## **CHAPTER 626A**

## WIRE, ELECTRONIC, OR ORAL COMMUNICATIONS; INTERCEPTION

626A.01	DEFINITIONS.	626A.25	INJUNCTION AGAINST ILLEGAL INTERCEPTION.
626A.02	INTERCEPTION AND DISCLOSURE OF WIRE, ELECTRONIC, OR ORAL COMMUNICATIONS	ELECTRONIC COMMUNICATION SERVICE; REMOTE COMPUTING SERVICE	
626A.03	PROHIBITED.  MANUFACTURE, DISTRIBUTION, POSSESSION, AND ADVERTISING OF WIRE, ELECTRONIC, OR ORAL COMMUNICATION INTERCEPTING DEVICES PROHIBITED.	626A.26	UNLAWFUL ACCESS TO STORED COMMUNICATIONS.
		626A.27	DISCLOSURE OF CONTENTS.
		626A.28	REQUIREMENTS FOR GOVERNMENTAL ACCESS.
626A.04	PROHIBITION OF USE AS EVIDENCE OF INTERCEPTED WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS.	626A.29	BACKUP PRESERVATION.
		626A.30	DELAYED NOTICE.
626A.05	AUTHORIZATION FOR INTERCEPTION OF WIRE, ELECTRONIC, OR ORAL COMMUNICATIONS.	626A.31	COST REIMBURSEMENT.
		626A.32	CIVIL ACTION.
626A.06	PROCEDURE FOR INTERCEPTION OF WIRE, ELECTRONIC, OR ORAL COMMUNICATIONS.	626A.33	EXCLUSIVITY OF REMEDIES.
		626A.34	DEFINITIONS.
626A.065	EMERGENCY INTERCEPTION.	PEN REGISTER; TRAP AND TRACE DEVICE; MOBILE	
626A.07	RETURN FILED BY OFFICER.		TRACKING DEVICE
626A.08	PRESERVATION OF MATERIAL OBTAINED, APPLICATIONS AND ORDERS; DESTRUCTION.	626A.35	GENERAL PROHIBITION ON PEN REGISTER, TRAP AND TRACE DEVICE, AND MOBILE TRACKING
626A.09	AUTHORIZATION FOR DISCLOSURE AND USE OF INTERCEPTED WIRE, ELECTRONIC, OR ORAL COMMUNICATIONS.	626A.36	DEVICE USE; EXCEPTION.  APPLICATION FOR ORDER FOR PEN REGISTER, TRAP AND TRACE DEVICE, OR MOBILE
626A.10	NOTICE TO DEFENDANT.		TRACKING DEVICE.
626A.11	ADMISSIBILITY OF INTERCEPTED EVIDENCE.	626A.37	ISSUANCE OF ORDER FOR PEN REGISTER, TRAP
626A.12	MOTION TO SUPPRESS EVIDENCE.		AND TRACE DEVICE, OR MOBILE TRACKING DEVICE.
626A.13	CIVIL REMEDIES.	626A.38	REGISTER, TRAP AND TRACE DEVICE, OR
626A.14	OBTAINING TELEPHONE AND TELEGRAPH		MOBILE TRACKING DEVICE.
	COMPANY INFORMATION.	626A.381	SERVICE OR NOTICE; INVENTORY.
626A.15	DUTY TO REPORT VIOLATIONS.	626A.39	DEFINITIONS.
626A.16	TELEPHONE COMPANY TO AID IN DETECTION.	626A.391	CIVIL ACTION; DAMAGES.
626A.17	REPORT CONCERNING INTERCEPTION OF COMMUNICATIONS.		GENERALLY
626A.18	ILLEGAL TRANSFERS OF INTERCEPTING DEVICES.	626A.40	SUBJECT TO OTHER LAWS.
		626A.41	CITATION.
626A.19	FORFEITURES.	ELECTRONIC DEVICE; TRACKING WARRANT	
626A.20	SUSPENSION OR REVOCATION OF LICENSES.	626A.42	ELECTRONIC DEVICE LOCATION INFORMATION.

### 626A.01 DEFINITIONS.

Subdivision 1. **Terms.** As used in this chapter, the terms defined in this section have the meanings given them.

- Subd. 2. **Person.** "Person" means any individual, partnership, corporation, joint stock company, trust, or association, including but not limited to, the subscriber to the telephone or telegraph service involved and any law enforcement officer.
- Subd. 3. **Wire communication.** "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception, including the use of such connection in a switching station. "Wire communication" includes any electronic storage of the communication.

- Subd. 4. **Oral communication.** "Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but the term does not include any electronic communication.
- Subd. 5. **Intercept.** "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.
- Subd. 6. **Electronic, mechanical or other device.** "Electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, electronic, or oral communication other than:
- (1) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider or wire or electronic communications service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by a subscriber or user for connection to the facilities of service and used in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of duties;
  - (2) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;
- (3) that which is specifically designed to only record conversations to which the operator of the device is a party;
  - (4) that which is used in the normal course of broadcasting by radio or television; or
- (5) that which is otherwise commonly used for a purpose or purposes other than overhearing or recording conversations.

In determining whether a device which is alleged to be an electronic, mechanical, or other device is, in fact, such a device there shall be taken into account, among other things, the size, appearance, directivity, range, sensitivity, frequency, power, or intensity, and the representations of the maker or manufacturer as to its performance and use.

- Subd. 7. **Investigative or law enforcement officer.** "Investigative or law enforcement officer" means any officer of the United States or of a state or political subdivision thereof, or a University of Minnesota peace officer who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, or any attorney authorized by law to prosecute or participate in the prosecution of such offenses.
- Subd. 8. **Contents.** "Contents," when used with respect to any wire, electronic, or oral communication, includes any information concerning the substance, purport, or meaning of that communication.
- Subd. 9. **Aggrieved person.** "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.
- Subd. 10. **Manufacturer.** "Manufacturer" means any person who is engaged in the business of manufacturing electronic, mechanical or other devices, or who otherwise produces any such device for sale or distribution.
- Subd. 11. **Dealer.** "Dealer" means any person not a manufacturer who is engaged in the business of selling electronic, mechanical or other devices. The term "dealer" shall include wholesalers, retailers and dealers in used intercepting devices.
  - Subd. 12. **Bureau.** "Bureau" means the Bureau of Criminal Apprehension.

- Subd. 13. **Communications common carrier.** "Communications common carrier" means any individual, partnership, corporation, or association which provides telephone or telegraph service to subscribers or users pursuant to tariffs on file with the Minnesota Public Utilities Commission or the Federal Communications Commission.
- Subd. 14. **Electronic communication.** "Electronic communication" means transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system but does not include:
  - (1) a wire or oral communication;
  - (2) a communication made through a tone-only paging device; or
- (3) a communication from a tracking device, defined as an electronic or mechanical device which permits the tracking of the movement of a person or object.
  - Subd. 15. User. "User" means a person or entity who:
  - (1) uses an electronic communication service; and
  - (2) is duly authorized by the provider of the service to engage in the use.
- Subd. 16. **Electronic communications system.** "Electronic communications system" means a wire, radio, electromagnetic, photooptical, or photoelectronic facility for the transmission of electronic communications, and a computer facility or related electronic equipment for the electronic storage of communications.
- Subd. 17. **Electronic communication service.** "Electronic communication service" means a service that provides to users of the service the ability to send or receive wire or electronic communications.
- Subd. 18. **Readily accessible to the general public.** "Readily accessible to the general public" means, with respect to a radio communication, that the communication is not:
  - (1) scrambled or encrypted;
- (2) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of the communication;
  - (3) carried on a subcarrier or other signal subsidiary to a radio transmission;
- (4) transmitted over a communication system provided by a common carrier, unless the communication is a tone-only paging system communication; or
- (5) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of title 47 of the Code of Federal Regulations, unless in the case of a communication transmitted on a frequency allocated under part 74 of title 47 of the Code of Federal Regulations that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio.
  - Subd. 19. Electronic storage. "Electronic storage" means:
- (1) a temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission of the communication; and
- (2) a storage of communication described in clause (1) by an electronic communication service for purposes of backup protection of the communication.

Subd. 20. **Aural transfer.** "Aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

**History:** 1969 c 953 s 1; 1977 c 82 s 6; 1980 c 614 s 123; 1986 c 444; 1988 c 577 s 1-13,62; 1989 c 336 art 2 s 8; 1990 c 455 s 1.2; 1991 c 199 art 2 s 1

## 626A.02 INTERCEPTION AND DISCLOSURE OF WIRE, ELECTRONIC, OR ORAL COMMUNICATIONS PROHIBITED.

Subdivision 1. **Offenses.** Except as otherwise specifically provided in this chapter any person who:

- (1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, electronic, or oral communication;
- (2) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:
- (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
- (ii) such device transmits communications by radio, or interferes with the transmission of such communication;
- (3) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this subdivision; or
- (4) intentionally uses, or endeavors to use, the contents of any wire, electronic, or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire, electronic, or oral communication in violation of this subdivision; shall be punished as provided in subdivision 4, or shall be subject to suit as provided in subdivision 5.
- Subd. 2. **Exemptions.** (a) It is not unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.
- (b) It is not unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of employment and in discharge of the monitoring responsibilities exercised by the commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.
- (c) It is not unlawful under this chapter for a person acting under color of law to intercept a wire, electronic, or oral communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.
- (d) It is not unlawful under this chapter for a person not acting under color of law to intercept a wire, electronic, or oral communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is

intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the United States or of any state.

- (e) It is not a violation of this chapter for a person:
- (1) to intercept or access an electronic communication made through an electronic communication system that is configured so that the electronic communication is readily accessible to the general public;
  - (2) to intercept any radio communication that is transmitted:
- (i) by a station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;
- (ii) by a governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;
- (iii) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
  - (iv) by a marine or aeronautical communications system;
  - (3) to engage in any conduct which:
  - (i) is prohibited by section 553 of title 47 of the United States Code; or
- (ii) is excepted from the application of section 605(a) of title 47 of the United States Code by section 605(b) of that title;
- (4) to intercept a wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or
- (5) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if the communication is not scrambled or encrypted.
  - (f) It is not unlawful under this chapter:
  - (1) to use a pen register or a trap and trace device as those terms are defined by section 626A.39; or
- (2) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful, or abusive use of the service.
- (g) It is not unlawful under this chapter for a person not acting under color of law to intercept the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit if the initial interception of the communication was obtained inadvertently.
- Subd. 3. **Disclosing communications.** (a) Except as provided in paragraph (b), a person or entity providing an electronic communications service to the public must not intentionally divulge the contents of any communication other than one to the person or entity, or an agent of the person or entity, while in transmission on that service to a person or entity other than an addressee or intended recipient of the communication or an agent of the addressee or intended recipient.

- (b) A person or entity providing electronic communication service to the public may divulge the contents of a communication:
  - (1) as otherwise authorized in subdivision 2, paragraph (a), and section 626A.09;
  - (2) with the lawful consent of the originator or any addressee or intended recipient of the communication;
- (3) to a person employed or authorized, or whose facilities are used, to forward the communication to its destination; or
- (4) that were inadvertently obtained by the service provider in the normal course of business if there is reason to believe that the communication pertains to the commission of a crime, if divulgence is made to a law enforcement agency.
- Subd. 4. **Penalties.** (a) Except as provided in paragraph (b) or in subdivision 5, whoever violates subdivision 1 shall be fined not more than \$20,000 or imprisoned not more than five years, or both.
- (b) If the offense is a first offense under paragraph (a) and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled or encrypted, then:
- (1) if the communication is not the radio portion of a cellular telephone communication, a public land mobile radio service communication, a cordless telephone communication transmitted between the cordless telephone handset and the base unit, or a paging service communication, and the conduct is not that described in subdivision 5, the offender shall be fined not more than \$3,000 or imprisoned not more than one year, or both; and
- (2) if the communication is the radio portion of a cellular telephone communication, a public land mobile radio service communication, a cordless telephone communication transmitted between the cordless telephone handset and the base unit, or a paging service communication, the offender shall be fined not more than \$500.
- (c) Conduct otherwise an offense under this subdivision that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted:
  - (1) to a broadcasting station for purposes of retransmission to the general public; or
- (2) as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls,

is not an offense under this subdivision unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

#### Subd. 5. Civil action. (a)(1) If the communication is:

- (i) a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or
- (ii) a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of title 47 of the Code of Federal Regulations and that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage

or private commercial gain, then the person who engages in such conduct is subject to suit by the county or city attorney in whose jurisdiction the violation occurs.

- (2) In an action under this subdivision:
- (i) if the violation of this chapter is a first offense for the person under subdivision 4, paragraph (a), and the person has not been found liable in a civil action under section 626A.13, the city or county attorney is entitled to seek appropriate injunctive relief; and
- (ii) if the violation of this chapter is a second or subsequent offense under subdivision 4, paragraph (a), or the person has been found liable in a prior civil action under section 626A.13, the person is subject to a mandatory \$500 civil fine.
- (b) The court may use any means within its authority to enforce an injunction issued under paragraph (a), clause (2)(i), and shall impose a civil fine of not less than \$500 for each violation of such an injunction.

**History:** 1969 c 953 s 2; 1984 c 628 art 3 s 11; 1986 c 444; 1988 c 577 s 14-18,62; 1989 c 336 art 1 s 1; art 2 s 8; 1990 c 455 s 3,4; 1991 c 199 art 2 s 1

# 626A.03 MANUFACTURE, DISTRIBUTION, POSSESSION, AND ADVERTISING OF WIRE, ELECTRONIC, OR ORAL COMMUNICATION INTERCEPTING DEVICES PROHIBITED.

Subdivision 1. **Acts**; **penalties.** Except as otherwise specifically provided in this chapter, any person who intentionally:

- (a) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, electronic, or oral communications;
  - (b) places in any newspaper, magazine, handbill, or other publication any advertisement of:
- (i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, electronic, or oral communications; or
- (ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purposes of the surreptitious interception of wire, electronic, or oral communications, shall be fined not more than \$20,000 or imprisoned not more than five years, or both.

### Subd. 2. **Offenses.** It is not unlawful under this section for:

- (a) a provider of wire or electronic communications service or an officer, agent or employee of, or a person under contract with, a provider, in the normal course of the business of providing that wire or electronic communications service; or
- (b) an officer, agent, or employee of, or a person under contract with, the United States, a state, or a political subdivision thereof, in the normal course of the activities of the United States, a state, or a political subdivision thereof, to manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, electronic, or oral communication.

**History:** 1969 c 953 s 3; 1984 c 628 art 3 s 11; 1988 c 577 s 19,20,62; 1989 c 336 art 2 s 8; 1991 c 199 art 2 s 1

# 626A.04 PROHIBITION OF USE AS EVIDENCE OF INTERCEPTED WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS.

Whenever any wire, oral, or electronic communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court or grand jury if the disclosure of that information would be in violation of this chapter.

**History:** 1969 c 953 s 4; 1988 c 577 s 62; 1989 c 336 art 1 s 2; art 2 s 8; 1990 c 426 art 2 s 1

## 626A.05 AUTHORIZATION FOR INTERCEPTION OF WIRE, ELECTRONIC, OR ORAL COMMUNICATIONS.

Subdivision 1. **Application for warrant.** The attorney general or a county attorney of any county may make application as provided in section 626A.06, to a judge of the district court, of the court of appeals, or of the supreme court for a warrant authorizing or approving the interception of wire, electronic, or oral communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made. No court commissioner shall issue a warrant under this chapter.

- Subd. 2. Offenses for which interception of wire or oral communication may be authorized. A warrant authorizing interception of wire, electronic, or oral communications by investigative or law enforcement officers may only be issued when the interception may provide evidence of the commission of, or of an attempt or conspiracy to commit, any of the following offenses:
- (1) a felony offense involving murder, manslaughter, assault in the first, second, and third degrees, aggravated robbery, kidnapping, criminal sexual conduct in the first, second, and third degrees, prostitution, bribery, perjury, escape from custody, theft, receiving stolen property, embezzlement, burglary in the first, second, and third degrees, forgery, aggravated forgery, check forgery, or financial transaction card fraud, as punishable under sections 609.185, 609.19, 609.195, 609.20, 609.221, 609.222, 609.223, 609.2231, 609.245, 609.25, 609.321 to 609.324, 609.342, 609.343, 609.344, 609.42, 609.48, 609.485, subdivision 4, paragraph (a), clause (1), 609.52, 609.53, 609.54, 609.582, 609.625, 609.631, 609.821, and 609.825;
- (2) an offense relating to gambling or controlled substances, as punishable under section 609.76 or chapter 152; or
- (3) an offense relating to restraint of trade defined in section 325D.53, subdivision 1 or 2, as punishable under section 325D.56, subdivision 2.

**History:** 1969 c 953 s 5; 1971 c 24 s 56; 1973 c 704 s 1; 1976 c 253 s 1; 1979 c 255 s 8; 1982 c 613 s 6; 1987 c 217 s 3; 1987 c 329 s 17; 1987 c 384 art 2 s 112; 1988 c 577 s 21,22,62; 1989 c 336 art 2 s 8; 1991 c 199 art 2 s 1; 1993 c 326 art 7 s 15; 1994 c 636 art 2 s 63

## 626A.06 PROCEDURE FOR INTERCEPTION OF WIRE, ELECTRONIC, OR ORAL COMMUNICATIONS.

Subdivision 1. **Applications.** Each application for a warrant authorizing or approving the interception of a wire, electronic, or oral communication shall be made in writing upon oath or affirmation to a judge of the district court, of the court of appeals, or of the supreme court and shall state the applicant's authority to make such application. Each application shall include the following information:

626A.06

- (1) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;
- (2) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify the applicant's belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subdivision 11, a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;
- (3) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;
- (4) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;
- (5) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, electronic, or oral communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application;
- (6) where statements in the application are solely upon the information or belief of the applicant, the grounds for the belief must be given; and
  - (7) the names of persons submitting affidavits in support of the application.
- Subd. 2. **Additional showing of probable cause.** The court to whom any such application is made, before issuing any warrant thereon, may examine on oath the person seeking the warrant and any witnesses the person may produce, and must take the person's affidavit or other affidavits in writing, and cause them to be subscribed by the party or parties making the same. The court may also require the applicant to furnish additional documentary evidence or additional oral testimony to satisfy itself of the existence of probable cause for issuance of the warrant.
- Subd. 3. **Finding of probable cause by judge.** Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, electronic, or oral communications within the territorial jurisdiction of the court in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant that:
- (1) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 626A.05, subdivision 2;
- (2) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
- (3) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;
- (4) except as provided in subdivision 11, there is probable cause for belief that the facilities from which, or the place where, the wire, electronic, or oral communications are to be intercepted are being used, or are

about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

Nothing in this chapter is to be considered as modifying in any way the existence or scope of those privileged communications defined in chapter 595. In acting upon an application for a warrant for intercepting communications, the potential contents of any such future communications that are within the provisions of chapter 595 shall not be considered by the court in making its finding as to the probability that material evidence will be obtained by such interception of communications.

- Subd. 4. **Warrant.** Each warrant to intercept communications shall be directed to a law enforcement officer, commanding the officer to hold the recording of all intercepted communications conducted under said warrant in custody subject to the further order of the court issuing the warrant. The warrant shall contain the grounds for its issuance with findings, as to the existence of the matters contained in subdivision 1 and shall also specify:
  - (1) the identity of the person, if known, whose communications are to be intercepted and recorded;
- (2) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted, and in the case of telephone or telegraph communications the general designation of the particular line or lines involved;
- (3) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;
- (4) the identity of the law enforcement office or agency authorized to intercept the communications, the name of the officer or officers thereof authorized to intercept communications, and of the person authorizing the application;
- (5) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained;
- (6) any other limitations on the interception of communications being authorized, for the protection of the rights of third persons;
- (7) a statement that using, divulging, or disclosing any information concerning such application and warrant for intercepting communications is prohibited and that any violation is punishable by the penalties of this chapter;
- (8) a statement that the warrant shall be executed as soon as practicable, shall be executed in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter and must terminate upon attainment of the authorized objective, or in any event in 30 days. The 30-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is received. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception.

An order authorizing the interception of a wire, oral, or electronic communication under this chapter must, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish the applicant immediately all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of

interference with the services that the service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. A provider of wire or electronic communication service, landlord, custodian, or other person furnishing facilities or technical assistance must be compensated by the applicant for reasonable expenses incurred in providing the facilities or assistance.

Denial of an application for a warrant to intercept communications or of an application for renewal of such warrant shall be by written order that shall include a statement as to the offense or offenses designated in the application, the identity of the official applying for the warrant and the name of the law enforcement office or agency.

- Subd. 4a. **Personnel used.** An interception under this chapter may be conducted in whole or in part by an employee of the state or any subdivision of the state who is an investigative or law enforcement officer authorized to conduct the investigation.
- Subd. 5. **Duration of warrant.** No warrant entered under this section may authorize or approve the interception of any wire, electronic, or oral communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days.

The effective period of any warrant for intercepting communications shall terminate immediately when any person named in the warrant has been charged with an offense specified in the warrant.

- Subd. 6. **Extensions.** Any judge of the district court, of the court of appeals, or of the supreme court may grant extensions of a warrant, but only upon application for an extension made in accordance with subdivision 1 and the court making the findings required by subdivision 3. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than 30 days. In addition to satisfying the requirements of subdivision 1, an application for an extension of any warrant for intercepting communications shall also:
- (1) contain a statement that all interception of communications under prior warrants has been in compliance with this chapter;
- (2) contain a statement setting forth the results thus far obtained from the interception or a reasonable explanation of the failure to obtain results;
  - (3) state the continued existence of the matters contained in subdivision 1; and
- (4) specify the facts and circumstances of the interception of communications under prior warrants which are relied upon by the applicant to show that such continued interception of communications is necessary and in the public interest.
- Subd. 7. **Delivery and retention of copies.** Any warrant for intercepting communications under this section, or any order renewing a prior warrant, together with the application made therefor and any supporting papers upon which the application was based, shall be delivered to and retained by the applicant as authority for the interception of communications authorized therein. A true copy of such warrant and the application made therefor shall be retained in the possession of the judge issuing the same, and, in the event of the denial of an application for such a warrant, a true copy of the papers upon which the application was based shall in like manner be retained by the judge denying the same.
- Subd. 8. **Periodic reports to issuing judge.** Whenever a warrant authorizing interception is entered pursuant to this section, the warrant may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

- Subd. 9. **Secrecy of warrant proceedings.** A warrant for intercepting communications and the application, affidavits, and return prepared in connection therewith, and also any information concerning the application for, the granting of, or the denial of a warrant for intercepting communications shall remain secret and subject to all the penalties of this chapter for unauthorized disclosure to persons not lawfully engaged in preparing and executing such a warrant, unless and until the same shall have been disclosed in a criminal trial or proceeding or shall have been furnished to a defendant pursuant to this chapter.
- Subd. 10. **Persons executing warrant.** A warrant for the interception of communications may in all cases be served by any of the officers mentioned in its direction, but by no other person except if the officer requires aid while present and acting in its execution.
- Subd. 11. **Requirements inapplicable.** The requirements of subdivision 1, clause (2), item (ii), and subdivision 3, clause (4), relating to the specification of the facilities from which, or the place where, the communication is to be interpreted do not apply if:
  - (1) in the case of an application with respect to the interception of an oral communication:
- (i) the application contains a full and complete statement as to why the specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and
  - (ii) the judge finds that the specification is not practical;
  - (2) in the case of an application with respect to a wire or electronic communication:
- (i) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and
  - (ii) the judge finds that the purpose has been adequately shown.
- Subd. 12. **Motion to quash order.** An interception of a communication under an order with respect to which the requirements of subdivision 1, clause (2), item (ii), and subdivision 3, clause (4), do not apply by reason of subdivision 11 must not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subdivision 11, clause (2), may move the court to modify or quash the order on the ground that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon notice to the attorney applying for the warrant, shall decide a motion expeditiously.

**History:** 1969 c 953 s 6; 1986 c 444; 1988 c 577 s 23-30,62; 1989 c 336 art 1 s 3; art 2 s 5,8; 1990 c 426 art 2 s 1; 1991 c 199 art 2 s 1; 1993 c 326 art 7 s 16-18

### 626A.065 EMERGENCY INTERCEPTION.

Notwithstanding any other provision in this chapter, any investigative or law enforcement officer, specially designated by the attorney general or a county attorney, who:

- (1) reasonably determines that:
- (i) an emergency situation exists that involves immediate danger of death or serious physical injury to any person that requires a wire, oral, or electronic communication to be intercepted before a warrant authorizing such interception can, with due diligence, be obtained; and

- (ii) there are grounds upon which a warrant could be issued under this chapter to authorize the interception; and
  - (2) obtains approval from a judge of the district court, of the court of appeals, or of the supreme court,

may intercept the wire, oral, or electronic communication. The judge's approval may be given orally and may be given in person or by using any medium of communication. The judge shall do one of the following: make written notes summarizing the conversation, tape record the conversation, or have a court reporter record the conversation. An application for a warrant approving the interception must be made in accordance with section 626A.06 within 36 hours after the interception has occurred, or begins to occur. In the absence of a warrant, the interception must immediately end when the communication sought is obtained or when the application for the warrant is denied, whichever is earlier. If application for approval is denied, or in any other case where the interception is ended without a warrant having been issued, the contents of a wire, oral, or electronic communication intercepted must be treated as having been obtained in violation of this chapter and an inventory shall be served as provided for in section 626A.10 on the person named in the application.

**History:** 1988 c 577 s 62; 1989 c 336 art 2 s 6,8; 1990 c 426 art 2 s 1

### 626A.07 RETURN FILED BY OFFICER.

Upon expiration of a warrant issued under section 626A.06, the officer designated in the warrant shall forthwith deliver the original warrant and accompanying papers to the judge issuing the same, together with a written return, verified by the certificate of the officer, setting forth:

- (1) the precise description of each installation of an instrument for the interception of communications, and the designation of any telephone or telegraph lines involved in such interception;
  - (2) the date or dates on which interception was conducted; and
- (3) an identification of all recordings made as required herein. Said recordings shall be delivered to the issuing judge with the return.

**History:** 1969 c 953 s 7; 1988 c 577 s 62; 1989 c 336 art 2 s 8

## 626A.08 PRESERVATION OF MATERIAL OBTAINED, APPLICATIONS AND ORDERS; DESTRUCTION.

Subdivision 1. **Material obtained.** Every part of any wire, oral, or electronic communication intercepted pursuant to this chapter shall be completely recorded on tape or wire or other comparable device and shall be done in such manner as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under the judge's directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge or a successor and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of section 626A.09 for investigations. The presence of the seal provided for by this subdivision, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, electronic, or oral communication or evidence derived therefrom under section 626A.09.

Subd. 2. **Application and orders.** Applications made and warrants issued under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of the district

1

court and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

- Subd. 3. **Destruction of recordings.** When an order for destruction is issued the person directed to destroy such recordings shall do so in the presence of at least one witness not connected with a law enforcement office or agency, all of whom shall execute affidavits setting forth the facts and circumstances thereof. The affidavits shall be filed with and approved by the court having custody of the original warrant and supporting papers.
- Subd. 4. **Contempt.** Any violation of the provisions of this section may be punished as contempt of the issuing or denying judge.

**History:** 1969 c 953 s 8; 1986 c 444; 1988 c 577 s 31,62; 1989 c 336 art 2 s 8; 1991 c 199 art 2 s 1

# 626A.09 AUTHORIZATION FOR DISCLOSURE AND USE OF INTERCEPTED WIRE, ELECTRONIC, OR ORAL COMMUNICATIONS.

Subdivision 1. **Disclosure.** 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 therefrom may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

- Subd. 2. Use of contents of wiretaps. 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 therefrom may use such contents to the extent such use is appropriate to the proper performance of official duties.
- Subd. 3. **Disclosure while giving testimony.** Any person who has received, by any means authorized by this chapter, any information concerning a wire, electronic, or oral communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any criminal proceeding in any court of the United States or of any state or in any federal or state grand jury proceeding.
- Subd. 4. **Privileged character retained.** No otherwise privileged wire, electronic, or oral communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.
- Subd. 5. **Application for authorized use.** When an investigative or law enforcement officer, while engaged in intercepting wire, electronic, or oral communications in the manner authorized herein, intercepts wire, electronic, or oral communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subdivisions 1 and 2. Such contents and any evidence derived therefrom may be used under subdivision 3 when authorized or approved by a judge of the district court where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

**History:** 1969 c 953 s 9; 1986 c 444; 1988 c 577 s 32-36,62; 1989 c 336 art 2 s 8; 1991 c 199 art 2 s

#### 626A.10 NOTICE TO DEFENDANT.

Subdivision 1. **Notice of order.** Within a reasonable time but not later than 90 days after the termination of the period of a warrant or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the warrant and the application, and such other parties to intercepted communications as the judge may determine that is in the interest of justice, an inventory which shall include notice of:

- (1) the fact of the issuance of the warrant or the application;
- (2) the date of the issuance and the period of authorized, approved or disapproved interception, or the denial of the application; and
  - (3) the fact that during the period wire, electronic, or oral communications were or were not intercepted.

On an ex parte showing to a court of competent jurisdiction that there is a need to continue the investigation and that the investigation would be harmed by service of the inventory at this time, service of the inventory required by this subdivision may be postponed for an additional 90-day period.

Subd. 2. Notice of intent to use evidence obtained by interception of wire or oral communication. The contents of any intercepted wire, electronic, or oral communication or evidence derived therefrom shall not be received in evidence otherwise disclosed in any trial, hearing, or other proceeding in a federal or state court unless each party, not less than ten 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 ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

**History:** 1969 c 953 s 10; 1986 c 444; 1988 c 577 s 37,38,62; 1989 c 336 art 2 s 8; 1993 c 326 art 7 s

#### 626A.11 ADMISSIBILITY OF INTERCEPTED EVIDENCE.

Subdivision 1. **Illegally obtained evidence inadmissible.** Evidence obtained by any act of intercepting wire, oral, or electronic communications, in violation of section 626A.02, and all evidence obtained through or resulting from information obtained by any such act, shall be inadmissible for any purpose in any action, proceeding, or hearing; provided, however, that: (1) any such evidence shall be admissible in any civil or criminal action, proceeding, or hearing against the person who has, or is alleged to have, violated this chapter; and (2) any evidence obtained by a lawfully executed warrant to intercept wire, oral, or electronic communications issued by a federal court or by a court of competent jurisdiction of another state shall be admissible in any civil or criminal proceeding.

Subd. 2. **Official available as witness.** No evidence obtained as a result of intercepting wire, oral, or electronic communications pursuant to a warrant issued under section 626A.06 shall be admissible in any proceeding unless the person or persons overhearing or recording such communication, conversation, or discussion be called or made available as witnesses subject to cross examination by the party against whom such intercepted evidence is being offered. The provisions of this clause shall not apply if the trial court finds that such person is dead; or is out of the state; or is unable to attend or testify because of age, sickness, infirmity, or imprisonment; or that such exceptional circumstances exist as to make it desirable, in the interest of justice and with due regard to the importance of presenting such persons in open court, to allow the evidence to be received.

- Subd. 3. **Failure to give notice.** In the absence of the notice to a defendant required by section 626A.10, no evidence relating to intercepted communications shall be admissible in evidence or otherwise disclosed in any criminal proceeding against the defendant.
- Subd. 4. **Remedies and sanctions.** The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving communications.

**History:** 1969 c 953 s 11; 1988 c 577 s 39-41,62; 1989 c 336 art 1 s 4,5; art 2 s 8; 1990 c 426 art 2 s 1; 1993 c 326 art 7 s 20

#### 626A.12 MOTION TO SUPPRESS EVIDENCE.

Subdivision 1. **Motion.** Any aggrieved person may move to suppress the contents of any intercepted wire, oral, or electronic communication, or evidence derived therefrom on the grounds that:

- (1) the wire, oral, or electronic communication was unlawfully intercepted;
- (2) the order of authorization or approval under which it was intercepted is insufficient on its face;
- (3) the interception was not made in conformity with the order of authorization or approval;
- (4) there was not probable cause for believing the existence of the grounds on which the warrant was issued; or
  - (5) the evidence was otherwise illegally obtained.

The court shall hear evidence upon any issue of fact necessary to a determination of the motion.

If the motion is granted, the contents of the intercepted wire, oral, or electronic communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter.

If the motion is denied, the order denying such may be reviewed on appeal from a judgment of conviction notwithstanding the fact that such judgment of conviction is predicated upon a plea of guilty.

Subd. 1a. [Repealed, 1989 c 336 art 1 s 17]

Subd. 2. **Time of making motion.** Upon receiving the notice required to be given by section 626A.10, subdivision 2, a defendant shall make a motion to suppress prior to the commencement of any trial or hearing in which the communications or conversations claimed to have been unlawfully obtained are proposed to be offered as evidence, except that the court shall entertain a motion made for the first time during trial upon a showing that (a) the defendant was unaware of the interception of communications until after the commencement of the trial, or (b) the defendant obtained material evidence previously unavailable to the defendant indicating it was unlawfully obtained, or (c) the defendant has not had adequate time or opportunity to make the motion before trial.

If a motion has been made and denied before trial, the determination shall be binding upon the trial court, except that, if it is established that, after the making of such motion, the defendant obtained additional material evidence of unlawfulness which could not have been obtained with reasonable diligence before the making of the motion, the court shall entertain another motion, or a renewal of a motion, during the trial.

When the motion is made before trial, the trial shall not be commenced until the motion has been determined.

When the motion is made during trial, the court shall, in the absence of the jury, if there be one, hear evidence in the same manner as if the motion had been made prior to trial, and shall decide all issues of fact and law.

If no motion is made in accordance with the provisions of this section, the defendant shall be deemed to have waived any objection during trial to the admission of evidence based on the ground that such evidence was unlawfully obtained.

- Subd. 3. **Where motion made.** The motion shall be made in the court having jurisdiction of the trial, hearing, or proceeding in which the evidence is being sought to be used.
- Subd. 4. **Examination of communications by court.** In any motion made under this section, if the court finds necessary to the determination of such motion to consider the contents of the intercepted communications in question, and the state does not consent to the examination thereof by the moving party, the court may order the state to deliver such recordings and any transcripts of the same for the inspection of the court in camera. Upon such delivery the court shall rule on the motion, and if the moving party objects to such ruling, and the trial is continued to an adjudication of the guilt of the moving party, the entire recordings shall be preserved by the state, and, in the event the defendant appeals, shall be made available to the appellate court for the purpose of determining the correctness of the ruling of the trial judge.
- Subd. 5. **Appeal by state.** The state shall be allowed to appeal from an order granting a motion to suppress evidence obtained through intercepted communications, if the prosecuting attorney shall certify to the judge or other official granting such motion that the appeal is not taken for purposes of delay. Such appeal shall be taken within 30 days after the date the order was entered and shall be diligently prosecuted. The appeal shall be made pursuant to rule 29.03 of the Rules of Criminal Procedure.

**History:** 1969 c 953 s 12; 1Sp1981 c 4 art 1 s 183; 1986 c 444; 1988 c 577 s 42,43,62; 1989 c 336 art 1 s 6; art 2 s 8; 1990 c 426 art 2 s 1

## 626A.13 CIVIL REMEDIES.

Subdivision 1. **In general.** Except as provided in section 2511 (2)(a)(ii) of title 18 of the United States Code, a person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity that engaged in that violation relief as may be appropriate.

- Subd. 2. **Relief.** In an action under this section, appropriate relief includes:
- (1) temporary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subdivision 3 and punitive damages in appropriate cases; and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.
- Subd. 3. **Computation of damages.** (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 of part 74 of title 47 of the Code of Federal Regulations 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, then the court shall assess damages as follows:
- (1) If the person who engaged in that conduct has not previously been enjoined under section 626A.02, subdivision 5, 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 statutory damages of not less than \$50 and not more than \$500.

- (2) If, on one prior occasion, the person who engaged in that conduct has been enjoined under section 626A.02, subdivision 5, or has been found 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:
- (1) the sum of three times the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or
  - (2) statutory damages of whichever is the greater of \$100 a day for each day of violation or \$10,000.
  - Subd. 4. **Defense.** A good faith reliance on:
  - (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;
- (2) a request of an investigative or law enforcement officer under United States Code, title 18, section 2518(7); or
- (3) a good faith determination that section 626A.02, subdivision 3, permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other law.

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

**History:** 1969 c 953 s 13; 1988 c 577 s 44,62; 1989 c 336 art 2 s 8; 1991 c 199 art 2 s 1; 1996 c 305 art 1 s 123

#### 626A.14 OBTAINING TELEPHONE AND TELEGRAPH COMPANY INFORMATION.

No person shall:

- (1) by trick or false representation or impersonation, obtain or attempt to obtain from any officer or any employee of any telegraph or telephone company information concerning the identification or location of any wires, cables, lines, terminals, or other apparatus used in furnishing telegraph or telephone service, or any information concerning any communication passing over telegraph or telephone lines of any such company, or the existence, content, or meaning of any record thereof; or
- (2) by trick or false representation or impersonation, obtain or attempt to obtain access to any premises or to installations of any telegraph or telephone company upon such premises.

**History:** 1969 c 953 s 14; 1988 c 577 s 62; 1989 c 336 art 2 s 8

### 626A.15 DUTY TO REPORT VIOLATIONS.

Any officer or employee of a telephone or telegraph company shall report to the police department or county attorney having jurisdiction, any violation of this chapter coming to the officer or employee's attention.

**History:** 1969 c 953 s 15; 1986 c 444; 1988 c 577 s 62; 1989 c 336 art 2 s 8; 1991 c 199 art 2 s 1

#### 626A.16 TELEPHONE COMPANY TO AID IN DETECTION.

Subject to regulation by the Minnesota public utilities commission, any telephone or telegraph company shall, upon request of any subscriber and upon responsible offer to pay the reasonable cost thereof, and with the discretion of the carrier; subject, however, to an appropriate court order to furnish whatever services may be within its command for the purpose of detecting any unlawful interception of communications. All such requests by subscribers shall be subject to the provisions of section 626A.05 and the company shall disclose only the existence or absence of interception that is not the subject of a court order under that section. All such requests by subscribers shall be kept confidential unless divulgence is authorized in writing by the requesting subscriber.

**History:** 1969 c 953 s 16; 1980 c 614 s 123; 1988 c 577 s 62; 1989 c 336 art 2 s 8

#### 626A.17 REPORT CONCERNING INTERCEPTION OF COMMUNICATIONS.

Subdivision 1. **Reports and transmittal of documents to state court administrator.** Within 30 days after the expiration of an order granting or denying an application under this chapter, or each extension thereof, or the denial of an order approving an interception or the use of a pen register, trap and trace device, or mobile tracking device, the issuing or denying judge shall report to the state court administrator:

- (1) the fact that an order or extension was applied for;
- (2) the kind of order or extension applied for;
- (3) the fact that the order or extension was granted as applied for, was modified, or was denied;
- (4) the period of interceptions or use of a pen register, trap and trace device, or mobile tracking device authorized by the order, and the number and duration of any extensions of the order;
  - (5) the offense specified in the order or application, or extension of an order;
- (6) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and
- (7) the nature of the facilities from which or the place where communications were to be intercepted or activity under the order was to be carried out.
- Subd. 2. **Report by county attorney.** No later than January 15 of each year each county attorney shall report to the state court administrator:
  - (1) with respect to each application for an order or extension made during the preceding year:
  - (i) the fact that an order or extension was applied for;
  - (ii) the kind of order or extension applied for;
  - (iii) the fact that the order or extension was granted as applied for, was modified, or was denied;
- (iv) the period of interceptions or use of a pen register, trap and trace device, or mobile tracking device authorized by the order, and the number and duration of any extensions of the order;
  - (v) the offense specified in the order or application, or extension of an order;
- (vi) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

- (vii) the nature of the facilities from which or the place where communications were to be intercepted or activity under the order was to be carried out;
- (2) a general description of the interceptions made or information obtained under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted or evidence obtained, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted or whose activities were monitored, and (iv) the approximate nature, amount, and cost of the personnel and other resources used in the interceptions or the use of the pen register, trap and trace device, or mobile tracking device;
- (3) the number of arrests resulting from interceptions made or activity conducted under such order or extension, and the offenses for which arrests were made;
  - (4) the number of trials resulting from such interceptions or activity;
- (5) the number of motions to suppress made with respect to such interceptions or activity, and the number granted or denied;
- (6) the number of convictions resulting from such interceptions or activity and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions or activity; and
- (7) the information required by clauses (2) to (6) with respect to orders or extensions obtained in a preceding calendar year.
- Subd. 3. **Report to legislature by state court administrator.** On or before November 15 of each even-numbered year, the state court administrator shall transmit to the legislature a report concerning (1) all warrants and orders authorizing the interception of communications and the use of a pen register, trap and trace device, mobile tracking device, or other electronic or mechanical device during the two previous calendar years and (2) all applications that were denied during the two previous calendar years. Each report shall include a summary and analysis of the data required to be filed under this section. The report is public and must be available for public inspection at the Legislative Reference Library and the state court administrator's office.

**History:** 1969 c 953 s 17; 1971 c 81 s 2; 1974 c 406 s 74; 1986 c 444; 1988 c 577 s 62; 1989 c 336 art 1 s 7; art 2 s 8

#### 626A.18 ILLEGAL TRANSFERS OF INTERCEPTING DEVICES.

No person shall receive an electronic, mechanical or other device, knowing or having reasonable cause to believe that such electronic, mechanical or other device has been sold or transported in violation of the provisions of this chapter. Whenever on the trial for a violation of this chapter the defendant is shown to have or have had possession of such electronic, mechanical or other device, such device shall be deemed sufficient evidence to authorize conviction unless the defendant explains such possession to the satisfaction of the jury.

**History:** 1969 c 953 s 18; 1988 c 577 s 62; 1989 c 336 art 2 s 8; 1991 c 199 art 2 s 1

#### 626A.19 FORFEITURES.

Subdivision 1. Laws applicable. Any electronic, mechanical or other device involved in any violation of the provisions of this chapter or any regulation promulgated thereunder, or which has come into the

custody of a law enforcement officer and the title thereto cannot be ascertained, shall be subject to seizure and forfeiture.

Subd. 2. **Disposal.** In the case of any forfeiture under this section no notice of public sale shall be required and no such electronic, mechanical or other device shall be sold at public sale. Such device shall be delivered to the bureau who may order the same destroyed or may sell or transfer the same without charge to the state of Minnesota or any political subdivision thereof for official use.

**History:** 1969 c 953 s 19; 1988 c 577 s 62; 1989 c 336 art 2 s 8; 1991 c 199 art 2 s 1

### 626A.20 SUSPENSION OR REVOCATION OF LICENSES.

On the conviction of any person of the violation of any provision of this chapter, a copy of the judgment and sentence, and of the opinion of the court, if any opinion be filed, shall be sent by the court administrator to the board or officer, if any, by whom the convicted defendant has been licensed or registered to practice a profession or to carry on a business. On the conviction of any such person, such board or officer may, in its discretion, suspend or revoke the license or registration of the convicted defendant to practice a profession or to carry on a business. On the application of any person whose license or registration has been suspended or revoked, and upon proper showing and for good cause the board or officer may, in its discretion, reinstate such license or registration.

**History:** 1969 c 953 s 20; 1986 c 444; 1Sp1986 c 3 art 1 s 82; 1988 c 577 s 62; 1989 c 336 art 2 s 8

**626A.21** [Repealed, 1991 c 199 art 1 s 87]

**626A.22** [Repealed, 1989 c 336 art 1 s 17]

**626A.23** [Repealed, 1989 c 336 art 1 s 17]

**626A.24** [Repealed, 1989 c 336 art 1 s 17]

## 626A.25 INJUNCTION AGAINST ILLEGAL INTERCEPTION.

Whenever it appears that a person is engaged or is about to engage in an act that constitutes or will constitute a felony violation of this chapter, the attorney general or a county attorney may initiate a civil action in district court to enjoin the violation. The court shall proceed as soon as practicable to the hearing and determination of the civil action, and may, at any time before final determination, enter a restraining order or prohibition, or take other action, as is warranted to prevent a continuing and substantial injury to the state, any of its subdivisions, or to a person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Rules of Civil Procedure, except that, if the defendant has been charged with the felony, discovery against that defendant is governed by the Rules of Criminal Procedure.

**History:** 1988 c 577 s 46,62; 1989 c 336 art 2 s 8; 1991 c 199 art 2 s 1

# ELECTRONIC COMMUNICATION SERVICE; REMOTE COMPUTING SERVICE

## 626A.26 UNLAWFUL ACCESS TO STORED COMMUNICATIONS.

Subdivision 1. **Offense.** Except as provided in subdivision 3, whoever:

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in the electronic storage in a system must be punished as provided in subdivision 2.

- Subd. 2. **Punishment.** The punishment for an offense under subdivision 1 is:
- (1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain:
- (i) a fine of not more than \$250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this clause; and
- (ii) a fine of not more than \$250,000 or imprisonment for not more than two years, or both, for any subsequent offense under this clause;
- (2) a fine of not more than \$5,000 or imprisonment for not more than six months, or both, in any other case.
  - Subd. 3. Exceptions. Subdivision 1 does not apply with respect to conduct authorized:
  - (1) by the person or entity providing a wire or electronic communications service;
  - (2) by a user of that service with respect to a communication of or intended for that user; or
  - (3) in sections 626A.05 to 626A.09, 626A.28, or 626A.29.

**History:** 1988 c 577 s 47,62; 1989 c 336 art 2 s 8

### 626A.27 DISCLOSURE OF CONTENTS.

Subdivision 1. **Prohibitions.** Except as provided in subdivision 2:

- (1) a person or entity providing an electronic communication service to the public must not knowingly divulge to a person or entity the contents of a communication while in electronic storage by that service; and
- (2) a person or entity providing remote computing service to the public must not knowingly divulge to a person or entity the contents of any communication that is carried or maintained on that service:
- (i) on behalf of, and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission, from a subscriber or customer of the service; and
- (ii) solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any communications for purposes of providing any services other than storage or computer processing.
  - Subd. 2. Exceptions. A person or entity may divulge the contents of a communication:
- (1) to an addressee or intended recipient of the communication or an agent of the addressee or intended recipient;
- (2) as otherwise authorized in section 626A.02, subdivision 2, paragraph (a); 626A.05; or section 626A.28;

- (3) with the lawful consent of the originator or an addressee or intended recipient of the communication, or the subscriber in the case of remote computing service;
- (4) to a person employed or authorized or whose facilities are used to forward a communication to its destination;
- (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or
  - (6) to a law enforcement agency, if the contents:
  - (i) were inadvertently obtained by the service provider; and
  - (ii) appear to pertain to the commission of a crime.

**History:** 1988 c 577 s 48,62; 1989 c 336 art 2 s 8

#### 626A.28 REQUIREMENTS FOR GOVERNMENTAL ACCESS.

Subdivision 1. **Contents of electronic communications in electronic storage.** A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications system for 180 days or less only under a warrant. A government entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than 180 days by the means available under subdivision 2.

- Subd. 2. **Contents of electronic communications in a remote computing service.** (a) A governmental entity may require a provider of remote computing service to disclose the contents of electronic communication to which this paragraph is made applicable by paragraph (b):
- (1) without required notice to the subscriber or customer, if the governmental entity obtains a warrant; or
  - (2) with prior notice if the governmental entity:
  - (i) uses an administrative subpoena authorized by statute or a grand jury subpoena; or
  - (ii) obtains a court order for such disclosure under subdivision 4;

except that delayed notice may be given under section 626A.30.

- (b) Paragraph (a) is applicable with respect to any electronic communication that is held or maintained on that service:
- (1) on behalf of, and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of such remote computing service; and
- (2) solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any communications for purposes of providing any services other than storage or computer processing.
- Subd. 3. Records concerning electronic communication service or remote computing service. (a) Except as provided in paragraph (b) or chapter 325M, a provider of electronic communication service or

remote computing service may disclose a record or other information pertaining to a subscriber to or customer of the service, not including the contents of communications covered by subdivision 1 or 2, to any person other than a governmental entity.

- (b) A provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of the service, not including the contents of communications covered by subdivision 1 or 2, to a governmental entity only when the governmental entity:
  - (1) uses an administrative subpoena authorized by statute, or a grand jury subpoena;
  - (2) obtains a warrant;
  - (3) obtains a court order for such disclosure under subdivision 4; or
  - (4) has the consent of the subscriber or customer to the disclosure.
- (c) A governmental entity receiving records or information under this subdivision is not required to provide notice to a subscriber or customer.
- (d) Notwithstanding paragraph (b), a provider of electronic communication service or remote computing service may not disclose location information covered by section 626A.42 to a government entity except as provided in that section.

## [See Note.]

- Subd. 4. **Requirements for court order.** A court order for disclosure under subdivision 2 or 3 must issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.
- Subd. 5. No cause of action against a provider disclosing certain information. No cause of action lies in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under sections 626A.26 to 626A.34.

**History:** 1988 c 577 s 49,62; 1989 c 336 art 2 s 8; 2002 c 395 art 1 s 10; 2014 c 278 s 1

**NOTE:** The amendment to subdivision 3 by Laws 2002, chapter 395, article 1, section 10, adding the cross reference to chapter 325M, is effective March 1, 2003, and expires on the effective date of federal legislation that preempts state regulation of the release of personally identifiable information by Internet service providers. Laws 2002, chapter 395, article 1, section 11.

## 626A.29 BACKUP PRESERVATION.

Subdivision 1. **Backup copy.** (a) A governmental entity acting under section 626A.28, subdivision 2, paragraph (b), may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of the subpoena or court order, the service provider shall create a backup copy, as soon as practicable, consistent with its regular business practices and shall confirm to the governmental entity that the backup copy has been made. The

backup copy must be created within two business days after receipt by the service provider of the subpoena or court order.

- (b) Notice to the subscriber or customer must be made by the governmental entity within three days after receipt of the confirmation, unless notice is delayed under section 626A.30, subdivision 1.
  - (c) The service provider must not destroy a backup copy until the later of:
  - (1) the delivery of the information; or
- (2) the resolution of any proceedings, including appeals of any proceeding, concerning the subpoena or court order.
- (d) The service provider shall release the backup copy to the requesting governmental entity no sooner than 14 days after the governmental entity's notice to the subscriber or customer if the service provider:
- (1) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and
  - (2) has not initiated proceedings to challenge the request of the governmental entity.
- (e) A governmental entity may seek to require the creation of a backup copy under paragraph (a) if in its sole discretion the entity determines that there is reason to believe that notification under section 626A.28 of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.
- Subd. 2. **Customer challenges.** (a) Within 14 days after notice by the governmental entity to the subscriber or customer under subdivision 1, paragraph (b), the subscriber or customer may file a motion to quash the subpoena or vacate the court order, with copies served upon the governmental entity and with written notice of the challenge to the service provider. A motion to vacate a court order must be filed in the court which issued the order. A motion to quash a subpoena must be filed in the district court of the county in which the governmental entity issuing the subpoena is located. The motion or application must contain an affidavit or sworn statement:
- (1) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for the applicant have been sought; and
- (2) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.
- (b) Service must be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received under sections 626A.26 to 626A.34. For the purposes of this section, the term "delivery" means handing it to the person specified in the notice or handing it to the person in charge of the office or department specified in the notice or the designee of the person in charge.
- (c) If the court finds that the customer has complied with paragraphs (a) and (b), the court shall order the governmental entity to file a sworn response. The response may be filed in camera if the governmental entity includes in its response the reasons that make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct additional proceedings as it considers appropriate. Proceedings must be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

- (d) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order the process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of sections 626A.26 to 626A.34, it shall order the process quashed.
- (e) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

**History:** 1986 c 444; 1988 c 577 s 50,62; 1989 c 336 art 2 s 8

## 626A.30 DELAYED NOTICE.

Subdivision 1. **Delay of notification.** (a) A governmental entity acting under section 626A.28, subdivision 2, may:

- (1) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 626A.28, subdivision 2, for a period not to exceed 90 days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (b); or
- (2) where an administrative subpoena or a grand jury subpoena is obtained, delay the notification required under section 626A.28 for a period not to exceed 90 days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (b).
  - (b) An adverse result for the purposes of paragraph (a) is:
  - (1) endangering the life or physical safety of an individual;
  - (2) flight from prosecution;
  - (3) destruction of or tampering with evidence;
  - (4) intimidation of potential witnesses; or
  - (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.
  - (c) The governmental entity shall maintain a true copy of certification under paragraph (a), clause (2).
- (d) Extensions of the delay of notification provided in section 626A.28 of up to 90 days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subdivision 2.
- (e) Upon expiration of the period of delay of notification under paragraph (a) or (d), the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that:
  - (1) states with reasonable specificity the nature of the law enforcement inquiry; and
  - (2) informs the customer or subscriber:

- (i) that information maintained for the customer or subscriber by the service provider named in the process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;
  - (ii) that notification of the customer or subscriber was delayed;
- (iii) what governmental entity or court made the certification or determination under which that delay was made; and
  - (iv) which provision of sections 626A.26 to 626A.34 allowed such delay.
- (f) As used in this subdivision, the term "supervisory official" means a peace officer with the rank of sergeant, or its equivalent, or above, a special agent in charge from the Bureau of Criminal Apprehension, the attorney general, the head of the attorney general's criminal division, a county attorney, or the head of a county attorney's criminal division.
- Subd. 2. **Preclusion of notice to subject of governmental access.** A governmental entity acting under section 626A.28 when it is not required to notify the subscriber or customer under section 626A.28, subdivision 2, paragraph (a), or to the extent that it may delay notice under subdivision 1, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for a period as the court considers appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in:
  - (1) endangering the life or physical safety of an individual;
  - (2) flight from prosecution;
  - (3) destruction of or tampering with evidence;
  - (4) intimidation of potential witnesses; or
  - (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

**History:** 1988 c 577 s 51,62; 1989 c 336 art 2 s 8

### 626A.31 COST REIMBURSEMENT.

Subdivision 1. **Payment.** Except as otherwise provided in subdivision 3, a governmental entity obtaining the contents of communications, records, or other information under sections 626A.27, 626A.28, and 626A.29 shall pay to the person or entity assembling or providing the information a fee for reimbursement for costs that are reasonably necessary and that have been directly incurred in searching for, assembling, reproducing, or otherwise providing the information. The reimbursable costs must include any costs due to necessary disruption of normal operations of the electronic communication service or remote computing service in which the information may be stored.

Subd. 2. **Amount.** The amount of the fee provided by subdivision 1, must be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, must be as determined by the court that issued the order for production of the information or the court before which a criminal prosecution relating to the information would be brought, if no court order was issued for production of the information.

Subd. 3. **Inapplicability.** The requirement of subdivision 1 does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 626A.28. The court may, however, order a payment as described in subdivision 1 if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

**History:** 1988 c 577 s 52,62; 1989 c 336 art 2 s 8

#### 626A.32 CIVIL ACTION.

Subdivision 1. **Cause of action.** Except as provided in section 626A.28, subdivision 5, a provider of electronic communication service, subscriber, or customer aggrieved by a violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation relief as may be appropriate.

- Subd. 2. **Relief.** In a civil action under this section, appropriate relief includes:
- (1) temporary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subdivision 3; and
- (3) a reasonable attorney's fee and other litigation costs reasonably incurred.
- Subd. 3. **Damages.** The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case is a person entitled to recover to receive less than the sum of \$1,000.
  - Subd. 4. **Defense.** A good faith reliance on:
- (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization; or
- (2) a good faith determination that section 626A.02, subdivision 3, permitted the conduct complained of;

is a complete defense to a civil or criminal action brought under sections 626A.26 to 626A.34 or any other law.

Subd. 5. **Limitation.** A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

**History:** 1988 c 577 s 53,62; 1989 c 336 art 2 s 8

#### 626A.33 EXCLUSIVITY OF REMEDIES.

The remedies and sanctions described in sections 626A.26 to 626A.34 are the only judicial remedies and sanctions for nonconstitutional violations of sections 626A.26 to 626A.34.

**History:** 1988 c 577 s 54,62; 1989 c 336 art 2 s 8

#### 626A.34 DEFINITIONS.

As used in sections 626A.26 to 626A.34, the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communication system.

**History:** 1988 c 577 s 55,62; 1989 c 336 art 2 s 8

#### PEN REGISTER; TRAP AND TRACE DEVICE; MOBILE TRACKING DEVICE

## 626A.35 GENERAL PROHIBITION ON PEN REGISTER, TRAP AND TRACE DEVICE, AND MOBILE TRACKING DEVICE USE; EXCEPTION.

Subdivision 1. **In general.** Except as provided in this section, no person may install or use a pen register, trap and trace device, or mobile tracking device without first obtaining a court order under section 626A.37.

- Subd. 2. **Exception.** The prohibition of subdivision 1 does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service:
- (1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of the provider, or to the protection of users of that service from abuse of service or unlawful use of service; or
- (2) to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful, or abusive use of service; or
  - (3) where the consent of the user of that service has been obtained.
- Subd. 2a. **Exception.** The prohibition of subdivision 1 does not apply to the use of a mobile tracking device where the consent of the owner of the object to which the mobile tracking device is to be attached has been obtained.
- Subd. 3. **Penalty.** Whoever knowingly violates subdivision 1 shall be fined not more than \$3,000 or imprisoned not more than one year, or both.

**History:** 1988 c 577 s 56,62; 1989 c 336 art 1 s 8; art 2 s 8

## 626A.36 APPLICATION FOR ORDER FOR PEN REGISTER, TRAP AND TRACE DEVICE, OR MOBILE TRACKING DEVICE.

Subdivision 1. **Application.** An investigative or law enforcement officer with responsibility for an ongoing criminal investigation may make application for an order or an extension of an order under section 626A.37 authorizing or approving the installation and use of a pen register, trap and trace device, or mobile tracking device under sections 626A.35 to 626A.39, in writing under oath or equivalent affirmation, to a district court.

#### Subd. 2. Contents of application. An application under subdivision 1 must include:

(1) the identity of the law enforcement or investigative officer making the application, the identity of any other officer or employee authorizing or directing the application, and the identity of the law enforcement agency conducting the investigation; and

(2) a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that an order should be issued.

**History:** 1988 c 577 s 57,62; 1989 c 336 art 1 s 9; art 2 s 8

## 626A.37 ISSUANCE OF ORDER FOR PEN REGISTER, TRAP AND TRACE DEVICE, OR MOBILE TRACKING DEVICE.

Subdivision 1. **In general.** Upon an application made under section 626A.36, the court may enter an ex parte order authorizing the installation and use of a pen register, trap and trace device, or mobile tracking device within the jurisdiction of the court if the court finds on the basis of the information submitted by the applicant that there is reason to believe that the information likely to be obtained by the installation and use is relevant to an ongoing criminal investigation.

#### Subd. 2. Contents of order. (a) An order issued under this section must specify:

- (1) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached or of the person to be traced by the mobile tracking device;
  - (2) the identity, if known, of the person who is the subject of the criminal investigation;
- (3) 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 or the identity or nature of the object or objects to which the mobile tracking device is to be attached, and, in the case of a trap and trace device, the geographic limits of the trap and trace order;
- (4) a statement of the offense to which the information likely to be obtained by the pen register, trap and trace device, or mobile tracking device relates;
- (5) the identity of the law enforcement or investigative officer responsible for installation and use of the pen register, trap and trace device, or mobile tracking device; and
- (6) the period during which the use of the pen register, trap and trace device, or mobile tracking device is authorized.
- (b) An order issued under this section must direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register, trap and trace device, or mobile tracking device under section 626A.38.
- Subd. 3. **Time period and extensions.** (a) An order issued under this section must authorize the installation and use of a pen register, a trap and trace device, or a mobile tracking device for a period not to exceed 60 days, or the period necessary to achieve the objective of the authorization, whichever is less.
- (b) Extensions of an order may be granted, but only upon an application for an order under section 626A.36 and upon the judicial finding required by subdivision 1. The extension must include a statement of any changes in the information required in subdivision 2. The period of extension must be for a period not to exceed 60 days, or the period necessary to achieve the objective for which it is granted, whichever is less.
- Subd. 4. **Nondisclosure of existence of pen register, trap and trace device, or mobile tracking device.** An order authorizing or approving the installation and use of a pen register, trap and trace device, or a mobile tracking device must direct that:

- (1) the order be sealed until otherwise ordered by the court; and
- (2) the person owning or leasing the line to which the pen register or a 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, trap and trace device, mobile tracking device, or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.
- Subd. 5. **Jurisdiction.** A warrant or other order for a mobile tracking device issued under this section or other authority may authorize the use of a mobile tracking device within the jurisdiction of the court and outside of that jurisdiction as long as the device is installed in the jurisdiction.

**History:** 1988 c 577 s 58,62; 1989 c 336 art 1 s 10; art 2 s 8

## 626A.38 REGISTER, TRAP AND TRACE DEVICE, OR MOBILE TRACKING DEVICE.

Subdivision 1. **Pen registers or mobile tracking devices.** Upon the request of an officer of a law enforcement agency authorized to install and use a pen register or mobile tracking device under sections 626A.35 to 626A.39, a provider of wire or electronic communication service, landlord, custodian, or other person shall furnish the investigative or law enforcement officer immediately with all information, facilities, and technical assistance necessary to accomplish the installation of the pen register or mobile tracking 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 assistance is directed by a court order as provided in section 626A.37, subdivision 2, paragraph (b).

- Subd. 2. **Trap and trace device.** Upon the request of an officer of a law enforcement agency authorized to receive the results of a trap and trace device under sections 626A.35 to 626A.39, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install the device immediately on the appropriate line and shall 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 as provided in section 626A.37, subdivision 2, paragraph (b). Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the officer of a law enforcement agency, designated by the court, at reasonable intervals during regular business hours for the duration of the order.
- Subd. 3. **Compensation.** A provider of a wire or electronic communication service, landlord, custodian, or other person who furnishes facilities or technical assistance under this section must be reasonably compensated for reasonable expenses incurred in providing facilities and assistance.
- Subd. 4. **No cause of action against provider disclosing certain information.** No cause of action lies in any court against a provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order under sections 626A.35 to 626A.39.

Subd. 5. [Repealed, 1989 c 336 art 1 s 17]

**History:** 1988 c 577 s 59,62; 1989 c 336 art 1 s 11; art 2 s 8

### 626A.381 SERVICE OR NOTICE; INVENTORY.

Subdivision 1. **Notice required.** Except as provided in subdivision 2, within a reasonable time not later than 90 days after the filing of an application under section 626A.36, if the application is denied, or of the

termination of an order, as extended under section 626A.37, the issuing or denying judge shall have served on the persons named in the order or application an inventory that includes notice of:

- (1) the fact of the entry of the order or the application;
- (2) the date of the entry and the period of authorized, approved, or disapproved activity under the order, or the denial of the application; and
  - (3) the fact that during the period, activity did or did not take place under the order.
- Subd. 2. **Exception.** On an ex parte showing of good cause, a judge may postpone or dispense with service of the inventory required by this section.
- Subd. 3. **Inspection.** The judge, upon the filing of a motion, may make available to a person or the person's counsel portions of the results of activity under the order or referred to in the application, or the order or application as the judge determines is in the interest of justice.

**History:** 1989 c 336 art 1 s 12

## 626A.39 DEFINITIONS.

Subdivision 1. Applicability. The terms in this section apply to sections 626A.35 to 626A.39.

- Subd. 2. Wire communication; electronic communication; electronic communication service. The terms "wire communication," "electronic communication," and "electronic communication service" have the meanings set forth for the terms in section 626A.01.
- Subd. 3. **Pen register.** "Pen register" means a device that records or decodes electronic or other impulses that identify the number dialed or otherwise transmitted on the telephone line to which the device is attached, but the term does not include a device used by a provider or customer of a wire or electronic communications service for billing, or recording as an incident to billing, for communications services provided by the provider or a device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.
- Subd. 4. **Trap and trace device.** "Trap and trace device" means a device which 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.
- Subd. 5. **Mobile tracking device.** "Mobile tracking device" means an electronic or mechanical device that permits the tracking of the movement of a person or object.

**History:** 1988 c 577 s 60,62; 1989 c 336 art 1 s 13; art 2 s 8

## 626A.391 CIVIL ACTION; DAMAGES.

Subdivision 1. **General.** A person who is harmed by a violation of sections 626A.35 to 626A.39 may bring a civil action against the person who violated these sections for damages and other appropriate relief, including:

- (1) preliminary and equitable or declaratory relief; and
- (2) reasonable costs and attorney fees.
- Subd. 2. Limitation. An action under this section must be commenced within two years after:

- (1) the occurrence of the violation; or
- (2) the date upon which the claimant first had a reasonable opportunity to discover the violation.
- Subd. 3. **Defenses.** (1) A good faith reliance on a court warrant or order, a grand jury subpoena, or a statutory authorization; or
- (2) a good faith reliance on a request of an investigative or law enforcement officer under United States Code, title 18, section 2518(7)

is a complete defense against any civil or criminal action brought under sections 626A.35 to 626A.39.

**History:** 1988 c 577 s 62; 1989 c 336 art 1 s 14; art 2 s 8

#### **GENERALLY**

#### 626A.40 SUBJECT TO OTHER LAWS.

Nothing in this chapter authorizes conduct constituting a violation of any law of the United States.

**History:** 1988 c 577 s 61,62; 1989 c 336 art 1 s 15; art 2 s 8

### **626A.41 CITATION.**

This chapter may be cited as the "Privacy of Communications Act."

**History:** 1988 c 577 s 62; 1989 c 336 art 1 s 16; art 2 s 8

#### **ELECTRONIC DEVICE; TRACKING WARRANT**

#### 626A.42 ELECTRONIC DEVICE LOCATION INFORMATION.

Subdivision 1. **Definitions.** (a) The definitions in this subdivision apply to this section.

- (b) "Electronic communication service" has the meaning given in section 626A.01, subdivision 17.
- (c) "Electronic device" means a device that enables access to or use of an electronic communication service, remote computing service, or location information service.
- (d) "Government entity" means a state or local agency, including but not limited to a law enforcement entity or any other investigative entity, agency, department, division, bureau, board, or commission or an individual acting or purporting to act for or on behalf of a state or local agency.
- (e) "Location information" means information concerning the location of an electronic device that, in whole or in part, is generated or derived from or obtained by the operation of an electronic device.
- (f) "Location information service" means the provision of a global positioning service or other mapping, locational, or directional information service.
  - (g) "Remote computing service" has the meaning given in section 626A.34.
- (h) "Tracking warrant" means an order in writing, in the name of the state, signed by a court other than a court exercising probate jurisdiction, directed to a peace officer, granting the officer access to location information of an electronic device.

- Subd. 2. **Tracking warrant required for location information.** (a) Except as provided in paragraph (b), a government entity may not obtain the location information of an electronic device without a tracking warrant. A warrant granting access to location information must be issued only if the government entity shows that there is probable cause the person who possesses an electronic device is committing, has committed, or is about to commit a crime. An application for a warrant must be made in writing and include:
- (1) the identity of the government entity's peace officer making the application, and the officer authorizing the application; and
- (2) a full and complete statement of the facts and circumstances relied on by the applicant to justify the applicant's belief that a warrant should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, and (ii) the identity of the person, if known, committing the offense whose location information is to be obtained.
  - (b) A government entity may obtain location information without a tracking warrant:
  - (1) when the electronic device is reported lost or stolen by the owner;
  - (2) in order to respond to the user's call for emergency services;
  - (3) with the informed, affirmative, documented consent of the owner or user of the electronic device;
- (4) with the informed, affirmative consent of the legal guardian or next of kin of the owner or user if the owner or user is believed to be deceased or reported missing and unable to be contacted; or
- (5) in an emergency situation that involves the risk of death or serious physical harm to a person who possesses an electronic communications device pursuant to sections 237.82 and 237.83.
- Subd. 3. **Time period and extensions.** (a) A tracking warrant issued under this section must authorize the collection of location information for a period not to exceed 60 days, or the period of time necessary to achieve the objective of the authorization, whichever is less.
- (b) Extensions of a tracking warrant may be granted, but only upon an application for an order and upon the judicial finding required by subdivision 2, paragraph (a). The period of extension must be for a period not to exceed 60 days, or the period of time necessary to achieve the objective for which it is granted, whichever is less.
- (c) Paragraphs (a) and (b) apply only to tracking warrants issued for the contemporaneous collection of electronic device location information.
- Subd. 4. **Notice**; **temporary nondisclosure of tracking warrant.** (a) Within a reasonable time but not later than 90 days after the court unseals the tracking warrant under this subdivision, the issuing or denying judge shall cause to be served on the persons named in the warrant and the application an inventory which shall include notice of:
  - (1) the fact of the issuance of the warrant or the application;
- (2) the date of the issuance and the period of authorized, approved, or disapproved collection of location information, or the denial of the application; and
  - (3) the fact that during the period location information was or was not collected.
  - (b) A tracking warrant authorizing collection of location information must direct that:

- (1) the warrant be sealed for a period of 90 days or until the objective of the warrant has been accomplished, whichever is shorter; and
  - (2) the warrant be filed with the court administrator within ten days of the expiration of the warrant.
- (c) The prosecutor may request that the tracking warrant, supporting affidavits, and any order granting the request not be filed. An order must be issued granting the request in whole or in part if, from affidavits, sworn testimony, or other evidence, the court finds reasonable grounds exist to believe that filing the warrant may cause the search or a related search to be unsuccessful, create a substantial risk of injury to an innocent person, or severely hamper an ongoing investigation.
- (d) The tracking warrant must direct that following the commencement of any criminal proceeding utilizing evidence obtained in or as a result of the search, the supporting application or affidavit must be filed either immediately or at any other time as the court directs. Until such filing, the documents and materials ordered withheld from filing must be retained by the judge or the judge's designee.
- Subd. 5. **Report concerning collection of location information.** (a) At the same time as notice is provided under subdivision 4, the issuing or denying judge shall report to the state court administrator:
  - (1) the fact that a tracking warrant or extension was applied for;
  - (2) the fact that the warrant or extension was granted as applied for, was modified, or was denied;
- (3) the period of collection authorized by the warrant, and the number and duration of any extensions of the warrant;
  - (4) the offense specified in the warrant or application, or extension of a warrant;
  - (5) whether the collection required contemporaneous monitoring of an electronic device's location; and
- (6) the identity of the applying investigative or peace officer and agency making the application and the person authorizing the application.
- (b) On or before November 15 of each even-numbered year, the state court administrator shall transmit to the legislature a report concerning: (1) all tracking warrants authorizing the collection of location information during the two previous calendar years; and (2) all applications that were denied during the two previous calendar years. Each report shall include a summary and analysis of the data required to be filed under this subdivision. The report is public and must be available for public inspection at the Legislative Reference Library and the state court administrator's office and website.
- Subd. 6. **Prohibition on use of evidence.** (a) Except as proof of a violation of this section, no evidence obtained in violation of this section shall be admissible in any criminal, civil, administrative, or other proceeding.
- (b) Any location information obtained pursuant to this chapter or evidence derived therefrom shall 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 ten days before the trial, hearing, or proceeding, has been furnished with a copy of the tracking warrant, and accompanying application, under which the information was obtained. This ten-day period may be waived by the judge if the judge finds that it was not possible to furnish a party with the required information ten days before the trial, hearing, or proceeding and that a party will not be prejudiced by the delay in receiving the information.

**History:** 2014 c 278 s 2