State of Minnesota

HOUSE OF REPRESENTATIVES

NINETY-SECOND SESSION

H. F. No. 4235

03/14/2022 Authored by Robbins, O'Neill, Scott, Grossell, Nash and others
The bill was read for the first time and referred to the Committee on Commerce Finance and Policy

A bill for an act

relating to commerce; prohibiting geolocation and smartphone monitoring of another in certain circumstances; providing a cause of action to individuals when geolocation information and other smartphone data has been recorded or shared; proposing coding for new law in Minnesota Statutes, chapter 325F.

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

Section 1. **[325F.6985] SMARTPHONE MONITORING; GEOLOCATION TRACKING CONSENT REQUIRED.**

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

(b) "Geolocation information" means any information (1) generated by or derived in whole or in part from the operation or use of an electronic communications device, and (2) sufficient to identify the street name and name of the city or town where the device is located. Geolocation information includes information provided by a global positioning service or any other mapping, locational, or directional information service. Geolocation information does not include information that is in the content of a communication; the Internet Protocol address of the home, business, or billing address of the individual; or any component parts of the addresses alone.

(c) "Smartphone" has the meaning given in section 325F.698.

Subd. 2. **Smartphone monitoring; prohibitions.** (a) Smartphone software and applications must appear on a phone in a conspicuous manner when the software or application allows:

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

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

(3) remote access to the phone user's microphone or camera, or data from the camera or microphone to be shared or recorded by another remote user.

(b) For the purposes of this section, an application appears in a conspicuous manner if it is displayed as an icon that can be found by a reasonable person. Software or applications that track or record geolocation information, allow saved or stored texts to be read by another remote user, or allow remote access to the phone user's microphone or camera must require at least two forms of identity verification before being installed or used on a device, and must accurately record the identity of the software or application user. Two-factor authentication required under this paragraph must occur at the time of installation, seven days after installation, and every 30 days after installation. When the two-factor authentication is not completed, the software must be disabled.

(c) Except as provided in subdivision 3, an individual is prohibited from installing an application or software on the smartphone of another individual that allows the collection, recording, sharing, or distribution of geolocation information, microphone or camera data, or texts of the other individual.

(d) Nothing in this section prevents an individual from installing software or an application on a smartphone that allows the individual to share the individual's own geolocation information or that allows a user to authorize a software application to access the microphone or camera on the individual's own smartphone. Nothing in this section prevents an application or software from being locked so an employee or child cannot remove or alter the software to secure the smartphone's location.

Subd. 3. **Smartphone monitoring; exceptions.** This section does not apply to:

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

(2) the collection of a minor child's geolocation information by a school or school district providing a smartphone to a minor child, if the child and the child's parent or legal guardian has been provided a written notice that geolocation information is collected by the smartphone;

(3) the collection of an employee's geolocation information by an employer for a legitimate business purpose, if the employer has provided the smartphone to an employee and given the employee written notice that geolocation information is collected; and

(4) the collection or viewing of geolocation information, access to text or electronic communication, or access to a microphone, camera, or data (i) pursuant to a court order or warrant, or (ii) by law enforcement authorized by state or federal law.

Subd. 4. **Geolocation tracking; consent required.** (a) Except as otherwise provided in this section, it is unlawful for any person to use a device that tracks the geolocation information of another person to (1) intentionally intercept, (2) endeavor to intercept, or (3) procure any other person to intercept or endeavor to intercept geolocation information pertaining to another person without the other person's consent.

(b) It is not unlawful under this section for an officer, employee, or agent of a covered services provider whose facilities are used to transmit geolocation information to intercept, disclose, or use that information in the normal course of the officer's, employee's, or agent's employment while engaged in any activity that is a necessary incident to render the service or protect the covered service provider's rights or property. A covered services provider that provides geolocation information service to the public must not use service observing or random monitoring, except for mechanical or service quality control checks.

Subd. 5. **Geolocation tracking; exceptions.** (a) Notwithstanding any law to the contrary, it is not unlawful under this section for an officer, employee, or agent of the United States in the normal course of official duties to conduct electronic surveillance, as authorized by the Foreign Intelligence Surveillance Act of 1978, United State Code, title 50, section 1801, et seq.

(b) It is not unlawful under this section for the parent, legal guardian, or another person who the parent or legal guardian has authorized, including a school, school district, or other caretaker, to track or collect a minor child's geolocation information.

(c) It is not unlawful under this section for any person to intercept or access geolocation information relating to another person through any system that is configured in a manner that makes the geolocation information readily accessible to the general public.

(d) It is not unlawful under this section for any investigative officer, law enforcement officer, or other emergency responder to intercept or access geolocation information relating to a person if the geolocation information is used to respond or provide assistance to a person if (1) the person requests assistance, or (2) the investigative officer, law enforcement officer, or emergency responder has reason to believe the person's life or safety is threatened.

(e) It is not unlawful under this section for a person to (1) intercept geolocation information pertaining to the location of another person who has unlawfully taken the device, and (2) send the geolocation information to the device owner, device operator, or law

enforcement officer if the device the owner or operator authorizes the geolocation information to be intercepted and sent.

(f) It is not unlawful under this section for a government entity or law enforcement officer to intercept or access geolocation information pursuant to a lawfully issued warrant or when there is an immediate danger of death or serious physical injury to a person.

Subd. 6. **Remedies.** (a) In addition to any remedies available under law and the remedies available under section 8.31, an individual whose geolocation information, text messages, data, camera, or microphone was accessed, recorded, or shared has a cause of action against the person who violated subdivision 2 or 4, including against (1) an individual who installed or used an application or device to collect or access the geolocation information of another person, and (2) the person who provided the software or application and failed to meet the standards required in subdivision 2, paragraph (a).

(b) The court may award the following damages to a prevailing plaintiff from a person found liable under this section:

(1) general and special damages, including any financial losses and damages for mental anguish suffered by an individual due to being tracked or having the individual's geolocation information, text messages, data, camera, or microphone accessed by another person; and

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

EFFECTIVE DATE. This section is effective August 1, 2022.