

# AZ Electronic Crime Statutes

(<http://www.azleg.state.az.us/ArizonaRevisedStatutes.asp>)

13-2301E

E. For the purposes of sections 13-2316, 13-2316.01 and 13-2316.02:

1. "Access" means to instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or network.
2. "Access device" means any card, token, code, account number, electronic serial number, mobile or personal identification number, password, encryption key, biometric identifier or other means of account access, including a canceled or revoked access device, that can be used alone or in conjunction with another access device to obtain money, goods, services, computer or network access or any other thing of value or that can be used to initiate a transfer of any thing of value.
3. "Computer" means an electronic device that performs logic, arithmetic or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities that are connected or related to such a device in a system or network.
4. "Computer contaminant" means any set of computer instructions that is designed to modify, damage, destroy, record or transmit information within a computer, computer system or network without the intent or permission of the owner of the information, computer system or network. Computer contaminant includes a group of computer instructions, such as viruses or worms, that is self-replicating or self-propagating and that is designed to contaminate other computer programs or computer data, to consume computer resources, to modify, destroy, record or transmit data or in some other fashion to usurp the normal operation of the computer, computer system or network.
5. "Computer program" means a series of instructions or statements, in a form acceptable to a computer, that permits the functioning of a computer system in a manner designed to provide appropriate products from the computer system.
6. "Computer software" means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.
7. "Computer system" means a set of related, connected or unconnected computer equipment, devices and software, including storage, media and peripheral devices.
8. "Critical infrastructure resource" means any computer or communications system or network that is involved in providing services necessary to ensure or protect the public health, safety or welfare, including services that are provided by any of the following:
  - (a) Medical personnel and institutions.
  - (b) Emergency services agencies.
  - (c) Public and private utilities, including water, power, communications and transportation services.
  - (d) Fire departments, districts or volunteer organizations.
  - (e) Law enforcement agencies.
  - (f) Financial institutions.
  - (g) Public educational institutions.

(h) Government agencies.

9. "False or fraudulent pretense" means the unauthorized use of an access device or the use of an access device to exceed authorized access.

10. "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card or marketable security or any other written instrument as defined in section 13-2001 that is transferable for value.

11. "Network" includes a complex of interconnected computer or communication systems of any type.

12. "Property" means financial instruments, information, including electronically produced data, computer software and programs in either machine or human readable form, and anything of value, tangible or intangible.

13. "Proprietary or confidential computer security information" means information about a particular computer, computer system or network that relates to its access devices, security practices, methods and systems, architecture, communications facilities, encryption methods and system vulnerabilities and that is not made available to the public by its owner or operator.

14. "Services" includes computer time, data processing, storage functions and all types of communication functions.

#### 13-2316. [Computer tampering; venue; forfeiture; classification](#)

A. A person who acts without authority or who exceeds authorization of use commits computer tampering by:

1. Accessing, altering, damaging or destroying any computer, computer system or network, or any part of a computer, computer system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or to control property or services by means of false or fraudulent pretenses, representations or promises.

2. Knowingly altering, damaging, deleting or destroying computer programs or data.

3. Knowingly introducing a computer contaminant into any computer, computer system or network.

4. Recklessly disrupting or causing the disruption of computer, computer system or network services or denying or causing the denial of computer or network services to any authorized user of a computer, computer system or network.

5. Recklessly using a computer, computer system or network to engage in a scheme or course of conduct that is directed at another person and that seriously alarms, torments, threatens or terrorizes the person. For the purposes of this paragraph, the conduct must both:

(a) Cause a reasonable person to suffer substantial emotional distress.

(b) Serve no legitimate purpose.

6. Preventing a computer user from exiting a site, computer system or network-connected location in order to compel the user's computer to continue communicating with, connecting to or displaying the content of the service, site or system.

7. Knowingly obtaining any information that is required by law to be kept confidential or any records that are not public records by accessing any computer, computer system or network that is operated by this state, a political subdivision of this state or a medical institution.

8. Knowingly accessing any computer, computer system or network or any computer software, program or data that is contained in a computer, computer system or network.

B. In addition to section 13-109, a prosecution for a violation of this section may be tried in any of the following counties:

1. The county in which the victimized computer, computer system or network is located.
2. The county in which the computer, computer system or network that was used in the commission of the offense is located or in which any books, records, documents, property, financial instruments, computer software, data, access devices or instruments of the offense were used.
3. The county in which any authorized user was denied service or in which an authorized user's service was interrupted.
4. The county in which critical infrastructure resources were tampered with or affected.

C. On conviction of a violation of this section, the court shall order that any computer system or instrument of communication that was owned or used exclusively by the defendant and that was used in the commission of the offense be forfeited and sold, destroyed or otherwise properly disposed.

D. A violation of subsection A, paragraph 6 of this section constitutes an unlawful practice under section 44-1522 and is in addition to all other causes of action, remedies and penalties that are available to this state. The attorney general may investigate and take appropriate action pursuant to title 44, chapter 10, article 7.

E. Computer tampering pursuant to subsection A, paragraph 1 of this section is a class 3 felony. Computer tampering pursuant to subsection A, paragraph 2, 3 or 4 of this section is a class 4 felony, unless the computer, computer system or network tampered with is a critical infrastructure resource, in which case it is a class 2 felony. Computer tampering pursuant to subsection A, paragraph 5 of this section is a class 5 felony. Computer tampering pursuant to subsection A, paragraph 7 or 8 of this section is a class 6 felony.

#### 13-2316.01. Unlawful possession of an access device; classification

A. A person commits unlawful possession of an access device by knowingly possessing, trafficking in, publishing or controlling an access device without the consent of the issuer, owner or authorized user and with the intent to use or distribute that access device.

B. The possession, trafficking, publishing or control of five or more access devices without the consent of the issuer, owner or authorized user may give rise to an inference that the person possessing, trafficking in, publishing or controlling the access devices intended to use or distribute the devices.

C. Unlawful possession of one hundred or more access devices is a class 4 felony. Unlawful possession of five or more but fewer than one hundred access devices is a class 5 felony. Unlawful possession of fewer than five access devices is a class 6 felony.

#### 13-2316.02. Unauthorized release of proprietary or confidential computer security information; exceptions; classification

A. A person commits unauthorized release of proprietary or confidential computer security information by communicating, releasing or publishing proprietary or confidential computer

security information, security-related measures, algorithms or encryption devices relating to a particular computer, computer system or network without the authorization of its owner or operator.

B. The following are exempt from this section:

1. The release by publishers, vendors, users and researchers of warnings or information about security measures or defects in software, hardware or encryption products if the release of the warnings or information is not specific to a particular owner's or operator's computer, computer system or network.
2. The release of security information among the authorized users of a computer, computer system or network or the notification to the owner or operator of a computer, computer system or network of a perceived security threat.
3. The release of security information in connection with the research, development and testing of security-related measures, products or devices if the release of the security information is not specific to a particular owner's or operator's computer, computer system or network.

C. At the conclusion of any grand jury, hearing or trial, the court shall preserve pursuant to section 44-405 any proprietary computer security information that was admitted in evidence or any portion of a transcript that contains information relating to proprietary computer security information.

D. Unauthorized release of proprietary or confidential computer security information is a class 6 felony, unless the security information relates to a critical infrastructure resource, in which case it is a class 4 felony.

### 13-3001. [Definitions](#)

In this chapter, unless the context otherwise requires:

1. "Aural transfer" means a communication containing the human voice at any point between and including the point of origin and the point of reception.
2. "Child monitoring device" means a device that is capable of transmitting an audio or audiovisual signal and that is installed or used in a residence for child supervision or safety monitoring by any parent, guardian or other responsible person in the person's own residence.
3. "Communication service provider" means any person who is engaged in providing a service that allows its users to send or receive oral, wire or electronic communications or computer services.
4. "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature that is transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system but that does not include any of the following:
  - (a) Any wire or oral communication.
  - (b) Any communication made through a tone-only paging device.
  - (c) Any communication from a tracking device.
5. "Electronic communication system" means any communication or computer facilities or related electronic equipment for the transmission, processing or electronic storage of electronic communications.

6. "Electronic storage" means either of the following:
- (a) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission.
  - (b) Any storage of the communication by an electronic communication service provider for purposes of backup protection of the communication.
7. "Intercept" means the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device.
8. "Oral communication" means a spoken communication that is uttered by a person who exhibits an expectation that the communication is not subject to interception under circumstances justifying the expectation but does not include any electronic communication.
9. "Pen register" means a device or process that records or decodes electronic or other impulses that identify the numbers dialed or otherwise transmitted on the telephone line or communication facility to which the device is attached or the dialing, routing, addressing or signaling information that is transmitted by an instrument or facility from which a wire or electronic communication is transmitted but does not include the contents of any communication, except when used in connection with a court order issued pursuant to section 13-3010 or 13-3012. A pen register does not include a publicly available device or process that is otherwise not unlawful.
10. "Person" means any individual, enterprise, public or private corporation, unincorporated association, partnership, firm, society, governmental authority or entity, including the subscriber to the communication service involved, and any law enforcement officer.
11. "Readily accessible to the general public" means a radio communication that is not:
- (a) Scrambled or encrypted.
  - (b) Transmitted using modulation techniques with essential parameters that have been withheld from the public to preserve the privacy of the communication.
  - (c) Carried on a subcarrier or other signal subsidiary to a radio transmission.
  - (d) Transmitted over a communication system provided by a common carrier, unless the communication is a tone-only paging system communication.
  - (e) Transmitted on frequencies allocated under part 25, subpart D, E or F or part 74 or part 94 of the rules of the federal communications commission. If a communication transmitted on a frequency allocated under part 74 is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication system by radio.
12. "Remote computing service" means providing to the public any computer storage or processing services by means of an electronic communication system.
13. "Trap and trace device" means a device or process 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 or the dialing, routing, addressing and signaling information that is reasonably likely to identify the source of a wire or electronic communication but does not include the content of any communication, except when used in connection with a court order issued pursuant to section 13-3010 or 13-3012. A trap and trace device does not include a publicly available device or process that is otherwise not unlawful.
14. "Wire communication" means any aural transfer that is made in whole or in part through the use of facilities for the transmission of communications by the aid of any wire, cable or other like connection between the point of origin and the point of reception, including the use

of a connection in a switching station, and that is furnished or operated by any person who is engaged in providing or operating the facilities for the transmission of communications.

13-3002. False or forged messages; classification

A. It is unlawful for a person:

1. Knowingly to send to any person by telegraph or telephone a false or forged message, purporting to be from a telegraph or telephone office, or from any other person.
2. Knowingly to deliver or cause to be delivered to any person a false or forged message, falsely purporting to have been received by telegraph or telephone.
3. To furnish or conspire to furnish, or cause to be furnished to an agent, operator or employee, to be sent by telegraph or telephone, or to be delivered, a message, knowing it is false or forged, with intent to deceive, injure or defraud another.

B. A person who violates any provision of this section is guilty of a class 6 felony.

13-3003. Opening, reading or publishing sealed letter of another without authority; classification

A person who knowingly opens or reads or causes to be read a sealed letter not addressed to himself, without being authorized so to do either by the writer of such letter, or by the person to whom it is addressed, or a person who, without like authority, publishes the contents of such letter, knowing it to have been unlawfully opened, is guilty of a class 2 misdemeanor.

13-3004. Sending threatening or anonymous letter; classification

A person who knowingly sends or delivers to another a letter or writing, whether subscribed or not, threatening to accuse him or another of a crime, or to expose or publish his failings or infirmities, and a writer or sender of an anonymous letter or writing calculated to create distrust of another or tending to impute dishonesty, want of chastity, drunkenness or any crime or infirmity to the receiver of the letter or to any other person, is guilty of a class 2 misdemeanor.

13-3005. Interception of wire, electronic and oral communications; installation of pen register or trap and trace device; classification; exceptions

A. Except as provided in this section and section 13-3012, a person is guilty of a class 5 felony who either:

1. Intentionally intercepts a wire or electronic communication to which he is not a party, or aids, authorizes, employs, procures or permits another to so do, without the consent of either a sender or receiver thereof.
2. Intentionally intercepts a conversation or discussion at which he is not present, or aids, authorizes, employs, procures or permits another to so do, without the consent of a party to such conversation or discussion.
3. Intentionally intercepts the deliberations of a jury or aids, authorizes, employs, procures or permits another to so do.

B. Except as provided in sections 13-3012 and 13-3017, a person who intentionally and without lawful authority installs or uses a pen register or trap and trace device on the

telephone lines or communications facilities of another person which are utilized for wire or electronic communication is guilty of a class 6 felony.

[13-3006. Divulging communication service information; classification; exception](#)

A person is guilty of a class 6 felony who either:

1. Intentionally and without lawful authority obtains any knowledge of the contents of a wire or electronic communication by connivance with a communication service provider or its officer or employee.
2. Is a communications service provider, officer or employee of a communications service provider and intentionally divulges to anyone but the person for whom it was intended, except with the permission of the sender or the person for whom it was intended or in any case covered by the exemption in section 13-3012, the contents or the nature of a wire or electronic communication entrusted to the communications service provider for transmission or delivery.

[13-3008. Possession of interception devices; classification](#)

A. It is unlawful for a person to have in his possession or control any device, contrivance, machine or apparatus designed or primarily useful for the interception of wire, electronic or oral communications as defined in section 13-3001 with the intent to unlawfully use or employ or allow the device, contrivance, machine or apparatus to be used or employed for the interception, or having reason to know the device, contrivance, machine or apparatus is intended to be so used.

B. All property possessed or controlled by any person in violation of this section is subject to seizure and forfeiture pursuant to chapter 39 of this title.

C. A person who violates this section is guilty of a class 6 felony.

[13-3009. Duty to report to law enforcement officers; classification](#)

It shall be the duty of every communications service provider and its officers and employees to report any violation of sections 13-3005, 13-3006 and 13-3008 coming within their knowledge to the county attorney having jurisdiction and to the attorney general. Any intentional violation of this section is a class 3 misdemeanor.

[13-3010. Ex parte order for interception; definition](#)

A. On application of a county attorney, the attorney general or a prosecuting attorney whom a county attorney or the attorney general designates in writing, any justice of the supreme court, judge of the court of appeals or superior court judge may issue an ex parte order for the interception of wire, electronic or oral communications if there is probable cause to believe both:

1. A crime has been, is being or is about to be committed.
2. Evidence of that crime or the location of a fugitive from justice from that crime may be obtained by the interception.

B. An application under subsection A shall be made in writing and upon the oath or affirmation of the applicant. It shall include:

1. The name and title of the applicant.
  2. A full and complete statement of the facts and circumstances relied upon by the applicant, including the supporting oath or affirmation of the investigating peace officer of this state or any political subdivision of this state to justify the officer's belief that an order should be issued. The statement shall include:
    - (a) Details as to the particular crime that has been, is being or is about to be committed.
    - (b) The identity of the person, if known, committing the offense and whose communications are to be intercepted.
    - (c) A particular description of the type of communications sought to be intercepted.
    - (d) A particular description of the nature, identification and location of the communication facility from which or the place where the communication is to be intercepted. If the identification or specific description of the communication facility from which or the place where the communication is to be intercepted is not practical, the affidavit in support of the application must state why:
      - (i) Specification is impractical.
      - (ii) Interception from any facility or at any place where the communication may occur is necessary.
  3. A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous.
  4. A statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that authorization to intercept should not automatically terminate when the described type of communication has been first obtained, the statement shall include a particular description of facts establishing probable cause to believe that additional communications of the same type will occur after the communication has been first obtained.
  5. A full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each application.
  6. If the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.
- C. Upon proper application, a judge may enter an ex parte order authorizing interception, as requested or with any appropriate modifications, if the judge determines on the basis of the facts submitted by the applicant that:
1. There is probable cause to believe that a person is committing, has committed or is about to commit a particular crime.
  2. There is probable cause to believe that particular communications concerning that offense will be obtained through the interception.
  3. Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.

4. There is probable cause to believe any of the following:

(a) Wire or electronic communications concerning the offense are being made or are about to be made by the person over the communication facilities for which interception authority is granted.

(b) Oral communications concerning the offense are being made or are about to be made by the person in the location for which interception authority is granted.

(c) Communications concerning the offense are being made or are about to be made by the person in different and changing locations, or from different and changing facilities.

D. Each order authorizing the interception of any wire, electronic or oral communication shall specify all of the following:

1. The identity of the person, if known, whose communications are to be intercepted.

2. The nature and location of the communication facilities as to which or the place where authority to intercept is granted. If authority is granted to intercept communications of a person wherever that person is located or from whatever communication facility is used, the order shall so state and shall include any limitations imposed by the authorizing judge as to location, time or manner of the interception. The order shall state that the interception shall not begin until the facilities from which or the place where the communication is to be intercepted is ascertained by the person implementing the interception order.

3. A particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates.

4. The identity of the agency authorized to intercept the communications and of the person authorizing the application.

5. The period of time during which the interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

6. That the authorization for interception be executed as soon as practicable, that it be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this section and that it terminate upon attainment of the authorized objective or on the date specified, whichever comes first.

7. That entry may be made to service, install or remove interception devices or equipment if entry is necessary to effect the interception.

E. An order that is entered under this section may not authorize the interception of any wire or oral communication for any period that is longer than is necessary to achieve the objective of the authorization and that exceeds thirty days. This thirty day period begins on the earlier of the day on which the interception actually begins under the order or ten days after the order is signed. The court may grant extensions of any order if an application for an extension is made pursuant to subsection A and the court makes the findings required by subsection C. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and shall not exceed thirty days.

F. Any ex parte order for interception, together with the papers on which the application was based, shall be delivered to and retained by the applicant during the duration of the interception as authority for the interception authorized in the order. The justice or judge issuing the order shall retain a true copy of the order at all times.

G. Within ten days after the termination of the authorized interception, applications made and orders granted under this section shall be returned to and sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. The applications and orders shall be disclosed only on a showing of good cause before a judge of competent jurisdiction or as otherwise provided.

H. If possible, the contents of any communication that is intercepted by any means authorized by this section shall be recorded on any tape, electronic, wire or other comparable device. The recording of the contents of any wire, electronic or oral communication under this subsection shall be done in such a way as will protect the recording from editing or alterations. Within ten days after the termination of the authorized interception, the recordings shall be made available to the judge who issued the order and shall be sealed under the judge's directions. Custody of the recordings shall be maintained pursuant to court order. The recordings shall be kept for ten years and shall not be destroyed except on an order of the issuing judge or another judge of competent jurisdiction.

I. Within ninety days after an application under subsection A is denied, or the period of an order or any extension expires, the issuing or denying judge shall serve the persons named in the order or application and any other parties to the intercepted communications as the judge may determine the interests of justice require with an inventory, including notice of all of the following:

1. The fact of the entry of the order or the application.
2. The date of the entry and the period of authorized interception, or the denial of the application.
3. The fact that during the period of authorized interception wire, electronic or oral communications were or were not intercepted. On motion, the judge may make available to the person or the person's attorney for inspection such portions of the intercepted communications, applications and order as the judge determines to be in the interest of justice. On an ex parte showing of good cause to the judge, the serving of the notice required by this subsection may be postponed.

J. On request of the applicant, any order authorizing interception shall direct that the communication service provider, landlords, custodians or other persons furnish the applicant with all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that these persons are according the person whose communications are to be intercepted.

K. The order may require written reports to be made to the issuing judge at specified intervals showing the progress made toward achieving the authorized objective and the need for continued interception.

L. Any order authorizing the interception of wire communications pursuant to this chapter is also deemed to authorize the interception of any electronic communication that may be made over the same equipment or by the same facility.

M. If the intercepted communication is in a code or foreign language and an expert in that code or foreign language is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after the interception.

N. An interception under this chapter may be conducted in whole or in part by government personnel or by an individual operating under a contract with the government or acting under the supervision of a law enforcement officer who is authorized to conduct the interception.

O. The applicant is responsible for providing to the administrative office of the United States courts all reports on applications for or interceptions of wire, electronic or oral communications that are required by federal statutes.

P. For the purposes of this section, "crime" means murder, gaming, kidnapping, robbery, bribery, extortion, theft, an act in violation of chapter 23 of this title, dealing in narcotic drugs, marijuana or dangerous drugs, sexual exploitation of children in violation of chapter 35.1 of this title or any felony that is dangerous to life, limb or property. Crime includes conspiracy to commit any of the offenses listed in this subsection.

#### 13-3011. Disclosing confidential information relating to ex parte order; exceptions; classification

A. Except in any trial, hearing or other judicial proceeding, a person shall not knowingly disclose to another person any information concerning either:

1. The application for or the granting or denial of orders for the interception or installation of a pen register or trap and trace device or a request for the preservation of records or evidence pursuant to section 13-3016 or a subpoena issued pursuant to section 13-3018.
2. The identity of the person or persons whose communications are the subject of an ex parte order, subpoena or records preservation request granted pursuant to sections 13-3010, 13-3015, 13-3016, 13-3017 and 13-3018.

B. Subsection A of this section does not apply to the disclosure of information to the communication service provider whose facilities are involved or to an employee or other authorized agent of the county attorney, attorney general or law enforcement agency that applies for an order permitting interception or installation of a pen register or trap and trace device or who requests the preservation of records or evidence pursuant to section 13-3016 or a subpoena issued pursuant to section 13-3018.

C. Notwithstanding subsection A of this section, a peace officer or prosecuting attorney who obtains knowledge of the contents of a wire, electronic or oral communication as authorized by sections 13-3010, 13-3015, 13-3016, 13-3017 and 13-3018 or evidence derived from that knowledge may:

1. Disclose the contents of the communication to a peace officer or prosecuting attorney to the extent the disclosure is appropriate to the proper performance of the official duties of the peace officer or prosecuting attorney making or receiving the disclosure.
2. Use the contents of the communication to the extent that the use is appropriate to the proper performance of the official duties of the peace officer or prosecuting attorney.

D. A person who violates this section is guilty of a class 1 misdemeanor.

#### 13-3012. Exemptions

The following are exempt from the provisions of this chapter:

1. The interception of wire, electronic or oral communications, the installation and operation of a pen register or trap and trace device, the providing of information, facilities or technical

assistance to an investigative or law enforcement officer pursuant to a subpoena or an ex parte order granted pursuant to sections 13-3010, 13-3015, 13-3016, 13-3017 and 13-3018 or an emergency interception made in good faith pursuant to section 13-3015, including any of the foregoing acts by a communication service provider or its officers, agents or employees.

2. The normal use of services, equipment and facilities that are provided by a communication service provider pursuant to tariffs that are on file with the Arizona corporation commission or the federal communications commission and the normal functions of any operator of a switchboard.

3. Any officer, agent or employee of a communication service provider who performs acts that are otherwise prohibited by this article in providing, constructing, maintaining, repairing, operating or using the provider's services, equipment or facilities, protecting the provider's service, equipment and facilities from illegal use in violation of tariffs that are on file with the Arizona corporation commission or the federal communications commission and protecting the provider from the commission of fraud against it.

4. Providing requested information or any other response to a subpoena or other order that is issued by a court of competent jurisdiction or on demand of any other lawful authority.

5. The interception of wire or electronic communications or the use of a pen register or trap and trace device by a communication service provider or by a person providing technical assistance at the request of the communication service provider if the interception or use either:

(a) Relates to the operation, maintenance and testing of that service, the protection of the rights or property of the provider or the protection of users of that service from fraudulent, abusive or unlawful use of that service.

(b) Records the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the communication or a user of that service from fraudulent, unlawful or abusive use of that service.

6. The interception of any radio communication that is transmitted:

(a) By any station for the use of the general public or if the transmission relates to ships, aircraft, vehicles or persons in distress.

(b) By any government, law enforcement, civil defense, private land mobile or public safety communication system, including police and fire systems, and that is readily accessible to the general public.

(c) By any station that operates on an authorized frequency within the bands that are allocated to the amateur, citizens band or general mobile radio services.

(d) By any marine or aeronautical communications system.

(e) Through a system using frequencies that are monitored by persons who are engaged in the provision or the use of the system or by other persons who use the same frequency if the communication is not scrambled or encrypted.

7. The interception of wire or electronic communication if the transmission is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of the interference.

8. The use of a pen register or trap and trace device by a communication service provider for billing or recording as an incident to billing for communication services, or for cost accounting or other like purposes in the ordinary course of business.
9. The interception of any wire, electronic or oral communication by any person, if the interception is effected with the consent of a party to the communication or a person who is present during the communication, or the installation of a pen register or trap and trace device with the consent of a user or subscriber to the service.
10. Divulging the contents of a wire or electronic communication and any related records or information to a law enforcement agency by a remote computing service or communication service provider, officer or employee if either:
  - (a) The contents, records or information were lawfully or inadvertently obtained by the service provider and appear to pertain to the commission of a crime.
  - (b) The provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies the disclosure of the contents, records or information without delay.
11. Divulging records or other information that pertains to a customer or subscriber by a remote computing service or communication service provider, other than the contents of a communication, either:
  - (a) As authorized by section 13-3016.
  - (b) With the customer's or subscriber's consent.
  - (c) As may be necessary incident to the rendition of the service or for the protection of the rights or property of the provider of that service.
  - (d) To any person other than a governmental agency.
12. The interception or access of an electronic communication that is made through an electronic communication system and that is configured so that the electronic communication is readily accessible to the general public.
13. For other users of the same frequency to intercept a radio communication that is made through a system that uses frequencies that are monitored by individuals who provide or use the system, if the communication is not scrambled or encrypted.
14. The interception of oral communications by means of a child monitoring device.

### 13-3013. [Defenses](#)

The following constitute a complete defense to any civil or criminal action brought under this chapter or under any other law:

1. A good faith reliance on an ex parte order or subpoena that is issued pursuant to section 13-3010, 13-3015, 13-3016, 13-3017 or 13-3018.
2. Providing information pursuant to section 13-3012.
3. Providing assistance, information or facilities for an emergency interception pursuant to section 13-3015.
4. Disclosing stored electronic communications or preserving records, content or evidence pursuant to section 13-3016.
5. Providing equipment, information or assistance to render stored electronic communications in a usable form pursuant to section 13-3016.

[13-3014. Communication service provider; right to compensation](#)

Any communication service provider who furnishes information, facilities or technical assistance pursuant to this chapter shall be compensated therefor by the applicant at the prevailing rates.

[13-3015. Emergency interception](#)

A. Notwithstanding any other provision of this chapter, if the attorney general or a county attorney or such prosecuting attorneys as they may designate in writing reasonably determines that an emergency situation exists involving immediate danger of death or serious physical injury to any person, and that such death or serious physical injury may be averted by interception of wire, electronic or oral communications before an order authorizing such interception can be obtained, the attorney general or a county attorney or his designee may specially authorize a peace officer or law enforcement agency to intercept such wire, electronic or oral communications.

B. The attorney general or county attorney or his designee specially authorizing an emergency interception pursuant to subsection A of this section shall apply for an order authorizing the interception, in accordance with the provisions of section 13-3010. The application shall be made as soon as practicable, and in no event later than forty-eight hours after commencement of the emergency interception. The application shall include an explanation and summary of any interception of communications occurring before the application for authorization.

C. If the prosecuting attorney fails to obtain an authorization within forty-eight hours after commencement of the emergency interception, or if authorization to intercept communications is denied, the interception shall immediately terminate and any communications intercepted without judicial authorization may not be used as evidence in any criminal or civil proceeding against any person. In either event, the prosecuting attorney shall furnish to the court an inventory of any communications intercepted, for service pursuant to the provisions of section 13-3010, subsection I. The provisions of this subsection do not prohibit the use as evidence of any communications intercepted without judicial authorization against the persons conducting or authorizing the interceptions if such interceptions were not made in good faith reliance on this section.

[13-3016. Stored oral, wire and electronic communications; agency access; backup preservation; delayed notice; records preservation request; violation; classification](#)

A. This section applies to oral, wire and electronic communications that are entrusted to a communication service provider or remote computing service solely for the purpose of transmission, storage or processing. Oral, wire and electronic communications that are in the possession of a person who is entitled to access the contents of such communications for any purpose other than transmission, storage or processing are ordinary business records that may be obtained by subpoena or court order.

B. An agency or political subdivision of this state may require the disclosure by a communication service provider or remote computing service of the contents of an oral, wire

or electronic communication that has been in electronic storage for one hundred eighty days or less in one of the following ways:

1. Without prior notice to the subscriber or party, by obtaining a search warrant issued pursuant to chapter 38, article 8 of this title.
2. With prior notice to the subscriber or party, by serving a subpoena, except that notice may be delayed pursuant to subsection D of this section.
3. With prior notice to the subscriber or party, by obtaining a court order on an application and certification that contains specific and articulable facts showing that there are reasonable grounds to believe that the communication content sought is relevant to an ongoing criminal investigation, except that notice may be delayed pursuant to subsection D of this section.

C. An agency or political subdivision of this state may require the disclosure by a communication service provider or remote computing service of the contents of an oral, wire or electronic communication that has been in electronic storage for more than one hundred eighty days in one of the following ways:

1. Without notice to the subscriber or party, by obtaining a search warrant issued pursuant to chapter 38, article 8 of this title.
2. With prior notice to the subscriber or party, by serving a subpoena, except that notice may be delayed pursuant to subsection D of this section.
3. With prior notice to the subscriber or party, by obtaining a court order on an application and certification that contains specific and articulable facts showing that there are reasonable grounds to believe that the communication content sought is relevant to an ongoing criminal investigation, except that notice may be delayed pursuant to subsection D of this section.

D. Except as provided in subsection E of this section, the notice to the subscriber or party that is required by this section may be delayed for a period of not to exceed ninety days under any of the following circumstances:

1. If the applicant for a search warrant or court order pursuant to this section requests a delay of notification and the court finds that delay is necessary to protect the safety of any person or to prevent flight from prosecution, tampering with evidence, intimidation of witnesses or jeopardizing an investigation.
2. If the investigator or prosecuting attorney proceeding by subpoena executes a written certification that there is reason to believe that notice to the subscriber or party may result in danger to the safety of any person, flight from prosecution, tampering with evidence, intimidation of witnesses or jeopardizing an investigation. The agency shall retain a true copy of the certification with the subpoena.

E. If further delay of notification is necessary, extensions of up to ninety days each may be obtained by application to the court or certification pursuant to subsection D of this section.

F. Any agency acting pursuant to this section may apply for a court order directing the communication service provider or remote computing service not to notify any other person of the existence of the subpoena, court order or warrant for such period as the court deems appropriate. The court shall grant the application if it finds that there is reason to believe that notice may cause an adverse result described in subsection D of this section. A person who violates an order issued pursuant to this subsection is guilty of a class 1 misdemeanor.

G. On the expiration of any period of delay under this section, the agency shall deliver to the subscriber or party a copy of the process used and notice including:

1. That information was requested from the service provider.
2. The date on which the information was requested.
3. That notification to the subscriber or party was delayed.
4. The identity of the court or agency ordering or certifying the delay.
5. The provision of this section by which delay was obtained.
6. That any challenge to the subpoena or order must be filed within fourteen days.

H. On the request of an agency or political subdivision of this state, a communication service provider or remote computing service shall take all necessary steps to preserve records, communication content and other evidence in its possession pending the issuance of a court order or other process. The communication service provider or remote computing service shall retain the preserved records, communication content and other evidence for ninety days. On the renewed request of an agency or political subdivision, the preservation period may be extended for an additional ninety days. Except as provided in section 13-3011, a person shall not notify the subscriber or party during the period of the preservation request.

[13-3017. Ex parte order for pen register or trap and trace device](#)

A. Any prosecuting attorney or investigating peace officer of this state or its political subdivisions may apply to any justice of the supreme court, judge of the court of appeals, judge of the superior court or magistrate for an ex parte order authorizing the installation and use of a pen register or a trap and trace device. The application shall be made in writing and under oath and shall state:

1. The name and title of the applicant.
2. The attributes of the communication, including the number or other identifier, the identity, if known, of the subscriber and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, if the order authorizes the installation of a trap and trace device, the geographic limits of the order.
3. A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation.
4. A statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.

B. On proper application pursuant to subsection A, the judge shall issue an ex parte order authorizing the installation and use of a pen register or trap and trace device or process if the judge finds that the applicant has certified that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation. On service, the order applies to any person or entity that provides wire or electronic communication service in this state or that does business in this state and whose assistance may facilitate the execution of the order. If an order is served on any person or entity that is not specifically named in the order and on request of the person or entity, the prosecuting attorney or peace officer who serves the order shall provide written or electronic certification that the order applies to the person or entity being served. An order that is issued under this subsection shall specify all of the following:

1. The identity, if known, of the subscriber of the communication service or telephone line to which the pen register or trap and trace device is to be attached or applied.
  2. The attributes of the communication to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, if the order authorizes the installation of a trap and trace device, the geographic limits of the order.
  3. A statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates.
  4. That, on the request of the applicant, the communication service provider shall furnish information, facilities and technical assistance necessary to accomplish the installation of the pen register or trap and trace device and to identify subscribers of any communication facility or telephone number obtained by operation of such device.
- C. An order that is issued under this section authorizes the installation and use of a pen register or trap and trace device for a period of not to exceed sixty days. Extensions of the order may be granted, but only on an application and judicial finding pursuant to subsections A and B. The period of each extension granted shall not exceed sixty days.

**13-3018. [Communication service records; subpoenas; application; certification; definition](#)**

- A. This section applies to all communication service providers that do business in this state or that furnish communication services to persons within this state.
- B. The prosecutor may issue a subpoena duces tecum to a communication service provider in order to obtain communication service records in connection with a criminal investigation or prosecution for any offense in which a prosecutor suspects that a computer or network was used. This subsection does not prevent the prosecutor from obtaining a grand jury subpoena duces tecum.
- C. The prosecutor who issues a subpoena pursuant to this section shall certify in the body of the subpoena that the information likely to be obtained is relevant to an ongoing criminal investigation.
- D. An authorized representative of a communication service provider may certify communication service records that are obtained by subpoena if all of the following apply:
1. The records are the regular communication service records that are used and kept by the communication service provider.
  2. The records are made at or near the time the underlying communications occur in the ordinary course of business.
  3. The authorized representative certifies that the record produced in response to the subpoena is an accurate copy of the communication service provider records.
- E. Certified communication service records that are obtained by subpoena may be introduced in evidence at a hearing or trial and constitute prima facie evidence of the facts contained in the records.
- F. If a certification of communication service provider records is acknowledged by any notary or other officer who is authorized by law to take acknowledgments, the certification shall be received in evidence without further proof of its authenticity.

G. For the purposes of this section, "communication service records" includes subscriber information, including name, billing or installation address, length of service, payment method, telephone number, electronic account identification and associated screen names, toll bills or access logs, records of the path of an electronic communication between the point of origin and the point of delivery and the nature of the communication service provided, such as caller identification, automatic number identification, voice mail, electronic mail, paging or other service features. Communication service records do not include the content of any stored oral, wire or electronic communication.

13-3019. Surreptitious photographing, videotaping, filming or digitally recording; exemptions; violation; classification; definitions

A. It is unlawful for any person to knowingly photograph, videotape, film, digitally record or by any other means use a device to secretly view or record another person without that person's consent under both of the following circumstances:

1. In a restroom, bathroom, locker room, bedroom or other location where the person has a reasonable expectation of privacy.
2. While the person is urinating, defecating, dressing, undressing, nude or involved in sexual intercourse or sexual contact.

B. It is unlawful to disclose, display, distribute or publish a photograph, videotape, film or digital recording made in violation of subsection A of this section without the consent of the person depicted.

C. This section does not apply to:

1. Photographing, videotaping, filming or digitally recording for security purposes where notice of the use of photographing, videotaping, filming or digital recording equipment is clearly posted in the location.
2. Photographing, videotaping, filming or digitally recording by correctional officials for security reasons or in connection with the investigation of alleged misconduct of persons on the premises of a jail or prison.
3. Photographing, videotaping, filming or digitally recording by law enforcement officers pursuant to an investigation, which is otherwise lawful.
4. The use of a child monitoring device as defined in section 13-3001.

D. A violation of subsection A or B of this section is a class 5 felony.

E. For the purposes of this section "sexual contact" and "sexual intercourse" have the same meanings prescribed in section 13-1401.