CHAPTER 82--S.F.No. 3072

An act relating to public safety; modifying criteria for publishing court of appeals opinions; requiring a government entity to obtain a search warrant before accessing electronic communication information; regulating use of unmanned aerial vehicles; classifying data; making clarifying, conforming, and technical changes; expanding the scope of location tracking warrants; amending Minnesota Statutes 2018, sections 13.82, subdivision 15, by adding a subdivision; 480A.08, subdivision 3; 626A.08, subdivision 2; 626A.26, subdivision 3; 626A.27, subdivision 2; 626A.28, subdivisions 3, 4, 5; 626A.31, subdivision 1; 626A.37, subdivision 4; 626A.42, subdivisions 1, 2, 3, 5; proposing coding for new law in Minnesota Statutes, chapter 626; repealing Minnesota Statutes 2018, sections 626A.28, subdivisions 1, 2; 626A.29; 626A.30.

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

Section 1. Minnesota Statutes 2018, section 13.82, subdivision 15, is amended to read:

Subd. 15. **Public benefit data.** Any law enforcement agency may make any data classified as confidential or protected nonpublic pursuant to subdivision 7 or as private or nonpublic under section 13.825 or 626.19 accessible to any person, agency, or the public if the agency determines that the access will aid the law enforcement process, promote public safety, or dispel widespread rumor or unrest.

Sec. 2. Minnesota Statutes 2018, section 13.82, is amended by adding a subdivision to read:

Subd. 32. **Unmanned aerial vehicles.** Section 626.19 governs data collected, created, or maintained through the use of an unmanned aerial vehicle.

Sec. 3. Minnesota Statutes 2018, section 480A.08, subdivision 3, is amended to read:

Subd. 3. **Decisions.** (a) A decision shall be rendered in every case within 90 days after oral argument or after the final submission of briefs or memoranda by the parties, whichever is later. The chief justice or the chief judge may waive the 90-day limitation for any proceeding before the court of appeals for good cause shown. In every case, the decision of the court, including any written opinion containing a summary of the case and a statement of the reasons for its decision, shall be indexed and made readily available.

(b) The decision of the court need not include a written opinion. A statement of the decision without a written opinion must not be officially published and must not be cited as precedent, except as law of the case, res judicata, or collateral estoppel.

~~(c) The court of appeals may publish only those decisions that:~~

~~(1) establish a new rule of law;~~

~~(2) overrule a previous court of appeals' decision not reviewed by the supreme court;~~

~~(3) provide important procedural guidelines in interpreting statutes or administrative rules;~~

~~(4) involve a significant legal issue; or~~

~~(5) would significantly aid in the administration of justice.~~

~~Unpublished opinions of the court of appeals are not precedential. Unpublished opinions must not be cited unless the party citing the unpublished opinion provides a full and correct copy to all other counsel at least 48 hours before its use in any pretrial conference, hearing, or trial. If cited in a brief or memorandum of law, a copy of the unpublished opinion must be provided to all other counsel at the time the brief or memorandum is served, and other counsel may respond.~~

EFFECTIVE DATE. This section is effective August 1, 2020, and applies to cases filed at the Minnesota Court of Appeals on or after that date.

Sec. 4. **[626.085] SEARCH WARRANT REQUIRED FOR ELECTRONIC COMMUNICATION INFORMATION.**

Subdivision 1. **Definitions.** As used in this section, the following terms have the meanings given them:

(1) "electronic communication" means the transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system;

(2) "electronic communication information" means any information about an electronic communication or the use of an electronic communication service, limited to the contents of electronic communications and precise or approximate location of the sender or recipients at any point during the communication;

(3) "electronic communication service" has the meaning given in section 626A.01, subdivision 17; and

(4) "government entity" has the meaning given in section 626A.42, subdivision 1, paragraph (d).

Subd. 2. **Warrant required; exceptions.** (a) Except as provided in paragraph (b), a government entity must obtain a search warrant to require disclosure of electronic communication information.

(b) A government entity may request disclosure of electronic communication information without a search warrant if the agency has valid consent from one authorized to give it, or exigent circumstances exist where there is a danger to the life or physical safety of an individual.

Subd. 3. **Notice to subject.** A government entity accessing electronic communication information under subdivision 2 must provide notice to the subject of the information consistent with the requirements of subdivision 4 and section 626.16.

Subd. 4. **Notice; temporary nondisclosure of search warrant.** (a) Within a reasonable time but not later than 90 days after the court unseals the search 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 issuance of the warrant or the application;

(2) the date of issuance and the period of authorized, approved, or disapproved collection of electronic communication information, or the denial of the application; and

(3) whether electronic communication information was or was not collected during the period.

(b) A search warrant authorizing collection of electronic communication 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 search 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 search 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 the filing, the documents and materials ordered withheld from filing must be retained by the judge or the judge's designee.

Subd. 5. **Reports.** (a) At the same time as notice is provided according to the requirements of subdivision 4, the issuing or denying judge shall report to the state court administrator:

(1) that a warrant was applied for under this section;

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

(3) the period of collection of electronic communication information 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; and

(5) 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 warrants authorizing the collection of electronic communication 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 section. 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.

(c) Nothing in this section prohibits or restricts a service provider from producing an annual report summarizing the demands or requests it receives under this section.

Sec. 5. **[626.19] USE OF UNMANNED AERIAL VEHICLES.**

Subdivision 1. **Application; definitions.** (a) This section applies to unmanned aerial vehicle data collected, created, or maintained by a law enforcement agency and to law enforcement agencies that maintain, use, or plan to use an unmanned aerial vehicle in investigations, training, or in response to emergencies, incidents, and requests for service. Unmanned aerial vehicle data collected, created, or maintained by a government entity is classified under chapter 13.

(b) For purposes of this section, the following terms have the meanings given:

(1) "government entity" has the meaning given in section 13.02, subdivision 7a, except that it does not include a law enforcement agency;

(2) "law enforcement agency" has the meaning given in section 626.84, subdivision 1;

(3) "unmanned aerial vehicle" or "UAV" means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft; and

(4) "terrorist attack" means a crime that furthers terrorism as defined in section 609.714, subdivision 1.

Subd. 2. **Use of unmanned aerial vehicles limited.** Except as provided in subdivision 3, a law enforcement agency must not use a UAV without a search warrant issued under this chapter.

Subd. 3. **Authorized use.** A law enforcement agency may use a UAV:

(1) during or in the aftermath of an emergency situation that involves the risk of death or bodily harm to a person;

(2) over a public event where there is a heightened risk to the safety of participants or bystanders;

(3) to counter the risk of a terrorist attack by a specific individual or organization if the agency determines that credible intelligence indicates a risk;

(4) to prevent the loss of life and property in natural or man-made disasters and to facilitate operational planning, rescue, and recovery operations in the aftermath of these disasters;

(5) to conduct a threat assessment in anticipation of a specific event;

(6) to collect information from a public area if there is reasonable suspicion of criminal activity;

(7) to collect information for crash reconstruction purposes after a serious or deadly collision occurring on a public road;

(8) over a public area for officer training or public relations purposes; and

(9) for purposes unrelated to law enforcement at the request of a government entity provided that the government entity makes the request in writing to the law enforcement agency and specifies the reason for the request and proposed period of use.

Subd. 4. **Limitations on use.** (a) A law enforcement agency using a UAV must comply with all Federal Aviation Administration requirements and guidelines.

(b) A law enforcement agency must not deploy a UAV with facial recognition or other biometric-matching technology unless expressly authorized by a warrant.

(c) A law enforcement agency must not equip a UAV with weapons.

(d) A law enforcement agency must not use a UAV to collect data on public protests or demonstrations unless expressly authorized by a warrant or an exception applies under subdivision 3.

Subd. 5. **Documentation required.** A law enforcement agency must document each use of a UAV, connect each deployment to a unique case number, provide a factual basis for the use of a UAV, and identify the applicable exception under subdivision 3 unless a warrant was obtained.

Subd. 6. **Data classification; retention.** (a) Data collected by a UAV are private data on individuals or nonpublic data, subject to the following:

(1) if the individual requests a copy of the recording, data on other individuals who do not consent to its release must be redacted from the copy;

(2) UAV data may be disclosed as necessary in an emergency situation under subdivision 3, clause (1);

(3) UAV data may be disclosed to the government entity making a request for UAV use under subdivision 3, clause (9);

(4) UAV data that are criminal investigative data are governed by section 13.82, subdivision 7; and

(5) UAV data that are not public data under other provisions of chapter 13 retain that classification.

(b) Section 13.04, subdivision 2, does not apply to data collected by a UAV.

(c) Notwithstanding section 138.17, a law enforcement agency must delete data collected by a UAV as soon as possible, and in no event later than seven days after collection unless the data is part of an active criminal investigation.

Subd. 7. **Evidence.** Information obtained or collected by a law enforcement agency in violation of this section is not admissible as evidence in a criminal, administrative, or civil proceeding against the data subject.

Subd. 8. **Remedies.** In addition to any other remedies provided by law, including remedies available under chapter 13, an aggrieved party may bring a civil action against a law enforcement agency to prevent or remedy a violation of this section.

Subd. 9. **Public comment.** A law enforcement agency must provide an opportunity for public comment before it purchases or uses a UAV. At a minimum, the agency must accept public comments submitted electronically or by mail. The governing body with jurisdiction over the budget of a local law enforcement agency must provide an opportunity for public comment at a regularly scheduled meeting.

Subd. 10. **Written policies and procedures required.** Prior to the operation of a UAV, the chief officer of every state and local law enforcement agency that uses or proposes to use a UAV must establish and enforce a written policy governing its use, including requests for use from government entities. In developing and adopting the policy, the law enforcement agency must provide for public comment and input as described in subdivision 9. The written policy must be posted on the agency's website, if the agency has a website.

Subd. 11. **Notice; disclosure of warrant.** (a) Within a reasonable time but not later than 90 days after the court unseals a 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 that shall include notice of:

(1) the issuance of the warrant or application;

(2) the date of issuance and the period of authorized, approved, or disapproved collection of information, or the denial of the application; and

(3) whether information was or was not collected during the period.

(b) A warrant authorizing collection of information with a UAV 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 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 warrant must direct that, following the commencement of any criminal proceeding using 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 the filing, the documents and materials ordered withheld from filing must be retained by the judge or the judge's designee.

Subd. 12. **Reporting.** (a) By January 15 of each year, each law enforcement agency that maintains or uses a UAV shall report to the commissioner of public safety the following information for the preceding calendar year:

(1) the number of times a UAV was deployed without a search warrant issued under this chapter, identifying the date of deployment and the authorized use of the UAV under subdivision 3; and

(2) the total cost of the agency's UAV program.

(b) By June 15 of each year, the commissioner of public safety shall compile the reports submitted to the commissioner under paragraph (a), organize the reports by law enforcement agency, submit the compiled report to the chairs and ranking minority members of the senate and house of representatives committees having jurisdiction over data practices and public safety, and make the compiled report public on the department's website.

(c) By January 15 of each year, a judge who has issued or denied approval of a warrant under this section that expired during the preceding year shall report to the state court administrator:

(1) that a warrant or extension was applied for;

(2) the type of warrant or extension applied for;

(3) whether the warrant or extension was granted as applied for, modified, or denied;

(4) the period of UAV use authorized by the warrant and the number and duration of any extensions of the warrant;

(5) the offense specified in the warrant or application or extension of a warrant; and

(6) the identity of the law enforcement agency making the application and the person authorizing the application.

(d) By June 15 of each year, the state court administrator shall submit to the chairs and ranking minority members of the senate and house of representatives committees or divisions having jurisdiction over data practices and public safety and post on the supreme court's website a full and complete report concerning the number of applications for warrants authorizing or approving use of UAVs or disclosure of information from the use of UAVs under this section and the number of warrants and extensions granted or denied under this section during the preceding calendar year. The report must include a summary and analysis of the data required to be filed with the state court administrator under paragraph (c).

EFFECTIVE DATE. This section is effective August 1, 2020, provided that the chief law enforcement officers shall adopt the written policy required under subdivision 10 no later than February 15, 2021.

Sec. 6. Minnesota Statutes 2018, section 626A.08, subdivision 2, is amended to read:

Subd. 2. **Application and orders.** (a) 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 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.

(b) Notwithstanding paragraph (a), the filing, sealing, and reporting requirements for applications made and warrants issued under this chapter that involve location information of electronic devices, as defined in section 626A.42, are governed by section 626A.42, subdivision 4. However, applications and warrants, or portions of applications and warrants, that do not involve location information of electronic devices continue to be governed by paragraph (a).

EFFECTIVE DATE. This section is effective the day following final enactment.

Sec. 7. Minnesota Statutes 2018, section 626A.26, subdivision 3, is amended to read:

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 626.085, 626A.05 to 626A.09, or 626A.28~~, or 626A.29~~.

Sec. 8. Minnesota Statutes 2018, section 626A.27, subdivision 2, is amended to read:

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 626.085; 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.

Sec. 9. Minnesota Statutes 2018, 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~~, 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. 10. Minnesota Statutes 2018, 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. 11. Minnesota Statutes 2018, section 626A.28, subdivision 5, is amended to read:

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~~ section 626.085 or 626A.26 to 626A.34.

Sec. 12. Minnesota Statutes 2018, section 626A.31, subdivision 1, is amended to read:

Subdivision 1. **Payment.** Except as otherwise provided in subdivision 3, a governmental entity obtaining ~~the contents of communications,~~ records~~,~~ or other information under ~~sections~~ section 626A.27~~,~~ or 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.

Sec. 13. Minnesota Statutes 2018, section 626A.37, subdivision 4, is amended to read:

Subd. 4. **Nondisclosure of existence of pen register, trap and trace device, or mobile tracking device.** (a) 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.

(b) Paragraph (a) does not apply to an order that involves location information of electronic devices, as defined in section 626A.42. Instead, the filing, sealing, and reporting requirements for those orders are governed by section 626A.42, subdivision 4. However, any portion of an order that does not involve location information of electronic devices continues to be governed by paragraph (a).

EFFECTIVE DATE. This section is effective the day following final enactment.

Sec. 14. Minnesota Statutes 2018, section 626A.42, subdivision 1, is amended to read:

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 or unique identifier that, in whole or in part, is generated or derived from or obtained by the operation of an electronic device or unique identifier.

(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 or unique identifier.

(i) "Unique identifier" means any numeric or alphanumeric string that is associated with a single entity or account within a given electronic communication application or service.

Sec. 15. Minnesota Statutes 2018, section 626A.42, subdivision 2, is amended to read:

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 or unique identifier 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 or is using a unique identifier 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 or request for emergency services;

(3) with the informed, affirmative, documented consent of the owner or user of the electronic device or unique identifier;

(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 or is using a unique identifier.

Sec. 16. Minnesota Statutes 2018, section 626A.42, subdivision 3, is amended to read:

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 or unique identifier location information.

Sec. 17. Minnesota Statutes 2018, section 626A.42, subdivision 5, is amended to read:

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 or unique identifier'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.

Sec. 18. **REPEALER.**

Minnesota Statutes 2018, sections 626A.28, subdivisions 1 and 2; 626A.29; and 626A.30, are repealed.

Presented to the governor May 14, 2020

Signed by the governor May 16, 2020, 11:06 a.m.