

SENATE
STATE OF MINNESOTA
EIGHTY-NINTH SESSION

S.F. No. 33

(SENATE AUTHORS: PETERSEN, B.)

DATE	D-PG	OFFICIAL STATUS
01/08/2015	42	Introduction and first reading Referred to Judiciary

A bill for an act

1.1 relating to public safety; requiring government entities to obtain search warrants
 1.2 before obtaining certain types of personal identifying information on an
 1.3 individual; amending Minnesota Statutes 2014, section 626A.28, subdivisions
 1.4 1, 3, 4; proposing coding for new law in Minnesota Statutes, chapter 626A;
 1.5 repealing Minnesota Statutes 2014, sections 626A.28, subdivision 2; 626A.42.
 1.6

1.7 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

1.8 Section 1. Minnesota Statutes 2014, section 626A.28, subdivision 1, is amended to read:

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

1.17 Sec. 2. Minnesota Statutes 2014, section 626A.28, subdivision 3, is amended to read:

1.18 Subd. 3. **Records concerning electronic communication service or remote**
 1.19 **computing service.** (a) Except as provided in paragraph (b) or chapter 325M, a provider
 1.20 of electronic communication service or remote computing service may disclose a record
 1.21 or other information pertaining to a subscriber to or customer of the service, not including
 1.22 the contents of communications covered by subdivision 1 or 2, to any person other than a
 1.23 governmental entity.

2.1 (b) A provider of electronic communication service or remote computing service
 2.2 may disclose a record or other information pertaining to a subscriber to or customer of the
 2.3 service, not including the contents of communications covered by subdivision 1 or 2, to a
 2.4 governmental entity only when the governmental entity:

2.5 (1) uses an administrative subpoena authorized by statute, or a grand jury subpoena;

2.6 (2) obtains a warrant;

2.7 (3) obtains a court order for such disclosure under subdivision 4; or

2.8 (4) has the consent of the subscriber or customer to the disclosure.

2.9 (c) A governmental entity receiving records or information under this subdivision is
 2.10 not required to provide notice to a subscriber or customer.

2.11 ~~(d) Notwithstanding paragraph (b), a provider of electronic communication service~~
 2.12 ~~or remote computing service may not disclose location information covered by section~~
 2.13 ~~626A.42 to a government entity except as provided in that section.~~

2.14 Sec. 3. Minnesota Statutes 2014, section 626A.28, subdivision 4, is amended to read:

2.15 Subd. 4. **Requirements for court order.** A court order for disclosure under
 2.16 subdivision 2 or 3 must issue only if the governmental entity shows that there is reason
 2.17 to believe the contents of a wire or electronic communication, or the records or other
 2.18 information sought, are relevant to a legitimate law enforcement inquiry. A court issuing
 2.19 an order pursuant to this section, on a motion made promptly by the service provider,
 2.20 may quash or modify such order, if the information or records requested are unusually
 2.21 voluminous in nature or compliance with such order otherwise would cause an undue
 2.22 burden on such provider.

2.23 Sec. 4. **[626A.415] PERSONAL IDENTIFYING INFORMATION; SEARCH**
 2.24 **WARRANT AND NOTICE REQUIRED.**

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

2.27 (b) An "adverse result" occurs when notification of the existence of a search warrant
 2.28 results in:

2.29 (1) danger to the life or physical safety of an individual;

2.30 (2) a flight from prosecution;

2.31 (3) destruction of or tampering with evidence;

2.32 (4) the intimidation of a potential witness; or

2.33 (5) serious jeopardy to an investigation or undue delay of a trial.

3.1 (c) "Electronic device" means a device that enables access to or use of an electronic
3.2 communication service, remote computing service, or global positioning or other mapping,
3.3 locational, or directional service.

3.4 (d) "Financial institution" has the meaning given in section 13A.01, subdivision 2.

3.5 (e) "Financial record" has the meaning given in section 13A.01, subdivision 3.

3.6 (f) "Government entity" means a state or local agency, including but not limited to a
3.7 law enforcement entity or any other investigative entity, agency, department, division,
3.8 bureau, board, or commission, or an individual acting or purporting to act for or on behalf
3.9 of a state or local agency.

3.10 (g) "Health record" has the meaning given in section 144.291, subdivision 2.

3.11 (h) "Personal identifying information" includes information concerning or that
3.12 reasonably could be construed as concerning the identity, location, or activities of an
3.13 individual. The term includes the individual's name, physical or electronic address,
3.14 telephone number, telephone numbers dialed or received, addresses from which electronic
3.15 communications were sent or received, addresses of Web sites visited, billing records,
3.16 health records, financial records, and physical location, including the location of electronic
3.17 devices and other personal property owned or possessed by the individual.

3.18 The term includes information that, in whole or in part, is generated or derived from
3.19 or obtained by the retrieval of records held by a third party and by the use of technology
3.20 that enables the user to obtain information in the aggregate or on a mass or comprehensive
3.21 scale, or that a reasonable person would consider private or otherwise not readily available
3.22 to the public. The term does not include information that is accessible to the public under
3.23 other law or readily available or observable to the public when actually obtained through
3.24 the direct observation by the line of sight of a person or group of persons.

3.25 (i) "Remote computing service" has the meaning given in section 626A.34.

3.26 Subd. 2. **Search warrant required for personal identifying information.** (a)
3.27 Except as provided in paragraphs (b) and (c), a government entity may not obtain personal
3.28 identifying information concerning an individual without a search warrant. A court order
3.29 granting access to this information must be issued only if the government entity shows
3.30 that there is probable cause for belief that the individual who is the subject of the personal
3.31 identifying information is committing, has committed, or is about to commit a criminal
3.32 offense.

3.33 (b) A government entity may obtain location information concerning the location of
3.34 an individual's electronic device without a search warrant:

3.35 (1) when the electronic device is reported lost or stolen by the owner;

3.36 (2) to respond to the user's call for emergency services;

4.1 (3) with the informed, affirmative consent of the owner or user of the device;

4.2 (4) with the informed, affirmative consent of the legal guardian or next of kin of the
4.3 owner or user of the device if the owner or user is believed to be deceased or reported
4.4 missing and unable to be contacted; or

4.5 (5) there exists a potentially life-threatening situation.

4.6 (c) A government entity may obtain personal identifying information other than that
4.7 described in paragraph (b) without a search warrant with the informed, affirmative consent
4.8 of the subject of the information or in the event of a potentially life-threatening situation.

4.9 Subd. 3. **Notice.** (a) Notice must be given to the subject of personal identifying
4.10 information obtained by a government entity under this section.

4.11 (b) Unless delayed notice is ordered under paragraph (c), the government entity shall
4.12 provide notice to the subject within three days of obtaining the information. The notice
4.13 must be made by service or delivered by registered or first-class mail, e-mail, or any other
4.14 means reasonably calculated to be effective as specified by the court issuing the warrant.

4.15 The notice must contain the following information:

4.16 (1) the nature of the law enforcement inquiry, with reasonable specificity;

4.17 (2) the type of information that was obtained by, supplied to, or requested by the
4.18 government entity and the date on which it was obtained, provided, or requested;

4.19 (3) if information was obtained from a third party, the identity of the provider of
4.20 the information; and

4.21 (4) whether the notification was delayed pursuant to paragraph (c) and, if so, the
4.22 court that granted the delay and the reasons for granting the delay.

4.23 (c) A government entity may include in the application for a warrant a request
4.24 for an order to delay the notification required under this subdivision for a period not to
4.25 exceed ten days. The court shall issue the order if the court determines that there is reason
4.26 to believe that notification may have an adverse result. Upon expiration of the period of
4.27 delay granted under this paragraph and any extension granted under paragraph (e), the
4.28 government entity shall provide the subject of the warrant a copy of the warrant together
4.29 with a notice pursuant to paragraph (b).

4.30 (d) A government entity may include in its application for a warrant a request for an
4.31 order directing a third party to whom a warrant is directed not to notify any other person
4.32 of the existence of the warrant for a period of not more than ten days. The court shall
4.33 issue the order if the court determines that there is reason to believe that notification of
4.34 the existence of the warrant may have an adverse result.

4.35 (e) The court, upon application, may grant one or more extensions of orders granted
4.36 under paragraph (c) or (d) for up to an additional ten days.

5.1 Subd. 4. **Construction.** This section shall be construed liberally by courts to
5.2 protect the privacy of individuals. Examples used in the definitions are illustrative and
5.3 not comprehensive.

5.4 Subd. 5. **Retention of information.** (a) A government unit may keep personal
5.5 identifying information obtained under this section for up to 60 days.

5.6 (b) A government unit may seek a court order extending the 60-day period. A
5.7 court shall grant this extension if the court determines that an extension is necessary to
5.8 avoid serious jeopardy to an investigation or undue delay of a trial. If the court grants an
5.9 extension, the court shall specify the duration of the extension.

5.10 (c) Notwithstanding section 138.17, a government unit shall destroy personal
5.11 identifying information obtained under this section at the end of the time period specified
5.12 in paragraphs (a) and (b).

5.13 Subd. 6. **Prosecutorial disclosure.** The prosecutor shall disclose to the defense any
5.14 search warrants for personal identifying information obtained under this section, along
5.15 with the information described in subdivision 3, paragraph (b), clauses (2) and (3). This
5.16 information must be provided no later than the omnibus hearing in a felony or gross
5.17 misdemeanor prosecution or the arraignment or trial in a misdemeanor prosecution.

5.18 Subd. 7. **Use of information.** Personal identifying information obtained pursuant
5.19 to a search warrant under this section may not be shared with or transferred to another
5.20 federal, state, or local government authority unless that authority has obtained a search
5.21 warrant for the information.

5.22 Subd. 8. **Admissibility of improperly obtained information.** Evidence obtained
5.23 in violation of this section, and all evidence obtained in any manner in whole or in part
5.24 through or resulting from information obtained in violation of this section, is inadmissible
5.25 for any purpose in any action, proceeding, or hearing, except that:

5.26 (1) the evidence is admissible in any civil or criminal action, proceeding, or hearing
5.27 against the person who has, or is alleged to have, violated this section; and

5.28 (2) any evidence obtained by a lawfully executed warrant issued by a federal
5.29 court or by a court of competent jurisdiction of another state is admissible in any civil
5.30 or criminal proceeding.

5.31 Subd. 9. **Conflicting provisions superseded.** This section supersedes any
5.32 conflicting provision in law in effect on March 1, 2015.

5.33 Sec. 5. **REVISOR'S INSTRUCTION.**

5.34 By January 15, 2016, the revisor of statutes shall prepare a bill for introduction in
5.35 the 2016 legislative session making conforming changes in law necessitated by this act.

6.1 Sec. 6. **REPEALER.**

6.2 Minnesota Statutes 2014, sections 626A.28, subdivision 2; and 626A.42, are
6.3 repealed.

626A.28 REQUIREMENTS FOR GOVERNMENTAL ACCESS.

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.

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

APPENDIX

Repealed Minnesota Statutes: 15-0813

(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 Web site.

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

APPENDIX

Repealed Minnesota Statutes: 15-0813

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.