under Section 76-5-310.1;

(g)

(i) arson under Section 76-6-102; or

(ii) aggravated arson under Section 76-6-103;

(h)

(i) burglary under Section 76-6-202; or

(ii) aggravated burglary under Section 76-6-203;

(i)

(i) robbery under Section 76-6-301; or

(ii) aggravated robbery under Section 76-6-302;

(j) an offense:

(i) of:

(A) theft under Section 76-6-404;
(B) theft by deception under Section 76-6-405; or
(C) theft by extortion under Section 76-6-406; and
(ii) punishable by a maximum term of imprisonment of more than one year;
(k) an offense of receiving stolen property that is punishable by a maximum term of imprisonment of more than one year under Section 76-6-408;
(l) a financial card transaction offense punishable by a maximum term of imprisonment of more than one year under Section 76-6-506.2, 76-6-506.3, or 76-6-506.6;
(m) bribery of a labor official under Section 76-6-509;
(n) bribery or threat to influence a publicly exhibited contest under Section 76-6-514;
(o) a criminal simulation offense punishable by a maximum term of imprisonment of more than one year under Section 76-6-518;
(p) criminal usury under Section 76-6-520;
(q) insurance fraud punishable by a maximum term of imprisonment of more than one year under Section 76-6-521;
(r) a violation under Title 76, Chapter 6, Part 7, Utah Computer Crimes Act, punishable by a maximum term of imprisonment of more than one year under Section 76-6-703;
(s) bribery to influence official or political actions under Section 76-8-103;
(t) misusing public money or public property under Section 76-8-402;
(u) tampering with a witness under Section 76-8-508;
(v) retaliation against a witness, victim, or informant under Section 76-8-508.3;
(w) tampering or retaliating against a juror under Section 76-8-508.5;
(x) receiving or soliciting a bribe as a witness under Section 76-8-508.7;
(y) extortion or bribery to dismiss a criminal proceeding under Section 76-8-509;
(z) obstruction of justice in a criminal investigation or proceeding under Section 76-8-306;
(aa) harboring or concealing offender who has escaped from official custody under Section 76-8-309.2;
(bb) destruction of property to interfere with preparations for defense or war under Section 76-8-802;
(cc) an attempt to commit crimes of sabotage under Section 76-8-804;
(dd) conspiracy to commit crimes of sabotage under Section 76-8-805;
(ee) advocating criminal syndicalism or sabotage under Section 76-8-902;
(ff) assembling for advocating criminal syndicalism or sabotage under Section 76-8-903;
(gg) riot punishable by a maximum term of imprisonment of more than one year under Section 76-9-101;
(hh) dog fighting, training dogs for fighting, or dog fighting exhibitions punishable by a maximum term of imprisonment of more than one year under Section 76-13-205;
(ii) delivery to a common carrier or mailing of an explosive, chemical, or incendiary device under Section 76-15-209;
(jj) unlawful conduct involving an explosive, chemical, or incendiary device under Section 76-15-210;
(kk) unlawful conduct involving an explosive, chemical, or incendiary part under Section 76-15-211;
(ll) exploiting prostitution under Section 76-5d-207;
(mm) aggravated exploitation of prostitution under Section 76-5d-208;
(nn) bus hijacking under Section 76-9-1502;
(oo) assault with intent to commit bus hijacking under Section 76-9-1503;

(pp) unlawful discharge of a firearm or hurling of a missile into a bus or terminal under Section 76-9-1504;
(qq) violations under Title 76, Chapter 17, Part 4, Offenses Concerning a Pattern of Unlawful Activity, and the offenses listed under the definition of unlawful activity in the act, including the offenses not punishable by a maximum term of imprisonment of more than one year when those offenses are investigated as predicates for the offenses prohibited by the act under Section 76-17-401;
(rr) communications fraud under Section 76-6-525;
(ss) money laundering under Sections 76-9-1602 and 76-9-1603; or
(tt) reporting by a person engaged in a trade or business when the offense is punishable by a maximum term of imprisonment of more than one year under Section 76-9-1604.

Amended by Chapter 173, 2025 General Session
Amended by Chapter 174, 2025 General Session

77-23a-9 Disclosure or use of intercepted information.

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, electronic, or oral communication, or evidence derived from any of these, may disclose those 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, electronic, or oral communication or evidence derived from any of them may use those contents to the extent the use is appropriate to the proper performance of the officer's official duties.
(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, electronic, or oral communication or evidence derived from any of them intercepted in accordance with this chapter may disclose the contents of that communication or the 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.
(4) An otherwise privileged wire, electronic, or oral communication intercepted in accordance with, or in violation of, the provisions of this chapter does not lose its privileged character.
(5) When an investigative or law enforcement officer, while engaged in intercepting wire, electronic, or oral communications in the manner authorized, intercepts wire, electronic, or oral communications relating to offenses other than those specified in the order of authorization or approval, the contents, and evidence derived from the contents, may be disclosed or used as provided in Subsections (1) and (2). The contents and any evidence derived from them may be used under Subsection (3) when authorized or approved by a judge of competent jurisdiction, if the judge finds on subsequent application that the contents were otherwise intercepted in accordance with this chapter. The application shall be made as soon as practicable.

Amended by Chapter 302, 2025 General Session

77-23a-10 Application for order -- Authority of order -- Emergency action -- Application -- Entry -- Conditions -- Extensions -- Recordings -- Admissibility or suppression -- Appeal by state.

(1) Each application for an order 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 competent

jurisdiction, and shall state the applicant's authority to make the application. Each application shall include:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

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

(ii) except as provided in Subsection (12), 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 communication sought to be intercepted; and

(iv) the identity of the person, if known, committing the offense and whose communication is to be intercepted;

(c) a full and complete statement as to whether other investigative procedures have been tried and failed or why they reasonably appear to be either unlikely to succeed if tried or too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained, and if the investigation is of a nature 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;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and the individual 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 application;

(f) when the application is for the extension of an order, a statement setting forth the results so far obtained from the interception, or a reasonable explanation of the failure to obtain results; and

(g) additional testimony or documentary evidence in support of the application as the judge may require.

(2) Upon 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 state if the judge determines on the basis of the facts submitted by the applicant that:

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense under Section 77-23a-8;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through the interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be either unlikely to succeed if tried or too dangerous; and

(d) except as provided in Subsection (12), 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 the offense, or are leased to, listed in the name of, or commonly used by that person.

(3) Each order authorizing or approving the interception of any wire, electronic, or oral communications shall specify:

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) except as provided in Subsection (12), 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 of the persons authorizing the application; and
(e) the period of time during which the interception is authorized, including a statement as to whether the interception shall automatically terminate when the described communications has been first obtained.

(4) An order authorizing the interception of a wire, electronic, or oral communications shall, upon request of the applicant, direct that a provider of wire or electronic communications service, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that the provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communications service, landlord, custodian, or other person furnishing the facilities or technical assistance shall be compensated by the applicant for reasonable expenses involved in providing the facilities or systems.

(5)
(a) An order entered under this chapter may not authorize or approve the interception of any wire, electronic, or oral communications for any period longer than is necessary to achieve the objective of the authorization, but in any event for no longer than 30 days. The 30-day period begins on the day the investigative or law enforcement officer first begins to conduct an interception under the order, or 10 days after the order is entered, whichever is earlier.
(b) Extensions of an order may be granted, but only upon application for an extension made under Subsection (1) and if the court makes the findings required by Subsection (2). The period of extension may be no longer than the authorizing judge considers necessary to achieve the purposes for which it was granted, but in no event for longer than 30 days.
(c) Every order and extension shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted so 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 within 30 days.
(d) If 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, the minimizing of the interception may be accomplished as soon as practicable after the interception.
(e) An interception under this chapter may be conducted in whole or in part by government personnel or by an individual under contract with the government and acting under supervision of an investigative or law enforcement officer authorized to conduct the interception.

(6) When an order authorizing interception is entered under this chapter, 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. These reports shall be made at intervals the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer who is specially designated by either the attorney general or a county attorney or district attorney, as provided under Sections 17-18a-202 and 17-18a-203 may intercept wire, electronic, or oral communications if an application for an order approving the interception is

made in accordance with this section and within 48 hours after the interception has occurred or begins to occur, when the investigative or law enforcement officer reasonably determines that:

(a) an emergency situation exists that involves:

(i) immediate danger of death or serious physical injury to any person;

(ii) conspiratorial activities threatening the national security interest; or

(iii) conspiratorial activities characteristic of organized crime, that require a wire, electronic, or oral communications to be intercepted before an order authorizing interception can, with diligence, be obtained; and

(b) there are grounds upon which an order could be entered under this chapter to authorize the interception.

(8)

(a) In the absence of an order under Subsection (7), the interception immediately terminates when the communication sought is obtained or when the application for the order is denied, whichever is earlier.

(b) If 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, electronic, or oral communications intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in Subsection (9)(d) on the person named in the application.

(9)

(a) The contents of any wire, electronic, or oral communications intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, electronic, or oral communications under this Subsection (9)(a) shall be done so as to protect the recording from editing or other alterations. Immediately upon the expiration of the period of an order or extension, the recordings shall be made available to the judge issuing the order and sealed under his directions. Custody of the recordings shall be where the judge orders. The recordings may not be destroyed, except upon an order of the issuing or denying judge. In any event, it shall be kept for 10 years. Duplicate recordings may be made for use or disclosure under Subsections 77-23a-9(1) and (2) for investigations. The presence of the seal provided by this Subsection (9)(a), or a satisfactory explanation for the absence of one, is a prerequisite for the use or disclosure of the contents of any wire, electronic, or oral communications or evidence derived from it under Subsection 77-23a-9(3).

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be where the judge directs. The applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and may not be destroyed, except on order of the issuing or denying judge. But in any event they shall be kept for 10 years.

(c) Any violation of any provision of this Subsection (9) may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time, but not later than 90 days after the filing of an application for an order of approval under Subsection 77-23a-10(7) that is denied or the termination of the period of an order or extensions, the issuing or denying judge shall cause to be served on the persons named in the order or the application, and other parties to the intercepted communications as the judge determines in his discretion is in the interest of justice, an inventory, which shall include notice:

(i) of the entry of the order or application;

(ii) of the date of the entry and the period of authorization, approved or disapproved interception, or the denial of the application; and

(iii) that during the period, wire, electronic, or oral communications were or were not intercepted.

(e) The judge, upon filing of a motion, may in the judge's discretion, make available to the person or the person's counsel for inspection the portions of the intercepted communications, applications, and orders 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 (9)(e) may be postponed.

(10) The contents of any intercepted wire, electronic, or oral communications, or evidence derived from any of these, may not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a federal or state court unless each party, not less than 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 or approved. This ten-day period may be waived by the judge if the judge finds that it was not possible to furnish the party with the above information 10 days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving the information.

(11)

(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, the state, or a political subdivision may move to suppress the contents of any intercepted wire, electronic, or oral communications, or evidence derived from any of them, on the grounds that:

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

(b) The motion shall 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. If the motion is granted, the contents of the intercepted wire, electronic, or oral communications, or evidence derived from any of these, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of the motion by the aggrieved person, may in the judge's discretion make available to the aggrieved person or the aggrieved person's counsel for inspection portions of the intercepted communication or evidence derived from the intercepted communication as the judge determines to be in the interests of justice.

(c) In addition to any other right to appeal, the state or its political subdivision may appeal from an order granting a motion to suppress made under Subsection (11)(a), or the denial of an application for an order of approval, if the attorney bringing the appeal certifies to the judge or other official granting the motion or denying the application that the appeal is not taken for the purposes of delay. The appeal shall be taken within 30 days after the date the order was entered and shall be diligently prosecuted.

(12) The requirements of Subsections (1)(b)(ii), (2)(d), and (3)(b) relating to the specification of the facilities from which, or the place where, the wire, electronic, or oral communications are to be intercepted do not apply if:

(a) in the case of an applicant regarding the interception of oral communications:

(i) the application is by a law enforcement officer and is approved by the state attorney general, a deputy attorney general, a county attorney or district attorney, or a deputy county attorney or deputy district attorney;

(ii) the application contains a full and complete statement of why the specification is not practical, and identifies the person committing the offense and whose communications are to be intercepted; or

(iii) the judge finds that the specification is not practical; and

(b) in the case of an application regarding wire or electronic communications:

(i) the application is by a law enforcement officer and is approved by the state attorney general, a deputy attorney general, a county attorney or district attorney, or a deputy county attorney or deputy district attorney;

(ii) 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

(iii) the judge finds that the purpose has been adequately shown.

(13)

(a) An interception of a communication under an order regarding which the requirements of Subsections (1)(b)(ii), (2)(d), and (3)(b) do not apply by reason of Subsection (12) does not begin until the facilities from which, or the place where, the communications are to be intercepted is ascertained by the person implementing the interception order.

(b) A provider of wire or electronic communications service that has received an order under Subsection (12)(b) 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 government, shall decide the motion expeditiously.

Amended by Chapter 237, 2013 General Session

77-23a-11 Civil remedy for unlawful interception -- Action for relief.

(1) Except under Subsections 77-23a-4(3), (4), and (5), a person whose wire, electronic, or oral communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover relief as appropriate from the person or entity that engaged in the violation.

(2) In an action under this section appropriate relief includes:

(a) preliminary and other equitable or declaratory relief as is appropriate;

(b) damages under Subsection (3) and punitive damages in appropriate cases; and

(c) a reasonable attorney's fee and reasonably incurred litigation costs.

(3)

(a) In an action under this section, if the conduct in violation of this chapter is the private viewing of a private satellite video communication that is not scrambled or encrypted, or if the communication is a radio communication that is transmitted on frequencies allocated under Subpart (D), Part 74, Rules of the Federal Communications Commission, that is not scrambled or encrypted, and the conduct is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, the court shall assess damages as follows:

(i) if the person who engaged in the conduct has not previously been enjoined under Subsection 77-23a-4(11) and has not been found liable in a prior civil action under this section, the court shall assess the greater of the sum of actual damages suffered by the plaintiff, or the statutory damages of not less than $50 nor more than $500;

(ii) if on one prior occasion the person who engaged in the conduct has been enjoined under Subsection 77-23a-4(11) or has been liable in a civil action under this section, the court

shall assess the greater of the sum of actual damages suffered by the plaintiff, or statutory damages of not less than $100 and not more than $1,000;

(b) in any other action under this section, the court may assess as damages whichever is the greater of:

(i) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violations; or

(ii) statutory damages of $100 a day for each day of violation, or $10,000, whichever is greater.

(4) A good faith reliance on any of the following is a complete defense against any civil or criminal action brought under this chapter or any other law:

(a) a court order, a warrant, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(b) a request of an investigative or law enforcement officer under Subsection 77-23a-10(7); or

(c) a good faith determination that Section 77-23a-4 permitted the conduct complained of.

(5) A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

(6) The remedies and sanctions described in this chapter regarding the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving these communications.

Amended by Chapter 122, 1989 General Session

77-23a-12 Enjoining a violation -- Civil action by attorney general.

(1) When it appears that a person is engaged or is about to engage in any act that constitutes or will constitute a felony violation of this chapter or is otherwise prohibited by this chapter, the attorney general may initiate a civil action in a district court of the state to enjoin the violation.

(2) The court shall proceed as soon as practicable to the hearing and determination of the action and may at any time before final determination enter a restraining order or prohibition, or take other action as warranted to prevent a continuing and substantial injury to the state or to any person or class of persons for whose protection the action is brought.

(3) A proceeding under this section is governed by the Utah Rules of Civil Procedure, except if an information has been filed or an indictment has been returned against the respondent, discovery is governed by the Utah Rules of Criminal Procedure.

Amended by Chapter 122, 1989 General Session

77-23a-13 Installation of device when court order required -- Penalty.

(1) Except as provided in this section, a person may not install or use a pen register or trap or trace device without previously obtaining a court order under Section 77-23a-15, or under federal law.

(2) Subsection (1) does not apply to the use of a pen register or trap and trace device by a provider of electronic or wire communications services:

(a) relating to the operation, maintenance, and testing of a wire or electronic communications 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

(b) to record that a wire or electronic communication was initiated or completed 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 that service; or

(c) when the consent of the user of that service has been obtained.
(3) A knowing or intentional violation of Subsection (1) is a class B misdemeanor.

Amended by Chapter 241, 1991 General Session

77-23a-14 Court order for installation -- Application.
(1) The attorney general, a deputy attorney general, a county attorney or district attorney, a deputy county attorney or deputy district attorney, or a prosecuting attorney for a political subdivision of the state, or a law enforcement officer, may make application for an order or extension of an order under Section 77-23a-15 authorizing or approving the installation and use of a pen register or trap and trace device, in writing and under oath or equivalent affirmation, to a court of competent jurisdiction.
(2) An application under Subsection (1) shall include:
(a) the identity of the attorney for the government or the law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
(b) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

Amended by Chapter 38, 1993 General Session

77-23a-15 Order for installation -- Contents -- Duration -- Extension -- Disclosure.
(1) In general, upon an application made under Section 77-23a-14, the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the attorney for the government or the law enforcement or investigative officer has certified to the court that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation.
(2)
(a) An order issued under this section shall specify:
(i) 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;
(ii) the identity, if known, of the person who is the subject of the criminal investigation;
(iii) 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 geographical limits of the trap and trace order; and
(iv) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.
(b) The order shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under Section 77-23a-16.
(3)
(a) An order issued under this section may authorize the installation and use of a pen register or trap and trace device for a period not to exceed 60 days.
(b) Extensions of an order may be granted, but only upon an application for an order under Section 77-23a-14 and upon the judicial finding required by Subsection (1). The period of extension shall be for a period not to exceed 60 days.
(4) An order authorizing or approving the installation and use of a pen register or trap and trace device shall direct that:

(a) the order be sealed until otherwise ordered by the court; and
(b) the person owning or leasing the line to which the pen register or trap and trace device is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless otherwise ordered by the court.

Enacted by Chapter 251, 1988 General Session

77-23a-16 Communications provider -- Cooperation and support services -- Compensation -- Liability defense.

(1) Upon the request of an attorney for the government or an officer of a law enforcement agency authorized to install and use pen registers under this chapter, a provider of wire or electronic communications service, landlord, custodian, or other person shall furnish investigative or law enforcement officers 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 the person ordered by the court accords the party regarding whom the installation and use is to take place, if such assistance is directed by a court order as provided in Subsection 77-23a-15(2)(b) of this chapter.

(2)
(a) Upon request of an attorney for the government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of wire or electronic communications service, landlord, custodian, or other person shall:
(i) install the device forthwith on the appropriate line; and
(ii) furnish the investigative or 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 the installation and assistance is directed by a court order under Subsection 77-23a-15(2)(b).
(b) Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the officer of the law enforcement agency designated by the court, at reasonable intervals and during regular business hours, for the duration of the order.

(3) A provider of wire or electronic communications service, landlord, custodian, or other person who furnishes facilities or technical assistance under this section shall be reasonably compensated for reasonable expenses incurred in providing the facilities and assistance.

(4) A cause of action does not lie in any court against the provider of wire or electronic communications 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 chapter.

(5) A good faith reliance on a court order, 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.

Amended by Chapter 302, 2025 General Session