SENATE BILL No. 341

May 22, 2019, Introduced by Senator LUCIDO and referred to the Committee on Judiciary and Public Safety.

A bill to require a law enforcement agency to obtain a search warrant to access certain electronic information or data; to prescribe the manner in which certain electronic information or data may be accessed or used; to require notification to the owner or user of the electronic information, data, or electronic device that the electronic information, data, or electronic device has been accessed; and to provide remedies.

THE PEOPLE OF THE STATE OF MICHIGAN ENACT:

Sec. 1. This act shall be known and may be cited as the "electronic information and data privacy act".

Sec. 2. As used in this act:

(a) "Cell-site simulator device" means a device that transmits or receives radio waves to or from a communications device and that can be used to intercept, collect, access, transfer, or forward the

SENATE BILL No. 341

data transmitted or received by the communications device, or stored on the communications device. Cell-site simulator device includes an international mobile subscriber identity catcher or other cellular telephone or telephone surveillance or eavesdropping device that mimics a cellular base station and transmits radio waves that cause cellular telephones or other communications devices in the area to transmit or receive radio waves, electronic data, location data, information used to calculate location, identifying information, communications content, or metadata, or otherwise obtains that information through passive means, such as through the use of a digital analyzer or other passive interception device. However, cell-site simulator device does not include any device used or installed by an electric utility solely to the extent that the device is used by that utility to measure electrical usage, to provide services to customers, or to operate the electric grid.

(b) "Electronic communication service" means a service that provides to users of the service the ability to send or receive wire or electronic communications.

(c) "Electronic device" means a device that enables access to or use of an electronic communication service, remote computing service, or location information service.

(d) "Electronic information or data" includes information or data including a sign, signal, writing, image, sound, or intelligence of any nature transmitted or stored in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system, and the location information, stored data, or

transmitted data of an electronic device.

(e) Electronic information or data does not include:

(*i*) A wire or oral communication.

(*ii*) A communication made through a tone-only paging device.

(*iii*) Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of money.

(f) "Law enforcement agency" means an entity of this state or a political subdivision of this state that exists to primarily prevent, detect, or prosecute crime and enforce criminal statutes or ordinances.

(g) "Location information" means information, obtained by means of a tracking device, 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.

(h) "Location information service" means the provision of a global positioning service or other mapping, location, or directional information service.

(i) "Oral communication" means any oral communication uttered by a person exhibiting an expectation that the communication is not subject to interception, under circumstances justifying that expectation, but does not include any electronic communication.

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

(k) "Subscriber record" means a record or information of a provider of an electronic communication service or remote computing

service that reveals any of the following information regarding the subscriber or customer:

(*i*) Name.

(*ii*) Address.

(*iii*) Local and long distance telephone connection record, or record of session time and duration.

(*iv*) Length of service, including the start date.

(*v*) Type of service used.

(*vi*) Telephone number, instrument number, or other subscriber or customer number or identification, including a temporarily assigned network address.

(*vii*) Means and source of payment for the service, including a credit card or bank account number.

(*l*) "Transmitted data" means electronic information or data that is transmitted wirelessly as follows:

(*i*) From an electronic device to another electronic device without the use of an intermediate connection or relay.

(*ii*) From an electronic device to a nearby antenna.

(m) "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception, including the use of the connection in a switching station, furnished or operated by any person engaged as a common carrier in providing or operating these facilities for the transmission of intrastate, interstate, or foreign communications.

Sec. 3. (1) Except as otherwise provided in this section,

during a criminal investigation or prosecution, a law enforcement agency may not obtain, including through the use of a cell-site simulator device or other methods, either of the following, without a search warrant issued by a court upon probable cause:

(a) The location information, stored data, or transmitted data of an electronic device.

(b) Electronic information or data transmitted by the owner of the electronic information or data to a remote computing service provider.

(2) Except as provided in subsection (3), a law enforcement agency may not use, copy, or disclose, for any purpose, the location information, stored data, transmitted data of an electronic device, or electronic information or data provided by a remote computing service provider that is not the subject of the warrant and is collected as part of an effort to obtain the location information, stored data, transmitted data of an electronic device, or electronic information or data provided by a remote computing service provider that is the subject of the warrant in subsection (1).

(3) A law enforcement agency may use, copy, or disclose the transmitted data of an electronic device used to communicate with the electronic device that is the subject of the warrant if the law enforcement agency reasonably believes that the transmitted data is necessary to achieve the objective of the warrant.

(4) The electronic information or data described in subsection (2) must be destroyed in an unrecoverable manner by the law enforcement agency as soon as reasonably possible after the

electronic information or data is collected.

(5) A law enforcement agency may obtain location information without a warrant for an electronic device under 1 or more of the following circumstances:

(a) The device is reported stolen by the owner.

(b) The owner or user of the device provides informed and affirmative consent.

(c) In accordance with a judicially recognized exception to the warrant requirement.

(d) The owner has voluntarily and publicly disclosed the location information.

(e) From the remote computing service provider if the remote computing service provider voluntarily discloses the location information under 1 of the following circumstances:

(*i*) Under a belief that an emergency exists involving an imminent risk to an individual of death, serious physical injury, sexual abuse, live-streamed sexual exploitation, kidnapping, or human trafficking.

(*ii*) The location information is inadvertently discovered by the remote computing service provider and appears to pertain to the commission of a felony, or of a misdemeanor involving physical violence, sexual abuse, or dishonesty.

(6) A law enforcement agency may obtain stored or transmitted data from an electronic device, or electronic information or data transmitted by the owner of the electronic information or data to a remote computing service provider, without a warrant under 1 or more of the following circumstances:

(a) With the informed consent of the owner of the electronic device or electronic information or data.

(b) In accordance with a judicially recognized exception to the warrant requirement.

(c) In connection with a report forwarded by the National Center for Missing and Exploited Children under 18 USC 2258A.

(d) From a remote computing service provider if the remote computing service provider voluntarily discloses the stored or transmitted data as otherwise permitted under 18 USC 2702.

(7) An electronic communication service provider or remote computing service provider or the provider's officers, employees, agents, or other specified persons may not be held liable for providing information, facilities, or assistance in good-faith reliance on the terms of a warrant issued under this section or without a warrant under subsection (5) or (6).

Sec. 4. (1) Except as provided in subsection (3), a law enforcement agency that executes a warrant under section 3 shall, within 14 days after the day on which the electronic information or data that is the subject of the warrant is obtained by the law enforcement agency, issue a notification to the owner of the electronic device or electronic information or data specified in the warrant. The notice must provide all of the following information:

(a) That a warrant was applied for and granted.

(b) The kind of warrant issued.

(c) The period of time during which the collection of the electronic information or data was authorized.

(d) The offense specified in the application for the warrant.

(e) The identity of the law enforcement agency that filed the application.

(f) The identity of the judge who issued the warrant.

(2) The notification requirement under subsection (1) is not triggered until the owner of the electronic device or electronic information or data specified in the warrant is known, or could be reasonably identified, by the law enforcement agency.

(3) A law enforcement agency seeking a warrant under section 3 may submit a request, and the court may grant permission, to delay the notification required by subsection (1) for a period not to exceed 30 days, if the court determines that there is reasonable cause to believe that the notification may result in 1 or more of the following circumstances:

(a) Endangering the life or physical safety of an individual.

(b) Causing a person to flee from prosecution.

(c) Leading to the destruction of or tampering with evidence.

(d) Intimidating a potential witness.

(e) Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(4) If a delay of notification is granted under subsection (3) and upon application by the law enforcement agency, the court may grant additional extensions of up to 30 days each.

(5) Notwithstanding subsection (4), when a delay of notification is granted under subsection (3), and upon application by a law enforcement agency, the court may grant an additional extension of up to 60 days if the court determines that a delayed

notification is justified because 1 or both of the following apply to the investigation involving the warrant:

(a) The investigation is interstate in nature and sufficiently complex.

(b) The investigation is likely to extend up to or beyond an additional 60 days.

(6) Upon expiration of the period of delayed notification granted under subsection (3), (4), or (5), the law enforcement agency shall serve upon or deliver by first-class mail, or by other means if delivery is impracticable, to the owner of the electronic device or electronic information or data a copy of the warrant together with a notice that contains all of the following:

(a) Information provided with reasonable specificity regarding the nature of the law enforcement inquiry.

(b) The information described in subsection (1)(a) through (f).

(c) A statement that notification of the search was delayed.

(d) The name of the court that authorized the delay of notification.

(e) A reference to the provision of this section that allowed the delay of notification.

(7) A law enforcement agency is not required to notify the owner of the electronic device or electronic information or data under this section if the owner is located outside of the United States.

Sec. 5. (1) Except as otherwise provided in this section or as permitted by law, a law enforcement agency shall not obtain,

including through the use of a cell-site simulator device or other methods, use, copy, or disclose a subscriber record.

(2) Except as provided in subsection (3), a law enforcement agency shall not obtain, including through the use of a cell-site simulator device or other methods, use, copy, or disclose, for a criminal investigation or prosecution, any record or information, other than a subscriber record, of a provider of an electronic communication service or remote computing service related to a subscriber or customer without a warrant.

(3) Notwithstanding subsections (1) and (2), a law enforcement agency may obtain, use, copy, or disclose a subscriber record, or other record or information related to a subscriber or customer, without a warrant under the following circumstances:

(a) With the informed and affirmative consent of the subscriber or customer.

(b) In accordance with a judicially recognized exception to the warrant requirement.

(c) If the subscriber or customer voluntarily disclosed the record in a manner that is publicly accessible.

(d) If the provider of an electronic communication service or remote computing service voluntarily discloses the record under 1 or more of the following circumstances:

(*i*) Under a belief that an emergency exists involving the imminent risk to an individual of 1 or more of the following:

(A) Death.

(B) Serious physical injury.

(C) Sexual abuse.

(D) Live-streamed sexual exploitation.

(E) Kidnapping.

(F) Human trafficking.

(*ii*) The record is inadvertently discovered by the provider, if the record appears to pertain to the commission of 1 or more of the following:

(A) A felony.

(B) A misdemeanor involving physical violence, sexual abuse, or dishonesty.

(*iii*) As otherwise permitted under 18 USC 2702.

(4) A provider of an electronic communication service or remote computing service, or the provider's officers, employees, agents, or other specified persons may not be held liable for providing information, facilities, or assistance in good-faith reliance on the terms of a warrant issued under this section or without a warrant in accordance with subsection (3).

Sec. 6. All electronic information or data and records of a provider of an electronic communications service or remote computing service pertaining to a subscriber or customer that are obtained in violation of the provisions of this act are subject to the rules governing exclusion as if the records were obtained in violation of Amendment IV to the Constitution of the United States and section 11 of article I of the state constitution of 1963.