

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:

1 Sec. 1. This act shall be known and may be cited as the

1 "electronic information and data privacy act".

2 Sec. 2. As used in this act:

3 (a) "Cell-site simulator device" means a device that transmits
4 or receives radio waves to or from a communications device and that
5 can be used to intercept, collect, access, transfer, or forward the
6 data transmitted or received by the communications device, or
7 stored on the communications device. Cell-site simulator device
8 includes an international mobile subscriber identity catcher or
9 other cellular telephone or telephone surveillance or eavesdropping
10 device that mimics a cellular base station and transmits radio
11 waves that cause cellular telephones or other communications
12 devices in the area to transmit or receive radio waves, electronic
13 data, location data, information used to calculate location,
14 identifying information, communications content, or metadata, or
15 otherwise obtains that information through passive means, such as
16 through the use of a digital analyzer or other passive interception
17 device. However, cell-site simulator device does not include any
18 device used or installed by an electric utility solely to the
19 extent that the device is used by that utility to measure
20 electrical usage, to provide services to customers, or to operate
21 the electric grid.

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

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

28 (d) "Electronic information or data" includes information or
29 data including a sign, signal, writing, image, sound, or

1 intelligence of any nature transmitted or stored in whole or in
2 part by a wire, radio, electromagnetic, photoelectronic, or
3 photooptical system, and the location information, stored data, or
4 transmitted data of an electronic device.

5 (e) Electronic information or data does not include:

6 (i) A wire or oral communication.

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

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

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

15 (g) "Location information" means information, obtained by
16 means of a tracking device, concerning the location of an
17 electronic device that, in whole or in part, is generated or
18 derived from or obtained by the operation of an electronic device.

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

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

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

29 (k) "Subscriber record" means a record or information of a

1 provider of an electronic communication service or remote computing
2 service that reveals any of the following information regarding the
3 subscriber or customer:

4 (i) Name.

5 (ii) Address.

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

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

9 (v) Type of service used.

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

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

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

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

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

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

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

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

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

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

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

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

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

29 (5) A law enforcement agency may obtain location information

1 without a warrant for an electronic device under 1 or more of the
2 following circumstances:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21 (b) The kind of warrant issued.

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

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

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

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

28 (2) The notification requirement under subsection (1) is not
29 triggered until the owner of the electronic device or electronic

1 information or data specified in the warrant is known, or could be
2 reasonably identified, by the law enforcement agency.

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

- 9 (a) Endangering the life or physical safety of an individual.
10 (b) Causing a person to flee from prosecution.
11 (c) Leading to the destruction of or tampering with evidence.
12 (d) Intimidating a potential witness.
13 (e) Otherwise seriously jeopardizing an investigation or
14 unduly delaying a trial.

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

18 (5) Notwithstanding subsection (4), when a delay of
19 notification is granted under subsection (3), and upon application
20 by a law enforcement agency, the court may grant an additional
21 extension of up to 60 days if the court determines that a delayed
22 notification is justified because 1 or both of the following apply
23 to the investigation involving the warrant:

- 24 (a) The investigation is interstate in nature and sufficiently
25 complex.
26 (b) The investigation is likely to extend up to or beyond an
27 additional 60 days.

28 (6) Upon expiration of the period of delayed notification
29 granted under subsection (3), (4), or (5), the law enforcement

1 agency shall serve upon or deliver by first-class mail, or by other
2 means if delivery is impracticable, to the owner of the electronic
3 device or electronic information or data a copy of the warrant
4 together with a notice that contains all of the following:

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

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

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

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

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

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

18 Sec. 5. (1) Except as otherwise provided in this section or as
19 permitted by law, a law enforcement agency shall not obtain,
20 including through the use of a cell-site simulator device or other
21 methods, use, copy, or disclose a subscriber record.

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

29 (3) Notwithstanding subsections (1) and (2), a law enforcement

1 agency may obtain, use, copy, or disclose a subscriber record, or
2 other record or information related to a subscriber or customer,
3 without a warrant under the following circumstances:

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

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

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

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

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

15 (A) Death.

16 (B) Serious physical injury.

17 (C) Sexual abuse.

18 (D) Live-streamed sexual exploitation.

19 (E) Kidnapping.

20 (F) Human trafficking.

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

24 (A) A felony.

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

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

28 (4) A provider of an electronic communication service or
29 remote computing service, or the provider's officers, employees,

1 agents, or other specified persons may not be held liable for
2 providing information, facilities, or assistance in good-faith
3 reliance on the terms of a warrant issued under this section or
4 without a warrant in accordance with subsection (3).

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