Legislative Analysis

Phone: (517) 373-8080
http://www.house.mi.gov/hfa

ELECTRONIC INFORMATION AND DATA PRIVACY ACT

Analysis available at
http://www.legislature.mi.gov

Senate Bill 341 (S-1) as passed by the Senate
Sponsor: Sen. Peter J. Lucido
House Committee: Judiciary
Senate Committee: Judiciary and Public Safety
Complete to 9-8-20

SUMMARY:

Senate Bill 341 would create a new act, the Electronic Information and Data Privacy Act, to do all of the following:

- Require a search warrant to obtain, use, copy, store, or disclose certain information obtained from or regarding an electronic device and specify circumstances under which electronic information from an electronic device could be obtained without a warrant.
- Require electronic information or data collected under a search warrant that is not the subject of the search warrant to be destroyed.
- Require notification that a warrant has been issued to be provided by law enforcement to the owner of the electronic device and allow the notification to be delayed for an additional 30 or 60 days under certain circumstances.
- Provide an electronic communication service provider or remote computing service provider with immunity from liability for assistance provided in good-faith reliance on the terms of a warrant.
- Subject electronic information and data obtained in violation of the act to the rules that govern exclusion under state and federal constitutional protections against unlawful searches.

Senate Bill 341 would, except as otherwise provided, require a law enforcement agency, during a criminal investigation or prosecution, to obtain a search warrant upon probable cause to obtain the ***location information***, stored data, or transmitted data of an ***electronic device*** or to obtain ***electronic information or data*** transmitted by the owner of the electronic information or data to a remote computing service provider.

Location information would mean information, obtained by a 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.

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. Electronic information or data 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.

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

Electronic communication service would mean a service that provides to users of the service the ability to send or receive wire or electronic communications.

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

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

Electronic information or data collected under a search warrant related to an electronic device that was not the subject of the warrant could not be used, copied, disclosed, stored, or retained by a law enforcement agency for any purpose and would have to be destroyed in an unrecoverable manner as soon as possible after being collected. However, transmitted data from that device to the electronic device that was the subject of the warrant could be used, copied, disclosed, stored, or retained by the law enforcement agency if the agency reasonably believed the data necessary to achieve the objective of the warrant.

Collection of information or data without a warrant for an electronic device

Senate Bill 341 would allow a law enforcement agency to collect certain information and data from an electronic device without a warrant in specified circumstances.

Location information could be obtained without a warrant under one or more of the following circumstances:

- The device is reported stolen by the owner.
- The owner or user of the device provides informed consent.
- In accordance with a judicially recognized exception to the warrant requirement.
- The owner voluntarily and publicly disclosed the location information.
- From the remote computing service provider if that provider voluntarily discloses the location information under one of the following circumstances:
  - 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.
  - The location information is inadvertently discovered by the provider and appears to pertain to the commission of a felony or of a misdemeanor involving physical violence, sexual abuse, or dishonesty.

Similarly, a law enforcement agency could, without a warrant, 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 under one or more of the following circumstances:

- The owner of the electronic device or electronic information or data provides informed consent.
- 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 under 18 USC 2258A.
- From the provider if the provider voluntarily discloses the stored or transmitted data as otherwise permitted under 18 USC 2702.[1]

Notification requirements

When a warrant is executed, the act would require a law enforcement agency to issue a notification to the owner of the electronic device or electronic information or data that is specified in the warrant. The notification would have to be issued within 14 days after the day on which the electronic information or data that is the subject of the warrant is obtained. 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 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 is known or could be reasonably identified by the law enforcement agency. Notification would not have to be made if the owner of the device or information or data is located outside of the United States.

A law enforcement agency could request, and a court could grant permission, to delay the notification for up to 30 days if the court determines that there is reasonable cause to believe that the notification could result in one or more of the following circumstances:

- 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 a trial.

If the 30-day extension were granted, an additional extension of up to 30 days could be granted upon application by the law enforcement agency. Notwithstanding this additional 30-day extension, the court could grant an additional extension (to the original 30-day extension) of up to 60 days upon application if the court determines that a delayed notification is justified because one or both of the following apply to the investigation involving the warrant:

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

Upon expiration of a delayed notification period granted under the above provisions, the law enforcement agency would have to serve upon or deliver by first-class mail (or by other means

[1] Generally speaking, 18 USC 2702 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 could divulge the contents of a communication under certain specified circumstances.

if delivery is impracticable) a copy of the warrant to the owner of the electronic device or electronic information or data, together with a notice that contains all of the following:

- Information provided with reasonable specificity regarding the nature of the law enforcement inquiry.
- The information required to be on the notice notifying the owner a warrant had been issued.
- 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 allowing a delay of notification.

Subscriber record

Except as provided in the act, a law enforcement agency would be prohibited from obtaining (including through the use of a ***cell-site simulator device*** or other methods), using, copying, or disclosing a ***subscriber record***. In addition, a law enforcement agency could not, without a warrant, obtain, 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.

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 about a subscriber or customer:

- Name and 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.

Cell-site simulator device would mean 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.

Notwithstanding the above provisions, 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 informed and affirmative consent of the subscriber or customer.
- In accordance with a judicially recognized exception to the warrant requirement.
- If the subscriber or customer voluntarily disclosed the record in a manner that is publicly accessible.
- If the provider of an electronic communication service or remote computing service voluntarily discloses the record under one or more of the following circumstances:
  - A belief that an emergency exists involving the imminent risk to an individual of death, serious physical injury, sexual abuse, live-streamed sexual exploitation, kidnapping, or human trafficking.

- The record is inadvertently discovered by the provider, if the record appears to pertain to the commission of a felony or a misdemeanor that involves physical violence, sexual abuse, or dishonesty.
- As otherwise permitted under 18 USC 2702.

Immunity for providing information under a warrant

An electronic communication service provider or remote computing service provider, or the provider's officers, employees, agents, or other specified persons 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

All electronic information or data and subscriber or customer records of an electronic communications service provider or remote computing service provider that are obtained in violation of the act would be subject to the rules governing exclusion as if they were obtained in violation of the Fourth Amendment to the United States Constitution and section 11 of Article I of the state constitution.

FISCAL IMPACT:

Senate Bill 341 would be unlikely to have a significant fiscal impact on the Department of State Police, other law enforcement agencies, or other units of state or local government. It is already a common practice for law enforcement to obtain warrants in the types of cases covered under this bill. There may be minor costs associated with the notification requirements under the bill, but these costs are not expected to be significant. A potential exists for long-term fiscal impacts if the requirements of the bill impact the types of investigations that state law enforcement agencies can conduct, as federal reimbursements in some cases may be compromised.

Legislative Analyst: Susan Stutzky
Fiscal Analyst: Marcus Coffin