

This Document can be made available in alternative formats upon request

State of Minnesota

HOUSE OF REPRESENTATIVES

NINETY-FOURTH SESSION

H. F. No. 2313

03/13/2025 Authored by Robbins, Scott, Franson, Gillman and Rarick
The bill was read for the first time and referred to the Committee on Commerce Finance and Policy

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

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

1.7 Section 1. 325F.6985 SMARTPHONE MONITORING; GEOLOCATION
1.8 TRACKING CONSENT REQUIRED.

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 information (1) generated by or derived in whole
1.12 or in part from operating and using an electronic communications device, and (2) 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 a mapping, locational, or directional information service. Geolocation information does not
1.16 include information that is in the content of a communication; the Internet Protocol address
1.17 of an individual's home, business, or billing address; or component parts of the addresses
1.18 alone.

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

1.20 Subd. 2. Smartphone monitoring; prohibitions. (a) Smartphone 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 the application is displayed as an icon that can be found by a reasonable person. Software
2.6 or an application that tracks or records geolocation information, allows saved or stored texts
2.7 to be read by another remote user, or allows remote access to the phone user's microphone
2.8 or camera must require at least two forms of identity verification before being installed or
2.9 used on a device, and must accurately record the identity of the software or application user.
2.10 Two-factor authentication required under this paragraph must occur at the time the software
2.11 or application is installed, seven days after the date the software or application is installed,
2.12 and every 30 days after the date the software or application is installed. When the two-factor
2.13 authentication is not completed, the software must be disabled.

2.14 (c) Except as provided in subdivision 3, an individual is prohibited from installing an
2.15 application or software on the smartphone of another individual that allows the individual
2.16 to collect, record, share, or distribute the other individual's geolocation information,
2.17 microphone or camera data, or texts.

2.18 (d) Nothing in this section prevents an individual from installing software or an
2.19 application on a smartphone that allows the individual to share the individual's own
2.20 geolocation information or that allows a user to authorize a software application to access
2.21 the microphone or camera on the individual's own smartphone. Nothing in this section
2.22 prevents an application or software from being locked so an employee or child is unable to
2.23 remove or alter the software to secure the smartphone's location.

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

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

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

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

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

3.4 Subd. 4. **Geolocation tracking; consent required.** It is not unlawful under this section
3.5 for an officer, employee, or agent of a covered services provider whose facilities are used
3.6 to transmit geolocation information to intercept, disclose, or use the information in the
3.7 normal course of the officer's, employee's, or agent's employment while engaged in any
3.8 activity that is necessary to render the service or protect the covered service provider's rights
3.9 or property. A covered services provider that provides geolocation information service to
3.10 the public must not use service observing or random monitoring, except for mechanical or
3.11 service quality control checks.

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

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

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

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

3.28 (e) It is not unlawful under this section for a person to (1) intercept geolocation
3.29 information pertaining to the location of another person who has unlawfully taken the device,
3.30 and (2) send the geolocation information to the device owner, device operator, or law
3.31 enforcement officer if the device the owner or operator authorizes the geolocation information
3.32 to be intercepted and sent.

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

4.4 (g) Except as otherwise provided in this section, it is unlawful for a person to use a
4.5 device that tracks the geolocation information of another person to (1) intentionally intercept,
4.6 (2) endeavor to intercept, or (3) procure any other person to intercept or endeavor to intercept
4.7 geolocation information pertaining to another person without the other person's consent.

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

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

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

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