State of Minnesota

HOUSE OF REPRESENTATIVES

EIGHTY-EIGHTH SESSION

H. F. No. 3173

03/19/2014 Authored by Lesch
The bill was read for the first time and referred to the Committee on Public Safety Finance and Policy

A bill for an act

relating to public safety; requiring government entities to obtain search warrants before obtaining certain types of personal identifying information on an individual; amending Minnesota Statutes 2012, section 626A.28, subdivisions 1, 4; proposing coding for new law in Minnesota Statutes, chapter 626A; repealing Minnesota Statutes 2012, section 626A.28, subdivision 2.

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

Section 1. Minnesota Statutes 2012, section 626A.28, subdivision 1, is amended to read:

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.~~

Sec. 2. Minnesota Statutes 2012, section 626A.28, subdivision 4, is amended to read:

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.

Sec. 3. **[626A.42] PERSONAL IDENTIFYING INFORMATION; SEARCH WARRANT AND NOTICE REQUIRED.**

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

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

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

(2) a flight from prosecution;

(3) the destruction of or tampering with evidence;

(4) the intimidation of a potential witness; or

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

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

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

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

(f) "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.

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

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

The term includes information that, in whole or in part, is generated or derived from or obtained by the retrieval of records held by a third party and by the use of technology that enables the user to obtain information in the aggregate or on a mass or comprehensive scale, or that a reasonable person would consider private or otherwise not readily available to the public. The term does not include information that is accessible to the public under

other law or readily available or observable to the public when actually obtained through the direct observation by the line of sight of a person or group of persons.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Subd. 9. **Conflicting provisions superseded.** This section supersedes any conflicting provision in law in effect on March 1, 2014.

Sec. 4. **REVISOR'S INSTRUCTION.**

By January 15, 2015, the revisor of statutes shall prepare a bill for introduction in the 2015 legislative session making conforming changes in law necessitated by this act.

Sec. 5. **REPEALER.**

Minnesota Statutes 2012, section 626A.28, subdivision 2, is 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.