State of Minnesota

HOUSE OF REPRESENTATIVES

NINETY-FIRST SESSION

H. F. No. 2232

03/07/2019 Authored by Lucero, Noor and Robbins
The bill was read for the first time and referred to the Judiciary Finance and Civil Law Division
02/24/2020 Adoption of Report: Amended and re-referred to the Higher Education Finance and Policy Division

A bill for an act

relating to government data practices; requiring public postsecondary institutions to keep certain student information private; requiring consent before collecting student location data; amending Minnesota Statutes 2018, section 13.32, subdivision 5; proposing coding for new law in Minnesota Statutes, chapter 135A.

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

Section 1. Minnesota Statutes 2018, section 13.32, subdivision 5, is amended to read:

Subd. 5. **Directory information.** (a) Information designated as directory information pursuant to the provisions of United States Code, title 20, section 1232g, and Code of Federal Regulations, title 34, section 99.37, which are in effect on January 3, 2012, is public data on individuals, to the extent required under federal law.

(b) When conducting the directory information designation and notice process required by federal law, an educational agency or institution shall give parents and students notice of the right to refuse to let the agency or institution designate any or all data about the student as directory information. This notice may be given by any means reasonably likely to inform the parents and students of the right.

(c) A public postsecondary institution must maintain documentation of a request for directory information on 100 students or more for four years from the date of the request. A public postsecondary institution's directory information policy must not permit an individual's e-mail address, physical address, telephone number, or identification card photograph to be publicly disclosed. A student whose directory information has been requested must be allowed to review the documentation maintained by the institution regarding that request.

Sec. 2. **[135A.146] STUDENT LOCATION DATA.**

Subdivision 1. **Definition.** "Technology provider" means a person who:

(1) contracts with a public or private postsecondary educational institution to provide technological devices for student use or to provide access to a software or online application; and

(2) creates, receives, or maintains location data pursuant or incidental to a contract with a public or private postsecondary educational institution.

Subd. 2. **Consent.** (a) A public or private postsecondary educational institution must not collect data on a student's location without the student consenting to having location data collected. A public or private postsecondary educational institution must not require a student's consent to location data collection as a condition of:

(1) enrolling in the institution or any program or class;

(2) receiving a scholarship or other financial aid award; or

(3) entering into a dining contract, housing contract, or any other agreement for the provision of a basic university service, including connecting to campus Wi-Fi.

(b) A student who gives consent to having location data collected may revoke that consent at any time.

Subd. 3. **Notice.** (a) Within 30 days of the start of each school year, a public or private postsecondary educational institution must give students notice, by United States mail, e-mail, or other direct form of communication, of any technology provider contract gathering a student's location data. The notice must:

(1) be written in plain language;

(2) identify each technology provider collecting location data;

(3) identify the location data gathered by the technology provider contract;

(4) include information about the consent required in subdivision 2, including the right to revoke consent; and

(5) include information about how to access a copy of the contract in accordance with paragraph (b).

(b) A public or private postsecondary educational institution must publish a complete copy of any contract with a technology provider on the institution's website for the duration of the contract.

Subd. 4. **Location data.** (a) A technology provider contracting with a public postsecondary institution is subject to the provisions of section 13.05, subdivision 11. An assignee or delegate that creates, receives, or maintains location data is subject to the same restrictions and obligations under this section as the technology provider.

(b) Location data created, received, or maintained by a technology provider pursuant or incidental to a contract with a public or private postsecondary educational institution are not the technology provider's property.

(c) If location data maintained by the technology provider are subject to a breach of the security of the data, as defined in section 13.055, the technology provider must, following discovery of the breach, disclose to the public postsecondary educational institution all information necessary to fulfill the requirements of section 13.055.

(d) Within 30 days of the expiration of the contract, unless renewal of the contract is reasonably anticipated, a technology provider must destroy or return to the appropriate public or private postsecondary educational institution all location data created, received, or maintained pursuant or incidental to the contract.

(e) A technology provider must not:

(1) sell, share, or disseminate location data, except as provided by this section or as part of a valid delegation or assignment of its contract with a public or private postsecondary educational institution; or

(2) use location data for any commercial purpose, including but not limited to marketing or advertising to a student or parent.

Subd. 5. **Procedures.** (a) A technology provider must establish written procedures to ensure appropriate security safeguards are in place for location data. A technology provider's written procedures must require that:

(1) only authorized employees or contractors can access the location data;

(2) a person is authorized to access location data only if access is necessary to fulfill official duties; and

(3) all actions in which location data are entered, updated, accessed, shared, or disseminated are recorded in a log of use that includes the identity of the person interacting with the data and what action was performed. Information recorded in the log of use must be retained for at least one year.

(b) A technology provider's written procedures establishing security safeguards for location data are public data, unless classified as not public under any other applicable law.

EFFECTIVE DATE. This section is effective July 1, 2020.