Senate Fiscal Agency
P.O. Box 30036
Lansing, Michigan 48909-7536

BILL ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986

Senate Bills 341 (as introduced 5-22-19)
Sponsor: Senator Peter J. Lucido
Committee: Judiciary and Public Safety

Date Completed: 5-22-19

CONTENT

The bill would enact the "Electronic Information and Data Privacy Act" to do the following:

- **Prohibit a law enforcement officer from obtaining without a search warrant the location information, stored data, or transmitted data of an electronic device, or electronic information or data transmitted by the owner of the information or data to a remote computing service provider, except as otherwise provided.**
- **Prohibit a law enforcement agency from using, copying, or disclosing the information or data that was not the subject of a warrant and was collected as part of an effort to obtain information or data that was the subject of the warrant.**
- **Allow a law enforcement agency to use, copy, or disclose the information that was subject to a warrant if the agency reasonably believed that the data were necessary to achieve the warrant's objectives.**
- **Require a law enforcement agency to destroy in an unrecoverable matter the electronic information or data described above as soon as reasonably possible after the electronic information or data was collected.**
- **Allow a law enforcement agency to obtain location information without a warrant under certain circumstances.**
- **Allow a law enforcement agency to obtain stored or transmitted data without a warrant under certain circumstances.**
- **Require a law enforcement agency that executed a search warrant to issue, within 14 days after the information or data was obtained, a notification to the owner of the electronic device, information, or data specified in the warrant.**
- **Allow a law enforcement agency to seek, and a court to grant permission, to delay a notification under certain circumstances.**
- **Prohibit a law enforcement agency from obtaining, using, copying, or disclosing a subscriber record, except as otherwise provided.**
- **Prohibit a law enforcement agency from obtaining, using, copying, or disclosing any record or information, other than a subscriber record, without a warrant.**
- **Allow a law enforcement officer to obtain, use, copy, or disclose a subscriber record, or other record or information related to a subscriber or customer, without a warrant under certain circumstances.**

Definitions

"Electronic device" would mean a device that enables access to or use of an electronic communication service, remote computing service, or location information service. "Location

information service" would mean the provision of a global positioning service or other mapping, location, or directional information service.

"Electronic information or data" would include 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. The term would not include:

-- A wire or oral communication.
-- A communication made through a tone-only paging device.
-- Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of money.

"Wire communication" would mean 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.

"Oral communication" would mean 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.

"Location information" would mean 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.

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

"Transmitted data" would mean electronic information or data that is transmitted wirelessly as follows:

-- From an electronic device to another electronic device without the use of an intermediate connection or relay.
-- From an electronic device to a nearby antenna.

Electronic Information & Data

Under the proposed Act, except as otherwise provided, during a criminal investigation or prosecution, a law enforcement agency could 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:

-- The location information, stored data, or transmitted data of an electronic device.
-- Electronic information or data transmitted by the owner of the electronic information or data to a remote computing service provider.

"Law enforcement agency" would mean an entity or a political subdivision of the State that exists to primarily prevent, detect, or prosecute crime and enforce criminal statutes or ordinances.

"Cell-site simulator device" would 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 data transmitted or received by the communications device, or stored on the communications device. The term would include 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. The term would 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.

Except as otherwise provided, a law enforcement agency could 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 was not the subject of the warrant and was collected as part of an effort to obtain the electronic information or data specified above provided by a remote computing service provider that was the subject of the warrant.

A law enforcement agency could use, copy, or disclose the transmitted data of an electronic device used to communicate with the electronic device that was the subject of a warrant if the agency reasonably believed that the transmitted data were necessary to achieve the warrant's objective.

The law enforcement agency would have to destroy in an unrecoverable matter the electronic information or data described above as soon as reasonably possible after it was collected.

A law enforcement agency could obtain location information without a warrant for an electronic device under one or more of the following circumstances:

-- The device was reported stolen by the owner.
-- The owner or user of the device provided informed and affirmative consent.
-- In accordance with a judicially recognized exception to the warrant requirement.
-- The owner had voluntarily and publicly disclosed the location information.

A law enforcement agency also could obtain location information without a warrant from the remote computing service provider if the provider voluntarily disclosed the location information under one of the following circumstances:

-- Under a belief that an emergency existed involving an imminent risk to an individual of death, serious physical injury, sexual abuse, live-streamed sexual exploitation, kidnapping, or human trafficking.
-- The remote computing service provider inadvertently discovered the location information, and the information appeared to pertain to the commission of a felony, or of a misdemeanor involving physical violence, sexual abuse, or dishonesty.

A law enforcement agency could 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 one or more of the following circumstances:

-- With the informed consent of the owner of the electronic device or electronic information or data.
-- In accordance with a judicially recognized exception to the warrant requirement.
-- In connection with a report forwarded by the National Center for Missing and Exploited Children.
-- From a remote computing service provider if the provider voluntarily disclosed the stored or transmitted data as otherwise permitted under 18 USC 2702.

(18 USC 2702 generally prohibits a person or entity providing an electronic communication service or remote computing service to the public from knowingly divulging the contents of certain communications. A provider may divulge the contents of a communication under certain specified circumstances.)

An electronic communication service provider or remote computing service provider or the provider's officers, employees, agents, or other specified individual could not be held liable for providing information, facilities, or assistance in good-faith reliance on the terms of a warrant, or without a warrant (as described above). "Electronic communication service" would mean a service that provides to users of the service the ability to send or receive wire or electronic communications.

Notice

Except as otherwise provided, a law enforcement agency that executed a search warrant, within 14 days after the day on which the electronic information or data that was the subject of the warrant was obtained by the law enforcement agency, would have to issue a notification to the owner of the electronic device or electronic information or data specified in the warrant. The notice would have to provide all of the following information:

-- That a warrant was applied for and granted.
-- The kind of warrant issued.
-- The period of time during which the collection of the electronic information or data was authorized.
-- The offense specified in the application for the warrant.
-- The identity of the law enforcement agency that filed the application.
-- The identity of the judge who issued the warrant.

The notification requirement would not be triggered until the owner of the electronic device or electronic information or data specified in the warrant was known, or could be reasonably identified, by the law enforcement agency.

A law enforcement agency seeking a warrant could submit a request, and a court could grant permission, to delay the notification for a period of up to 30 days, if the court determined that there was reasonable cause to believe that the notification could result in one or more of the following:

-- Endangering the life or physical safety of an individual.
-- Causing a person to flee from prosecution.
-- Leading to the destruction of or tampering with evidence.
-- Intimidating a potential witness.
-- Otherwise seriously jeopardizing an investigation or unduly delaying trial.

If a delay of notification were granted and upon application by the law enforcement agency, the court could grant additional extensions of up to 30 days each.

Notwithstanding the grant of additional extensions described above, when a delay of notification was granted, and upon application by a law enforcement agency, the court could grant an additional extension of up to 60 days if it determined that a delayed notification was justified because one or both of the following applied to the investigation involving the warrant:

-- The investigation was interstate in nature and sufficiently complex.
-- The investigation likely was to extend up to or beyond an additional 60 days.

When a period of delayed notification expired, the law enforcement agency would have to serve on or deliver by first-class mail, or by other means if delivery were impracticable, to the owner of the electronic device or electronic information or data a copy of the warrant together with a notice that contained all of the following:

-- Information provided with reasonable specificity regarding the nature of the law enforcement inquiry.
-- The information described above for a notification issued within 14 days after a warrant was executed.
-- A statement that notification of the search was delayed.
-- The name of the court that authorized the delay of notification.
-- A reference to the Act's provision that allowed the delay of notification.

A law enforcement agency would not have to notify the owner if the owner were located outside of the United States.

Subscriber Record

Except as otherwise provided in the Act or as permitted by law, a law enforcement agency could not obtain, including through the use of a cell-site simulator device or other methods, use, copy, or disclose a subscriber record.

"Subscriber record" would mean 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:

-- Name.
-- Address.
-- Local and long distance telephone connection record, or record of session time and duration.
-- Length of service, including the start date.
-- Type of service used.
-- Telephone number, instrument number, or other subscriber or customer number or identification, including a temporarily assigned network address.
-- Means and source of payment for the service, including a credit card or bank account number.

Except as otherwise provided, a law enforcement agency could not obtain, including the 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 provider related to a subscriber without a warrant.

Notwithstanding the above prohibitions, a law enforcement agency could 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:

-- With the subscriber's or customer's informed and affirmative consent.
-- In accordance with a judicially recognized exception to the warrant requirement.
-- If the subscriber or customer voluntarily disclosed the record in a manner that was publicly accessible.

A law enforcement agency also could obtain, use, copy, or disclose a subscriber record, or other record or information related to a subscriber or customer, without a warrant if the provider of an electronic communication or remote computing service provider voluntarily disclosed the record under one or more of the following circumstances:

-- A belief that an emergency existed involving the imminent risk to an individual of one or more of the following: a) death, b) serious physical injury, c) sexual abuse, d) live-streamed sexual exploitation, e) kidnapping, or f) human trafficking.
-- The record was inadvertently discovered by the provider, if the record appears to pertain to the commission of a felony, or a misdemeanor involving physical violence, sexual abuse, or dishonesty.
-- As otherwise permitted under 18 USC 2702.

A provider of electronic communication service or remote computing service, or the provider's officer's employees, agents, or other specified people could not be held liable for providing information, facilities, or assistance in good faith reliance on the terms of a warrant or without a warrant (as described above).

Exclusion of Evidence

All electronic information or data and records of a provider of an electronic communications services or remote computing service pertaining to a subscriber or customer that were obtained in violation of the Act would be subject to the rules governing exclusion as if the records were obtained in violation of the Fourth Amendment to the United States Constitution or Article I, Section 11 of the Michigan Constitution.

Legislative Analyst: Stephen Jackson

FISCAL IMPACT

The bill would have a minor fiscal impact on the Department of State Police and other law enforcement agencies. According to the Department, nearly all electronic device interception activity is currently performed under the authority of a warrant. However, all such acts have not been subject to the notification and reporting requirements proposed under the bill, which would add administrative costs to these agencies, at an amount that cannot be determined at this time.

Fiscal Analyst: Bruce Baker
Michael Siracuse

SAS\S1920\s341sa