MN HOUSE RESEARCH

Bill Summary

H.F. 631

First engrossment

Subject	Data Practices and Civil Law Policy Omnibus Bill
Authors	Lesch
Analyst	Nathan Hopkins Mary Mullen
Date	March 19, 2019

Overview

This is an omnibus bill covering data practices and civil law policy.

Article 1: Government Data Practices Provisions

This article contains policy provisions regarding government data practices.

Section	Description
1	***Data Breach Notification:*** **Definitions.** Removes the intent requirement from the data breach notification statute. *From H.F. 54 (Scott and others)*
2	***Transit Data:*** **Rideshare data.** Expands a private/nonpublic classification of rideshare data so that it includes rideshare programs administered by any government entity. Adds "place of employment, photograph, [and] biographical information" to the existing list of data classified as private/nonpublic. *From H.F. 361, as amended (Liebling and others)*
3	***Transit Data:*** **Transit customer data.** Expands a private/nonpublic classification of public transit data so that it includes public transit services administered by any government entity. *From H.F. 361, as amended (Liebling and others)*
4	***Ignition Interlock:*** **Definitions** Amends the definition of "location tracking capabilities" in the ignition interlock device program statute to specify that the term includes direct or indirect location tracking via GPS or cell-site location information. *From H.F. 1567 (Lesch and others)*

Section	Description
5	***Transit Data:*** **Data classification.** Conforming change given the repealer at section 18. *From H.F. 361, as amended (Liebling and others)*
6	***Tracking Warrants:*** **Applications and orders.** Amends the statute concerning the sealing and disclosure of a wiretap warrant to distinguish location-tracking warrants, which have their own sealing and disclosure requirements under section 626A.42. Also clarifies procedure for filing applications and warrants under seal. *From H.F. 631, as amended (Lesch)*
7	***Tracking Warrants:*** **Notice of order.** For wiretap warrants, amends the notice requirement so that the law enforcement agency, rather than the judge, will notify the subject regarding the existence of the warrant and other specified information. *From H.F. 631, as amended (Lesch)*
8	***Tracking Warrants:*** **Nondisclosure of existence of pen register, trap and trace device, or mobile tracking device.** Amends the statute concerning the sealing and disclosure of a warrant for a pen register, trap-and-trace device, or mobile tracking device to distinguish location-tracking warrants, which have their own sealing and disclosure requirements under section 626A.42. *From H.F. 631, as amended (Lesch)*
9	***Tracking Warrants:*** **Notice required.** For pen register, trap-and-trace device, or mobile tracking device warrants, amends the notice requirement so that the law enforcement agency, rather than the judge, will notify the subject regarding the existence of the warrant and other specified information. *From H.F. 631, as amended (Lesch)*
10	***Tracking Warrants:*** **Mobile tracking device.** Amends the definition of a "mobile tracking device" to distinguish it from a cell site simulator device or any other device that may be used to access information concerning the location of an electronic device that, in whole or in part, is generated from the operation of the electronic device. *From H.F. 631, as amended (Lesch)*

Section	Description
11	***Tracking Warrants:*** **Electronic device location information.** **Subd. 1. Definitions.** At paragraph (h), amends the definition of "tracking warrant" to specify that it includes, but is not limited to the use of a cell site simulator device. At paragraph (i), creates a new definition of "cell site simulator device." **Subd. 4. Notice; temporary nondisclosure of tracking warrant.** Amends the notice requirement so that the law enforcement agency, rather than the judge, will notify the subject regarding the existence of the warrant and other specified information. Also, throughout this section, any use of the general term "warrant" is changed to "tracking warrant" to further clarify that this section applies only to tracking warrants. *From H.F. 631, as amended (Lesch)*
12	***Electronic Communications:*** **Short title.** The act may be cited as the "Minnesota Electronic Communications Privacy Act." *From H.F. 1197 (Lesch and others)*
13	***Electronic Communications:*** **Definitions.** Defines the following terms: "adverse result," "authorized possessor," "electronic communication," "electronic communication information," "electronic communication service," "electronic device," "electronic device information," "electronic information," "government entity," "service provider," "specific consent," and "subscriber information." *From H.F. 1197 (Lesch and others)*
14	***Electronic Communications:*** **Government entity prohibitions; exceptions.** **Subd. 1. Prohibitions.** Prohibits a government entity from: (1) compelling or incentivizing a service provider to produce or allow government access to electronic communication information; (2) compelling any person other than the authorized possessor of a device to allow access to the electronic device information; or (3) accessing electronic device information by physical interaction or electronic communication with the device. **Subd. 2. Exceptions.** Paragraph (1) provides that—with a proper court-issued search warrant or wiretap order—a government entity may compel a service provider or a person other than the authorized possessor of a device to produce or allow access to electronic communication information. Paragraph (2) allows a government entity to access electronic device information by physical interaction or electronic communication with the device under circumstances specified in clauses (i) through (v).

Section	Description

Subd. 3. Warrant. Adds additional requirements for a court issuing a warrant for electronic communication information. Allows the court to appoint a special master to oversee execution of the warrant.

Subd. 4. Service provider; voluntary disclosure. Allows a service provider to voluntarily disclose electronic communication information or subscriber information. But requires a government entity who receives that voluntarily disclosed information to destroy it unless the entity has certain consents or a court order. Also imposes requirements and restrictions on a court order to retain such voluntarily disclosed information.

Subd. 5. Emergency. Permits a government entity to obtain electronic communication information in a life-threatening emergency situation, but requires the entity to seek court approval of that action after the fact.

Subd. 6. Subpoena. Specifies that this section does not limit the ability of a government entity to obtain certain information via subpoena.

Subd. 7. Recipient voluntary disclosure. Specifies that this section does not prohibit a person who receives an electronic communication from voluntarily disclosing that information to a government entity.

Subd. 8. Construction. Provides that courts should not interpret this section to expand any existing government authority to access electronic information.

From H.F. 1197 (Lesch and others)

15 ***Electronic Communications:*** **Notices required.**

Subd. 1. Notice. Requires a government entity that obtains electronic communication information must notify targets of the warrant.

Subd. 2. Emergency; delay of notice. For emergency situations under section 14, subdivision 5, allows a government entity to request a court order to delay the notice required under subdivision 1.

Subd. 3. No identified target. For instances where a government entity obtains electronic communication information in an emergency situation, but no target is identified, requires the entity to submit required information to the Minnesota Supreme Court, which must publish reports on the information.

Subd. 4. Service provider. Specifies that nothing in this section prevents a service provider from disclosing information about a request for electronic information.

From H.F. 1197 (Lesch and others)

Section	Description
16	***Electronic Communications:*** **Remedies.** **Subd. 1. Suppression.** Permits a party in any trial, hearing, or legal proceeding to move to suppress electronic communication information obtained in violation of this act, or the state or federal constitutions. **Subd. 2. Attorney general.** Empowers the attorney general to file a civil lawsuit against a government entity to compel compliance with this act. **Subd. 3. Petition.** Provides that any person whose information is sought in violation of this act or the state or federal constitutions may petition the relevant court for relief. **Subd. 4. No cause of action.** Provides immunity from suit for corporations that disclose information in compliance with this act. *From H.F. 1197 (Lesch and others)*
17	***Electronic Communications:*** **Reports.** Requires the judge who issues or denies a warrant for electronic communication information under section 14 to report specified information to the state court administrator, who must prepare a biennial report to the legislature regarding the warrants. *From H.F. 1197 (Lesch and others)*
18	***Transit Data:*** **Repealer.** Repeals a duplicative data classification for rideshare data. *From H.F. 361, as amended (Liebling and others)*

Article 2: General Civil Law Provisions

Section	Description
1	**Employee username and password privacy protection.** **Subd. 1. Definitions.** Provides definition for the following terms: • "applicant" is a person applying for employment • "employee" is a person who works for wages or other compensation • "employer" is a person who employs people or acts on behalf of an employer in relation to their employees

Section	Description

- "personal social media account" is an electronic account or service where users create user generated content such as videos, photos, written content, messages, or emails, but does not include an employer or school provided account or an account the employer or school requested the employee to sign up for

- "specific content" means data or information on a personal social media that can be identified as information unique to the account

Subd. 2. Employer access prohibited. Prohibits an employer from requiring or forcing an employee or applicant for a job to:

- tell the employer their username or password to a social media account

- show the employer their social media account

- give the employer access by adding them as a friend or follower to a private account or require the employee to make an account public

Subd. 3. Employer actions prohibited. Prohibits an employer from:

- taking negative action against an employee if they refuse to share social media information

- refusing to hire an applicant for a job because they refuse to share their social media information

Provides an exception to subdivisions 2 and 3 for law enforcement applicants.

Subd. 4. Employer actions permitted. Provides that employers can access information about employees and applicants when it is publically available, and allows employers to comply with other state and federal laws or industry or regulator standards as required. This section also allows employers to request specific content on an employee or applicant's social media account so that the employer can verify that it does not violate laws and regulatory requirements. If the employer is shown that there may be evidence through social media of certain prohibited activities, then the employer can also ask to see specific content on a personal media site to investigate an allegation that:

- the employee has stolen proprietary or confidential information or financial data or violated the law;

- committed an act of unlawful harassment; or

- used the account during work hours when it is prohibited or used the account for business purposes when it has been prohibited.

Section	Description
	Subd. 5. Employer protected if access inadvertent; use prohibited. Provides that an employer has not violated the provisions of this section by receiving an employee's password or protected materials through virus scans or other employer monitoring of the network on employer provided devices, but the employer may not use the information to access the employee's social media account or share the information with anyone. This section provides the employer should delete the information as soon as practical. **Subd. 6. Enforcement.** An employer, an employee of an employer, or an agent of an employer is liable for actual damages, including pain and suffering, equitable relief, and reasonable attorneys' fees and costs for violations of this section if an employee has been injured or an employee's reputation has been injured due to the violation. **Subd. 7. Severability.** Provides that the provisions in this chapter are severable. **Effective date.** Provides that this section is effective on August 1, 2019, and applies to actions which occur on or after that date.
2	**Actions under section 257.55, subdivision 1, paragraph (a), (b), or (c).** Changes when an action for nonpaternity can be brought in cases where the parents are married from two years after the father had a reason to believe he is not the father to three years. Removes the bar to bringing an action from three years after the child's birth.
3	**Actions under other paragraphs of section 257.55, subdivision 1.** Creates a limit to the time in which an action for nonpaternity can be brought after a father starts holding a child out as his own without paternity being established under any other section.
4	**Nonexistence of father-child relationship.** Provides what should be in a petition for nonpaternity, what factors the court should consider in determining nonpaternity, requires the proof to declare nonpaternity be proven by clear and convincing evidence, and provides what the court order must contain if the court grants the relief requested. Current law does not provide a specific procedure for declaring nonpaternity.
5	**Action to vacate a recognition.** Change the amount of time a person has to bring an action to vacate a recognition of paternity to allow an action to be brought within three years of the time the person believes the father listed on the recognition of parentage is not the father of the child. This section is effective on August 1, 2018, and applies to recognition of parentage signed on or after that date.

Section	Description
6	**Reopening.** Provides that in actions to review a divorce decree for issues of mistake, fraud, or other reasons, when the action is to declare the nonexistence of the father and child relationship then the action must be brought within a reasonable time and within three years of the time the person has reason to believe the father is not the father of the child. Current law for all motions under this section is that the action must be brought within one year of the entry of the judgment and decree.
7	**Implementation; administration.** Requires court in each judicial district in the state to include information about parenting education programs on the court's website. Under current law, parties to disputed custody and parenting time cases are required to go to a parenting education program, and this bill specifies that when the parties have not agreed to custody or parenting time they will need to attend the program.
8	**Attendance.** Specifies that parties need to attend the class in person or online before the Initial Case Management Conference (ICMC) and within 30 days of the initial filing in the case, and that prior to the ICMC the court must notify parties that they have the option to resolve their disputes through private mediation.
9	**General.** Requires the court to use a rebuttable presumption that the child shall have the maximum amount of time with each parent, unless the court finds the parenting time will endanger the child's physical, mental, or emotional health or safety. This section also provides parents should get close to 50 percent of the parenting time and if the court does not award the 50 percent then the court must include in a court order the reasons for the deviation and show that the findings provide by clear and convincing evidence that one of the parents meets a qualification that requires the parenting time to be limited, or that the distance between the parties is so great that the parenting time plan would be impractical, or because the child's medical condition requires it. This section removes the ability of the court to consider the child's age when making determinations about parenting time, but does allow the court to issue a graduate reunification parenting time plan for children under the age of one year or when the parent and child have been separated for a long period of time. This section also prohibits the court to consider a parents gender or marital status in issuing a court order related to parenting time, and requires the court to evaluate whether a parent has engaged in interfering with the other parent's time with the child, provided false allegations of domestic abuse, or chronically denied parenting time to the other parent to gain advantages in custody matters.

Section	Description
10	**When required; exception.** Amends the requirements for background studies for parents who are guardians of their children. Under existing law, when a child with a disability is raised by their parent and then that parent becomes the guardian of that child, the parent does not have to provide a background check unless the attorney appointed for the ward (the parent's child) has requested one. The law requires that the child turn 18 while in the parent's care. This bill amends the background check exemption to extend to parents when their children are under their care but go into a residential facility before they turn 18. This section applies to background checks required on or after August 1, 2019.