SENATE
STATE OF MINNESOTA
EIGHTY-NINTH SESSION

S.F. No. 686

(SENATE AUTHORS: PETERSEN, B. and Wiger)

DATE	D-PG	OFFICIAL STATUS
02/09/2015	244	Introduction and first reading Referred to Judiciary
02/12/2015	283	Author added Wiger

A bill for an act

relating to public safety; requiring the government to secure a search warrant for the use of unmanned aerial vehicles except in specific circumstances; requiring law enforcement to secure a search warrant in order to receive electronic device location information; amending Minnesota Statutes 2014, section 626A.28, subdivision 3; proposing coding for new law in Minnesota Statutes, chapters 626; 626A.

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

Section 1. **[626.19] USE OF UNMANNED AERIAL VEHICLES.**

Subdivision 1. **Definitions.** (a) For the purposes of this section, the terms in this subdivision have the meanings given them.

(b) "Adverse result" means:

(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) "Governmental entity" means any entity of the state executive, legislative, or judicial branches; the University of Minnesota; the Minnesota State Colleges and Universities; and local entities including, but not limited to, a county; home rule, charter, or statutory city; town; school district; metropolitan or regional agency; public corporation; political subdivision; or special district as defined in section 6.465, subdivision 3.

(d) "Unmanned aerial vehicle" or "UAV" means a powered, aerial vehicle that:

(1) does not carry a human operator;

(2) can fly autonomously or be piloted remotely; and

(3) can be expendable or recoverable.

Subd. 2. **Use of unmanned aerial vehicles limited.** Except as provided in subdivision 3, a governmental entity may not operate an unmanned aerial vehicle without a search warrant.

Subd. 3. **Exceptions.** (a) A governmental entity may operate an unmanned aerial vehicle and disclose information collected from that operation in an emergency situation that involves an imminent threat to the life or safety of a person. A governmental entity that deploys a UAV pursuant to this paragraph must document the factual basis for the emergency on a form created for that purpose by the Bureau of Criminal Apprehension and submit a sworn statement with the district court setting forth the grounds for the emergency use not later than 48 hours after operation of an unmanned aerial vehicle commenced.

(b) A governmental entity may operate an unmanned aerial vehicle to counter a high risk of a terrorist attack by a specific individual or organization if the secretary of the United States Department of Homeland Security determines that credible intelligence indicates that there is this risk.

(c) A governmental entity may operate an unmanned aerial vehicle to collect information from a public area if a court, upon motion, determines that there are specific and articulable facts demonstrating reasonable suspicion of criminal activity, that the operation of the public unmanned aircraft system will uncover such activity, and that alternative methods of data collection are either cost-prohibitive or present a significant risk to any person's bodily safety. A court order under this paragraph shall not be issued for a period greater than 48 hours. Extensions of an order may be granted but 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.

(d) A governmental entity may operate an unmanned aerial vehicle to prevent the loss of life and property in natural or man-made disaster situations and to facilitate the operational planning, rescue, and recovery operations in the aftermath of those disasters.

(e) A governmental entity may operate an unmanned aerial vehicle for non-law enforcement purposes. Information and images gathered when a governmental entity acts under this paragraph may not be used for intelligence purposes or admitted as evidence in a legal, regulatory, or administrative matter unless consensual disclosure is authorized under subdivision 5.

Subd. 4. **Limitations on use.** (a) A governmental entity operating a UAV must fully comply with all Federal Aviation Administration requirements and guidelines.

(b) Acquisition of unmanned aerial vehicles must be approved by the governmental entity's legislative body.

(c) A UAV shall be operated in a manner to collect data only on a clearly and narrowly defined target and to avoid data collection on individuals, homes, or areas other than the defined target.

(d) A governmental entity may not deploy facial recognition or other biometric matching technology via a UAV unless expressly authorized to do so through a court order.

(e) Unmanned aerial vehicles may not be equipped with weapons.

Subd. 5. **Consensual disclosure of information.** Notwithstanding subdivision 6, paragraph (b), a governmental entity may disclose or receive information about any person acquired through the operation of an unmanned aerial vehicle if such person has given written consent to the disclosure.

Subd. 6. **Data retention and classification.** (a) No data collected on an individual, home, or area other than the subject identified in the warrant or order may be used, copied, or disclosed for any purpose except as provided in subdivision 5. Notwithstanding sections 138.163 and 138.17, the data must be deleted as soon as possible, and in no event later than 24 hours after collection.

(b) Data collected pursuant to this section shall be classified as criminal investigative data under section 13.82, subdivision 7.

Subd. 7. **Evidence.** Information obtained or collected by a governmental entity in violation of this section is not admissible as evidence in a criminal prosecution in any court of law in this state.

Subd. 8. **Notice.** (a) Notice must be given to the subject of a search warrant or order issued under this section.

(b) Unless delayed notice is ordered under paragraph (c), the governmental entity shall provide notice to the subject within three days of completing surveillance with a UAV. 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 time period that the subject was under surveillance by a UAV; and

(3) 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 governmental entity may include in the application for a warrant a request for an order to delay the notification required under this section 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 subdivision and any extension granted under paragraph (d),

the governmental entity shall provide the subject a copy of the warrant together with a notice pursuant to paragraph (b).

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

Subd. 9. **Remedies for violation.** A person aggrieved by a governmental entity's violation of this section may bring a civil action against the governmental entity.

Subd. 10. **Reporting.** (a) In June of each year, each governmental entity that uses unmanned aerial vehicles shall report to the legislature and make public on its Web site:

(1) the number of times an unmanned aerial vehicle was used, organized by the types of incidents and the types of justification for deployment;

(2) the number of criminal investigations aided by the use of unmanned aerial vehicles, including a description of how the unmanned aerial vehicle was helpful to each investigation;

(3) the number of uses of unmanned aerial vehicles for reasons other than criminal investigations, including a description of how the unmanned aerial vehicle was helpful in each instance;

(4) the frequency and type of data collected on individuals or areas other than targets; and

(5) the total cost of the entity's unmanned aerial vehicle program.

(b) In January of each year, any judge who has issued a warrant or order under this section that expired during the preceding year, or who has denied approval during that year, 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 unmanned aerial vehicle use 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; and

(6) the identity of the applying governmental entity making the application and the person authorizing the application.

(c) In June of each year, the state court administrator shall transmit to the legislature and post on the Supreme Court's Web site a full and complete report concerning the number of applications for orders authorizing or approving operation of unmanned aerial vehicles or disclosure of information from the operation of unmanned aerial vehicles pursuant to this section and the number of orders and extensions granted or denied pursuant

to this section during the preceding calendar year. The report shall include a summary and analysis of the data required to be filed with the state court administrator by paragraph (b).

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

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, or location information covered by section 626A.43, 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.

Sec. 3. **[626A.43] ELECTRONIC DEVICE LOCATION INFORMATION.**

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 potential witnesses; or

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

(c) "Electronic communication service" has the meaning given in section 626A.01, subdivision 17.

(d) "Electronic device" means a device that enables access to or use of an electronic communication service, remote computing service, or location information service.

(e) "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.

(f) "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.

(g) "Location information service" means the provision of a global positioning service or other mapping, locational, or directional information service.

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

Subd. 2. **Search 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 search warrant. A search warrant granting access to location information must be issued only if the government entity shows that there is probable cause that the person who possesses an electronic device is committing, has committed, or is about to commit a felony-level offense or a qualified domestic violence-related offense, as defined in section 609.02, subdivision 16.

(b) A government entity may obtain location information without a search 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 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) when an emergency involving immediate danger of death or serious physical injury to any person requires obtaining information relating to the emergency without delay, and the search is narrowly tailored to address the emergency.

(c) A government entity exercising the warrantless emergency search authority under paragraph (b), clause (5), must document the basis for determining that an emergency involving immediate danger of death or serious physical injury to a person requires obtaining, without delay, location information relating to the emergency and, not later than 48 hours after the date on which the government entity obtains access to location

information, the government entity shall file with the appropriate court a signed, sworn statement of a supervisory official setting forth the grounds for the emergency access.

Subd. 3. **Notice.** (a) Notice must be given to the owner or user of an electronic device whose location information was obtained by a government entity.

(b) Unless delayed notice is ordered under paragraph (c), the government entity shall provide notice to the owner or user that location information was obtained by the government entity from that owner's or user's electronic device within three days of obtaining the location 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 location information of the owner or user 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 location information was obtained from a provider of electronic communication service or other third party, the identity of the provider of electronic communication service or the third party from whom the information was obtained; 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 subdivision and any extension granted under paragraph (e), the government entity shall provide the owner or user 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 provider of electronic communication service to which 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. **Reporting requirements.** (a) By January 31 of each calendar year, any judge issuing or denying a warrant or receiving a report of emergency access to location

information under subdivision 2 during the preceding calendar year shall report on each warrant or notice of emergency access to the state court administrator:

(1) the date the warrant was applied for or the notice was received;

(2) the agency making the application or notice;

(3) the offense, if any, specified in the warrant application, warrant, or notice;

(4) the nature of the facilities from which, the place where, or the technique by which location information was to be obtained;

(5) the expected number of devices about which location information was obtained;

(6) whether the warrant was granted as applied for, was modified, or was denied; and

(7) the period of disclosures authorized by the warrant, and the number and duration of any extensions of the warrant.

(b) In June of each year, beginning in 2014, the state court administrator shall transmit to the legislature a full and complete record concerning the number of applications for warrant authorizing or requiring the disclosure of location information, the number of times access to location information was obtained pursuant to subdivision 2, paragraph (b), clause (5), and the number of notices of emergency access received under subdivision 2, paragraph (b), during the preceding calendar year. The report shall include a summary and analysis of the data required to be filed with the state court administrator by paragraph (a). The state court administrator is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by paragraph (a).

(c) In June of each year, beginning in 2014, a nonclassified summary of the report shall be made publicly available on the Web site for the state court administrator.

Subd. 5. **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 from the location information 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 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 required information.