State of Minnesota

HOUSE OF REPRESENTATIVES

NINETY-FIRST SESSION

H. F. No. 4436

1.1   A bill for an act

1.2   relating to commerce; prohibiting geolocation and smart phone monitoring of
1.3   another in certain circumstances; providing a cause of action to individuals when
1.4   their geological information and other smart phone data has been recorded or
1.5   shared by another; proposing coding for new law in Minnesota Statutes, chapter
1.6   325F.

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

1.8   Section 1. **[325F.6985] SMART PHONE MONITORING.**

1.9   Subdivision 1. **Definitions.** (a) For the purposes of this section the following terms have

1.10   the meanings given.

1.11   (b) "Geolocation information" means any information generated by or derived in whole

1.12   or in part from the operation or use of an electronic communications device and sufficient

1.13   to identify the street name and name of the city or town where the device is located.

1.14   Geolocation information includes information provided by a global positioning service or

1.15   any other mapping, locational, or directional information service. Geolocation information

1.16   does not include information that is in the content of a communication; the Internet Protocol

1.17   address of the home, business, or billing address of the individual; or any component parts

1.18   of the addresses alone.

1.19   (c) "Smart phone" has the meaning given in section 325F.698.

1.20   Subd. 2. **Smart phone monitoring; prohibitions.** (a) Smart phone software and

1.21   applications must appear on a phone in a conspicuous manner when the software or

1.22   application allows:

1.23   (1) geolocation information to be shared with another remote user;

2.1   (2) saved or stored texts to be read by another remote user; or

2.2   (3) remote access to the phone user's microphone or camera, or data from the camera or

2.3   microphone to be shared or recorded by another remote user.

2.4   (b) For the purposes of this section, an application appears in a conspicuous manner if

2.5   it is displayed as an icon that can be found by a reasonable person. Software or applications

2.6   that track or record geolocation information, allow saved or stored texts to be read by another

2.7   remote user, or allow remote access to the phone user's microphone or camera must require

2.8   at least two forms of identity verification before being installed or used on a device, and

2.9   must accurately record the identity of the software or application user. Two-factor

2.10   authentication required under this paragraph must occur at the time of installation, seven

2.11   days after installation, and every 30 days after installation. When the two-factor authentication

2.12   is not completed, the software must be disabled.

2.13   (c) Except as provided in subdivision 3, an individual is prohibited from installing an

2.14   application or software on the smart phone of another individual that allows the collection,

2.15   recording, sharing, or distribution of geolocation information, microphone or camera data,

2.16   or texts of the other individual.

2.17   (d) Nothing in this section prevents an individual from installing software or an

2.18   application on a smart phone that allows the individual to share the individual's own

2.19   geolocation information or that allows a user to authorize a software application access the

2.20   microphone or camera on the individual's own smart phone. Nothing in this section prevents

2.21   an application or software from being locked so an employee or child cannot remove or

2.22   alter the software to secure the smart phone's location.

2.23   Subd. 3. **Smart phone monitoring; exceptions.** This section does not apply to:

2.24   (1) the collection of a minor child's geolocation information by the child's parent or legal

2.25   guardian;

2.26   (2) the collection of a minor child's geolocation information by a school or school district

2.27   providing a smart phone to a minor child, if the child and the child's parent or legal guardian

2.28   has been provided a written notice that geolocation information is collected by the smart

2.29   phone;

2.30   (3) the collection of an employee's geolocation information by an employer for a

2.31   legitimate business purpose, if the employer has provided the smart phone to an employee

2.32   and given the employee written notice that geolocation information is collected; and

3.1   (4) the collection or viewing of geolocation information, access to text or electronic

3.2 communication, or access to a microphone or camera or data pursuant to a court order or

3.3 warrant, or access by law enforcement authorized by state or federal law.

3.4   Subd. 4. **Remedies.** (a) In addition to any remedies available under law and the remedies

3.5 available under section 8.31, an individual whose geolocation information, text, data, camera,

3.6 or microphone was accessed, recorded, or shared has a cause of action against the person

3.7 who violated the provision of subdivision 2, including against (1) an individual who installed

3.8 or used an application to collect the geolocation information of another, and (2) the person

3.9 who provided the software or application and failed to meet the standards required in

3.10 subdivision 2, paragraph (a).

3.11   (b) The court may award the following damages to a prevailing plaintiff from a person

3.12 found liable under subdivision 2:

3.13   (1) general and special damages, including any financial losses and damages for mental

3.14 anguish suffered by an individual due to being tracked or having the individual's geolocation

3.15 information, texts, data, camera, or microphone accessed by another; and

3.16   (2) court costs, fees, and reasonable attorney fees.

3.17   **EFFECTIVE DATE.** This section is effective August 1, 2020, and applies to smart

3.18 phone software and applications installed or used on or after that date.