Senator ..... moves to amend S.F. No. 1263 as follows:

Delete everything after the enacting clause and insert:

"Section 1. Minnesota Statutes 2018, section 3.8843, subdivision 7, is amended to read:

Subd. 7. **Expiration.** This section expires June 30, ~~2019~~ 2026.

Sec. 2. Minnesota Statutes 2018, section 13.201, is amended to read:

13.201 RIDESHARE DATA.

The following data on participants, collected by ~~the Minnesota Department of Transportation and the Metropolitan Council~~ a government entity to administer rideshare programs, are classified as private under section 13.02, subdivision 12, or nonpublic under section 13.02, subdivision 9: residential address and telephone number; beginning and ending work hours; current mode of commuting to and from work; place of employment; photograph; biographical information; and type of rideshare service information requested.

Sec. 3. Minnesota Statutes 2018, section 13.72, subdivision 19, is amended to read:

Subd. 19. **Transit customer data.** (a) Data on applicants, users, and customers of public transit collected by or through ~~the Metropolitan Council's~~ a government entity's personalized web services or the Metropolitan Council's regional fare collection system are private data on individuals. As used in this subdivision, the following terms have the meanings given them:

(1) "regional fare collection system" means the fare collection system created and administered by the council that is used for collecting fares or providing fare cards or passes for transit services which includes:

(i) regular route bus service within the metropolitan area and paratransit service, whether provided by the council or by other providers of regional transit service;

(ii) light rail transit service within the metropolitan area;

(iii) rideshare programs administered by the council;

(iv) special transportation services provided under section 473.386; and

(v) commuter rail service;

(2) "personalized web services" means services for which transit service applicants, users, and customers must establish a user account; and

(3) "metropolitan area" means the area defined in section 473.121, subdivision 2.

(b) ~~The council~~ A government entity may disseminate data on user and customer transaction history and fare card use to government entities, organizations, school districts, educational institutions, and employers that subsidize or provide fare cards to their clients, students, or employees. "Data on user and customer transaction history and fare card use" means:

(1) the date a fare card was used;

(2) the time a fare card was used;

(3) the mode of travel;

(4) the type of fare product used; and

(5) information about the date, time, and type of fare product purchased.

Government entities, organizations, school districts, educational institutions, and employers may use customer transaction history and fare card use data only for purposes of measuring and promoting fare card use and evaluating the cost-effectiveness of their fare card programs. If a user or customer requests in writing that the council limit the disclosure of transaction history and fare card use, the council may disclose only the card balance and the date a card was last used.

(c) ~~The council~~ A government entity may disseminate transit service applicant, user, and customer data to another government entity to prevent unlawful intrusion into government electronic systems, or as otherwise provided by law.

Sec. 4. Minnesota Statutes 2018, section 171.306, subdivision 2, is amended to read:

Subd. 2. **Performance standards; certification; manufacturer and provider requirements.** (a) The commissioner shall establish performance standards and a process for certifying devices used in the ignition interlock program, except that the commissioner may not establish standards that, directly or indirectly, require devices to use or enable location tracking capabilities without a court order.

(b) The manufacturer of a device must apply annually for certification of the device by submitting the form prescribed by the commissioner. The commissioner shall require manufacturers of certified devices to:

(1) provide device installation, servicing, and monitoring to indigent program participants at a discounted rate, according to the standards established by the commissioner; ~~and~~

(2) include in an ignition interlock device contract a provision that a program participant who voluntarily terminates participation in the program is only liable for servicing and monitoring costs incurred during the time the device is installed on the motor vehicle, regardless of whether the term of the contract has expired; and

(3) include in any contract between the manufacturer and an Internet or cellular service provider a requirement that the provider not sell or transfer to, or share with, another entity, information about the actual or approximate location of the device at any point in time unless required to do so under a court order or warrant.

(c) The manufacturer of a certified device must include with an ignition interlock device contract a separate notice to the program participant regarding any location tracking capabilities of the device.

(d) The manufacturer of a certified device may not sell or transfer to, or share with, any entity, other than the Department of Public Safety, information about the actual or approximate location of a device at any point in time unless required to do so under a court order or warrant.

Sec. 5. Minnesota Statutes 2018, section 363A.35, subdivision 3, is amended to read:

Subd. 3. **Access to closed files.** (a) Except as otherwise provided in this subdivision, human rights investigative data contained in a closed case file are private data on individuals or nonpublic data. The name and address of the charging party and respondent, factual basis of the allegations, the statute under which the action is brought, the part of the summary of the investigation that does not contain identifying data on a person other than the complainant or respondent, and the commissioner's memorandum determining whether probable cause has been shown are public data.

(b) The commissioner may make human rights investigative data contained in a closed case file inaccessible to the charging party or the respondent in order to protect medical or other security interests of the parties or third persons.

(c) Except for paragraph (b), when the charging party files a case in district court, the commissioner may provide private data or nonpublic data in a closed case file to the charging party and respondent.

Sec. 6. Minnesota Statutes 2018, section 465.719, subdivision 14, is amended to read:

Subd. 14. **Data classification.** The following data created, collected, or maintained by a corporation subject to this section are classified as private data under section 13.02,

subdivision 12, or as nonpublic data under section 13.02, subdivision 9: (1) data relating either (i) to private businesses consisting of financial statements, credit reports, audits, business plans, income and expense projections, customer lists, balance sheets, income tax returns, and design, market, and feasibility studies not paid for with public funds, or (ii) to enterprises operated by the corporation that are in competition with entities offering similar goods and services, so long as the data are not generally known or readily ascertainable by proper means and disclosure of specific data would cause harm to the competitive position of the enterprise or private business, provided that the goods or services do not require a tax levy; and (2) any data identified in ~~sections~~ section 13.201 ~~and 13.72, subdivision 9,~~ collected or received by a transit organization.

Sec. 7. **[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 access electronic communication information.

(b) A government entity may access 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 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 electronic communication information, or the denial of the application; and

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

(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 such 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) the fact that a warrant was applied for under this section;

(2) the fact that 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. 8. **[626.19] USE OF UNMANNED AERIAL VEHICLES.**

Subdivision 1. **Application; definitions.** (a) This section applies 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.

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

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

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

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

Subd. 3. **Authorized use.** (a) A law enforcement agency may use a UAV during or immediately after an emergency situation that involves the risk of death or serious physical harm to a person.

(b) A law enforcement agency may use a UAV over a public event where there is a substantial risk to the safety of participants or bystanders. If a law enforcement agency collects information under this paragraph it must document each use, connect each deployment to a unique case number, and provide a description of the facts giving rise to a substantial risk.

(c) A law enforcement agency may operate a UAV to counter a high risk of a terrorist attack by a specific individual or organization if the agency determines that credible intelligence indicates this risk.

(d) A law enforcement agency may use a UAV to prevent the loss of life and property in natural or man-made disasters and to facilitate the operational planning, rescue, and recovery operations in the aftermath of these disasters.

(e) A law enforcement agency may use a UAV for officer training purposes.

(f) A law enforcement agency may operate a UAV for a non-law-enforcement purpose at the request of a government entity, as defined in section 13.02, subdivision 7a, provided that the government entity makes the request in writing and specifies the reason for the request and proposed period of use.

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

(b) The governing body overseeing the law enforcement agency must approve the agency's acquisition of a UAV.

(c) Unless specifically authorized in a warrant, a law enforcement agency must use a UAV to collect data only on a clearly and narrowly defined target and avoid data collection on individuals, homes, or areas other than the defined target.

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

(e) A law enforcement agency may not equip a UAV with weapons.

(f) A law enforcement agency may 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. A law enforcement agency must document which exception applies or whether a warrant was obtained.

Subd. 5. **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, paragraph (a);

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

(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. 6. **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. 7. **Remedies.** An aggrieved party may initiate a civil action against a law enforcement agency to obtain all appropriate relief to prevent or remedy a violation of this section, including remedies available under chapter 13.

Subd. 8. **Written policies required.** The chief officer of every state and local law enforcement agency that uses or plans to use a UAV must establish and enforce a written policy governing UAV use. The agency must post the written policy on its website, if the agency has a website.

Subd. 9. **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 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 information, or the denial of the application; and

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

(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 such filing, the documents and materials ordered withheld from filing must be retained by the judge or the judge's designee.

Subd. 10. **Reporting.** (a) By January 15 of each year, each law enforcement agency that deploys 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, organized by the types of incidents and the types of justification for deployment;

(2) the number of criminal investigations aided by the deployment of UAVs;

(3) the number of deployments of UAVs for reasons other than criminal investigations; and

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

(b) By June 15 of each year, the commissioner of public safety shall compile a full and complete report summarizing the information submitted to the commissioner under paragraph (a), and submit the report to the chairs and ranking minority members of the senate and house of representatives committees having jurisdiction over criminal justice and public safety issues and make the report public on the department's website.

(c) By January 15 of each year, any judge who has issued a warrant 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 a warrant or extension was applied for;

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

(3) the fact that the warrant or extension was granted as applied for, was modified, or was 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 transmit to the chairs and ranking minority members of the senate and house of representatives committees having jurisdiction over criminal justice and public safety issues and post on the supreme court's website a full and complete report concerning the number of applications for warrants authorizing or approving operation of UAVs or disclosure of information from the operation 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 by paragraph (c).

Sec. 9. 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).

Sec. 10. 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~~ section 626.085, 626A.05 to 626A.09~~,~~ or 626A.28~~, or 626A.29~~.

Sec. 11. 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. 12. 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. 13. 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. 14. 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. 15. 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. 16. 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).

Sec. 17. **REPEALER.**

Minnesota Statutes 2018, sections 13.72, subdivision 9; 626A.28, subdivisions 1 and 2; 626A.29; and 626A.30, are repealed.

Sec. 18. **EFFECTIVE DATE.**

Sections 1, 2, 6, 9, and 16 are effective the day following final enactment."

Delete the title and insert:

"A bill for an act

relating to privacy; delaying expiration of the legislative commission on data practices; expanding rideshare data classification to include all government entities; providing unredacted information to the parties in a closed case under certain circumstances; enabling reporting of information related to use of electronic device location tracking warrants; requiring a government entity to obtain a search warrant before accessing electronic communication information; restricting the sharing of location information on ignition interlock devices in certain circumstances; regulating the use of unmanned aerial vehicles by law enforcement agencies; amending Minnesota Statutes 2018, sections 3.8843, subdivision 7; 13.201; 13.72, subdivision 19; 171.306, subdivision 2; 363A.35, subdivision 3; 465.719, subdivision 14; 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; proposing coding for new law in Minnesota Statutes, chapter 626; repealing Minnesota Statutes 2018, sections 13.72, subdivision 9; 626A.28, subdivisions 1, 2; 626A.29; 626A.30."