SB2359

LRB10330648DTM57106b

103RD GENERAL ASSEMBLY

State of Illinois

2023 and 2024

SB2359

Introduced 2/10/2023, by Sen. Rachel Ventura

SYNOPSIS AS INTRODUCED:

New Act

Creates the Protecting Privacy from Government Intrusion Act. Provides that a government entity may not obtain the location information of an electronic device without a tracking warrant. Provides that a warrant granting access to location information must be issued only if the government entity shows that there is probable cause that the person who possesses an electronic device is committing, has committed, or is about to commit a crime. Provides for requirements of an application for a warrant. Describes when a government entity may obtain location information without a tracking warrant. Provides for a time period to achieve the objective of the authorization; notice on the persons named in the warrant; a report on collection of location information; a prohibition on the use of evidence; a limit on storage of license plate data; a prohibition on transfer of license plate data; and student online personal information protection. Defines terms.

LRB103 30648 DTM 57106 b

A BILL FOR

AN ACT concerning criminal law.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Protecting Privacy from Government Intrusion Act.

Section 5. Definitions. In this Act:

"Automated license plate recognition system" means one or more mobile or fixed cameras combined with computer algorithms to convert images of license plates into computer-readable data.

"Captured plate data" means the global positioning device coordinates, date and time, photograph, license plate number, and any other data captured by or derived from any automated license plate recognition system.

"Electronic communication service" means any service that provides to its subscribers or users the ability to send or receive electronic communications, including any service that acts as an intermediary in the transmission of electronic communications, or stores electronic communication information.

"Government entity" means a State or local agency, including, but not limited to, a law enforcement entity or any other investigative entity, agency, department, division,

bureau, board, commission, or an individual acting or purporting to act for or on behalf of a State or local agency or any unit of local government or political subdivision of this State.

"Location information" means information concerning the location of an electronic device that, in whole or in part, is generated or derived from or obtained by the operation of an electronic device.

"Location information service" means the provision of a global positioning service or other mapping, locational, or directional information service.

"Operator" means the operator of an Internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes.

"Remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

"Tracking warrant" means an order in writing, in the name of the State, signed by a court other than a court exercising probate jurisdiction, directed to a peace officer, granting the officer access to location information of an electronic device.

Section 10. Tracking warrant required for location

information.

(a) Except as provided in paragraph (2), a government entity may not obtain the location information of an electronic device without a tracking warrant. A warrant granting access to location information must be issued only if the government entity shows that there is probable cause the person who possesses an electronic device is committing, has committed, or is about to commit a crime. An application for a warrant must be made in writing and include:

(1) the identity of the government entity's peace officer making the application and the officer authorizing the application; and

(2) a full and complete statement of the facts and circumstances relied on by the applicant to justify the applicant's belief that a warrant should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, and (ii) the identity of the person, if known, committing the offense whose location information is to be obtained.

(b) A government entity may obtain location information without a tracking warrant:

(1) when the electronic device is reported lost or stolen by the owner;

(2) in order to respond to the user's call for emergency services;

(3) with the informed, affirmative, documented consent

of the owner or user of the electronic device;

(4) with the informed, affirmative consent of the legal guardian or next of kin of the owner or user if the owner or user is believed to be deceased or reported missing and unable to be contacted; or

(5) in an emergency situation that involves the risk of death or serious physical harm to a person who possesses an electronic communications device.

Section 15. Time period. A tracking warrant issued under this Act must authorize the collection of location information for a period not to exceed 60 days or the period of time necessary to achieve the objective of the authorization, whichever is less.

Extensions of a tracking warrant may be granted, but only upon an application for an order and upon the judicial finding required by paragraph (2) of subsection (a) of Section 10. The period of extension must be for a period not to exceed 60 days or the period of time necessary to achieve the objective for which it is granted, whichever is less.

This Section applies only to tracking warrants issued for the contemporaneous collection of electronic device location information.

Section 20. Notice.

(a) Within a reasonable time, but not later than 90 days

after the court unseals the tracking warrant under this Section, the issuing or denying judge shall cause to be served on the persons named in the warrant and the application an inventory which shall include notice of:

(1) the fact of the issuance of the warrant or the application;

(2) the date of the issuance and the period of authorized, approved, or disapproved collection of location information or the denial of the application; and

(3) the fact that during the period location information was or was not collected.

(b) A tracking warrant authorizing collection of location information must direct:

(1) the warrant to be sealed for a period of 90 days or until the objective of the warrant has been accomplished, whichever is shorter; and

(2) the warrant to be filed with the court administrator within 10 days of the expiration of the warrant.

(c) The State's Attorney may request that the tracking warrant, supporting affidavits, and any order granting the request not be filed. An order must be issued granting the request in whole or in part if, from affidavits, sworn testimony, or other evidence, the court finds reasonable grounds exist to believe that filing the warrant may cause the search or a related search to be unsuccessful, create a

substantial risk of injury to an innocent person, or severely hamper an ongoing investigation.

(d) The tracking warrant must direct that following the commencement of any criminal proceeding utilizing evidence obtained in or as a result of the search, the supporting application or affidavit must be filed either immediately or at any other time as the court directs. Until such filing, the documents and materials ordered withheld from filing must be retained by the judge or the judge's designee.

Section 25. Report on collection of location information.

(a) At the same time as notice is provided under paragraph (4), the issuing or denying judge shall report to the State court administrator:

(1) the fact that a tracking warrant or extension was applied for;

(2) the fact that the warrant or extension was granted as applied for, was modified, or was denied;

(3) the period of collection authorized by the warrant and the number and duration of any extensions of the warrant;

(4) the offense specified in the warrant or application or an extension of a warrant;

(5) whether the collection required contemporaneous monitoring of an electronic device's location; and

(6) the identity of the applying investigative or

peace officer and agency making the application and the person authorizing the application.

(b) On or before November 15 of each even-numbered year, the State court administrator shall transmit to the General Assembly a report concerning:

(1) all tracking warrants authorizing the collection of location information during the 2 previous calendar years; and

(2) all applications that were denied during the 2 previous calendar years. Each report shall include a summary and analysis of the data required to be filed under this Section. The report is public and must be available for public inspection at the library of the Legislative Reference Bureau and the State court administrator's office and website.

Section 30. Prohibition on the use of evidence.

(a) Except as proof of a violation of this Section, no evidence obtained in violation of this Section shall be admissible in any criminal, civil, administrative, or other proceeding.

(b) Any location information obtained pursuant to this Act or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a federal or State court unless each party, not less than 10 days before the trial, hearing, or

proceeding, has been furnished with a copy of the tracking warrant and accompanying application under which the information was obtained. This 10-day period may be waived by the judge if the judge finds that it was not possible to furnish a party with the required information 10 days before the trial, hearing, or proceeding and that a party will not be prejudiced by the delay in receiving the information.

Section 35. Limit on storage of license plate data. Any captured plate data collected or retained by any governmental or private entity or individual through the use of an automated license plate recognition system may not be stored for more than 180 days unless, in the case of a governmental entity, the data is retained or stored as part of an ongoing governmental investigation, and in that case, the data shall be destroyed at the conclusion of either:

(1) an investigation that does not result in any criminal charges being filed; or

(2) any criminal action undertaken in the matter involving the captured plate data.

Section 40. Prohibition on transfer of license plate data. No governmental entity shall transfer captured plate data except for the purpose of conducting criminal investigations and ensuring compliance with the law.

No governmental entity, private entity, or individual

shall sell captured plate data for any purpose.

Section 45. Student online personal information protection.

(a) An operator shall not knowingly engage in any of the following activities with respect to the operator's site, service, or application:

(1) engage in targeted advertising on the operator's site, service, or application or target advertising on any other site, service, or application when the targeting of the advertising is based upon any information, including covered information and persistent unique identifiers that the operator has acquired because of the use of that operator's site, service, or application;

(2) use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application to amass a profile about a K-12 student except in furtherance of a K-12 school purpose;

(3) sell a student's information, including covered information. This prohibition does not apply to the purchase, merger, or other type of acquisition of an operator by another entity, provided that the operator or successor entity continues to be subject to the provisions of this Section with respect to previously acquired student information; and

(4) disclose covered information unless the disclosure

is made:

(A) in furtherance of the K-12 school purpose of the site, service, or application, provided the recipient of the covered information disclosed pursuant to this subsection:

(i) shall not further disclose the information unless done to allow or improve operability and functionality within that student's classroom or school; and

(ii) is legally required to comply with subsection (c);

(B) to ensure legal and regulatory compliance;

(C) to respond to or participate in judicial process;

(D) to protect the safety of users or others or security of the site; or

(E) to a service provider, provided the operator contractually: (i) prohibits the service provider from using any covered information for any purpose other than providing the contracted service to, or on behalf of, the operator; (ii) prohibits the service provider from disclosing any covered information provided by the operator with subsequent third parties; and (iii) requires the service provider to implement and maintain reasonable security procedures and practices as provided in subsection (c).

(b) Nothing in subsection (a) shall be construed to prohibit the operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application.

(c) An operator shall:

(1) implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information and protect that information from unauthorized access, destruction, use, modification, or disclosure; and

(2) delete a student's covered information if the school or district requests deletion of data under the control of the school or district.

(d) Notwithstanding paragraph (4) of subsection (a), an operator may disclose covered information of a student, as long as paragraphs (1) through (3) of subsection (a) are not violated, under the following circumstances:

(1) if other provisions of federal or State law require the operator to disclose the information, and the operator complies with the requirements of federal and state law in protecting and disclosing that information;

(2) for legitimate research purposes: (i) as required by State or federal law and subject to the restrictions under applicable State and federal law; or (ii) as allowed by State or federal law and under the direction of a school, school district, or state department of education,

if no covered information is used for any purpose in furtherance of advertising or to amass a profile on the student for purposes other than K-12 school purposes; and

(3) to a State or local educational agency, including schools and school districts for K-12 school purposes, as permitted by State or federal law.

(e) Nothing in this Section prohibits an operator from using deidentified student covered information as follows:

(1) within the operator's site, service, or application or other sites, services, or applications owned by the operator to improve educational products; and

(2) to demonstrate the effectiveness of the operator's products or services, including in the operator's marketing.

(f) Nothing in this Section prohibits an operator from sharing aggregated deidentified student covered information for the development and improvement of educational sites, services, or applications.

(g) As used in this Section:

"Covered information" means personally identifiable information or materials, in any media or format that meets any of the following:

(1) is created or provided by a student, or the student's parent or legal guardian, to an operator in the course of the student's, parent's, or legal guardian's use of the operator's site, service, or application for K-12

school purposes;

(2) is created or provided by an employee or agent of the K-12 school, school district, local education agency, or county office of education, to an operator; or

(3) is gathered by an operator through the operation of a site, service, or application and is descriptive of a student or otherwise identifies a student, including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

"K-12 school purposes" means purposes that customarily take place at the direction of the K-12 school, teacher, or school district or aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, collaboration between students, school personnel, or parents, or are for the use and benefit of the school.

"Online service" means cloud computing services, which must comply with this Section if the cloud computing services otherwise meet the definition of an operator.

(h) This Section shall not be construed to limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

(i) This Section does not limit the ability of an operator to use student data, including covered information, for adaptive learning or customized student learning purposes.

(j) This Section does not apply to general audience Internet websites, general audience online services, general audience online applications, or general audience mobile applications, even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications.

(k) This Section does not limit Internet service providers from providing Internet connectivity to schools or students and the students' families.

(l) This Section shall not be construed to prohibit an operator of an Internet website, online service, online application, or mobile application from marketing educational products directly to parents so long as the marketing did not result from the use of covered information obtained by the operator through the provision of services covered under this Section.

(m) This Section does not impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance of this Section on those applications or software.

(n) This Section does not impose a duty upon a provider of an interactive computer service, as defined in 47 U.S.C. 230, to review or enforce compliance with this Section by third-party content providers.

(o) This Section does not impede the ability of students to download, export, or otherwise save or maintain the student's own student created data or documents.

Section 97. Severability. The provisions of this Act are severable under Section 1.31 of the Statute on Statutes.