

STATE OF OKLAHOMA

1st Session of the 58th Legislature (2021)

SENATE BILL 852

By: Dahm

AS INTRODUCED

An Act relating to electronic information privacy; creating the Electronic Communication and Device Privacy Act; providing short title; defining terms; prohibiting a government entity from access or compelling production of certain electronic information; authorizing compelled production of certain information under certain circumstances; stating special circumstances; allowing physical interaction with certain devices under warrants and consent; providing for certain good faith and emergency access; providing for access to devices in correctional facility; requiring warrant for information to comply with certain provisions; stating provisions; establishing court procedures for warrants and petitions; stating authority; requiring destruction of certain information within certain time; providing for emergency access to electronic device information; construing authority for other processes to secure electronic information; requiring notification for accessing electronic information; providing for delayed notification under certain circumstances; providing for extension of delayed notification; directing copy of all electronic information be notified to targets of warrants; directing certain information be submitted to the Department of Public Safety if there is no identified target for warrant; providing for publication and redacting of names on certain reports; construing service providers ability to disclose information; providing for suppression of evidence; requiring compliance with state and federal law and procedure in trial; authorizing the Attorney General to institute civil action; authorizing petition for court order to avoid access to electronic information in violation of law; granting immunity for certain

1 corporation officers for release of certain
2 information; providing for codification; and
3 providing an effective date.

4
5 BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

6 SECTION 1. NEW LAW A new section of law to be codified
7 in the Oklahoma Statutes as Section 1265 of Title 22, unless there
8 is created a duplication in numbering, reads as follows:

9 This act shall be known and may be cited as the "Electronic
10 Communication and Device Privacy Act".

11 SECTION 2. NEW LAW A new section of law to be codified
12 in the Oklahoma Statutes as Section 1265.1 of Title 22, unless there
13 is created a duplication in numbering, reads as follows:

14 For purposes of this act, the following definitions apply:

15 1. "Adverse result" means any of the following:

- 16 a. danger to the life or physical safety of an
17 individual,
18 b. flight from prosecution,
19 c. destruction of or tampering with evidence,
20 d. intimidation of potential witnesses, or
21 e. serious jeopardy to an investigation or undue delay of
22 a trial;

1 2. "Authorized possessor" means the possessor of an electronic
2 device when that person is the owner of the device or has been
3 authorized to possess the device by the owner of the device;

4 3. "Electronic communication" means the transfer of signs,
5 signals, writings, images, sounds, data or intelligence of any
6 nature in whole or in part by a wire, radio, electromagnetic,
7 photoelectric, or photo-optical system;

8 4. "Electronic communication information" means any information
9 about an electronic communication or the use of an electronic
10 communication service including, but not limited to, the contents,
11 sender, recipients, format, or location of the sender or recipients
12 at any point during the communication, the time or date the
13 communication was created, sent, or received or any information
14 pertaining to any individual or device participating in the
15 communication including, but not limited to, an IP address.
16 Electronic communication information does not include subscriber
17 information as defined in this act;

18 5. "Electronic communication service" means a service that
19 provides to its subscribers or users the ability to send or receive
20 electronic communications including any service that acts as an
21 intermediary in the transmission of electronic communications, or
22 stores electronic communication information;

23 6. "Electronic device" means a device that stores, generates or
24 transmits information in electronic form;

1 7. "Electronic device information" means any information stored
2 on or generated through the operation of an electronic device
3 including the current and prior locations of the device.

4 8. "Electronic information" means electronic communication
5 information or electronic device information;

6 9. "Government entity" means a department or agency of the
7 state or a political subdivision thereof, or an individual acting
8 for or on behalf of the state or a political subdivision thereof;

9 10. "Service provider" means a person or entity offering an
10 electronic communication service;

11 11. "Specific consent" means consent provided directly to the
12 government entity seeking information including, but not limited to,
13 when the government entity is the addressee or intended recipient or
14 a member of the intended audience of an electronic communication.

15 Specific consent does not require that the originator of the
16 communication have actual knowledge that an addressee, intended
17 recipient or member of the specific audience is a government entity;
18 and

19 12. "Subscriber information" means the name, street address,
20 telephone number, email address or similar contact information
21 provided by the subscriber to a service provider to establish or
22 maintain an account or communication channel, a subscriber or
23 account number or identifier, the length of service, and the types
24 of services used by a user of or subscriber to a service provider.

1 SECTION 3. NEW LAW A new section of law to be codified
2 in the Oklahoma Statutes as Section 1265.2 of Title 22, unless there
3 is created a duplication in numbering, reads as follows:

4 A. Except as provided in this section, a government entity
5 shall not do any of the following:

6 1. Compel the production of or access to electronic
7 communication information from a service provider;

8 2. Compel the production of or access to electronic device
9 information from any person or entity other than the authorized
10 possessor of the device;

11 3. Access electronic device information by means of physical
12 interaction or electronic communication with the electronic device.

13 This section does not prohibit the intended recipient of an
14 electronic communication from voluntarily disclosing electronic
15 communication information concerning that communication to a
16 government entity;

17 B. A government entity may compel the production of or access
18 to electronic communication information from a service provider, or
19 compel the production of or access to electronic device information
20 from any person or entity other than the authorized possessor of the
21 device only under the following circumstances:

22 1. Pursuant to a lawful warrant issued pursuant to the Oklahoma
23 Statutes or federal law and subject to subsection D of this section;

1 2. Pursuant to a wiretap order issued pursuant to the Oklahoma
2 Statutes or federal law;

3 3. Pursuant to an order for electronic reader records issued
4 pursuant to Oklahoma Statutes or federal law; or

5 4. Pursuant to a subpoena issued pursuant to existing state law
6 provided that the information is not sought for the purpose of
7 investigating or prosecuting a criminal offense, and that compelling
8 the production of or access to the information via the subpoena is
9 not otherwise prohibited by state or federal law. Nothing in this
10 paragraph shall be construed to expand any authority under state law
11 to compel the production of or access to electronic information.

12 C. A government entity may access electronic device information
13 by means of physical interaction or electronic communication with
14 the device only as follows:

15 1. Pursuant to a warrant issued pursuant to the Oklahoma
16 Statutes or federal law and subject to subsection D of this section;

17 2. Pursuant to a wiretap order issued pursuant to the Oklahoma
18 Statutes or federal law;

19 3. With the specific consent of the authorized possessor of the
20 device;

21 4. With the specific consent of the owner of the device, only
22 when the device has been reported as lost or stolen;

1 5. If the government entity, in good faith, believes that an
2 emergency involving danger of death or serious physical injury to
3 any person requires access to the electronic device information;

4 6. If the government entity, in good faith, believes the device
5 to be lost, stolen, or abandoned; provided, that the entity shall
6 only access electronic device information in order to attempt to
7 identify, verify, or contact the owner or authorized possessor of
8 the device; or

9 7. Except where prohibited by state or federal law, if the
10 device is seized from an inmate's possession or found in an area of
11 a correctional facility under the jurisdiction of the Department of
12 Corrections where inmates have access and the device is not in the
13 possession of an individual and the device is not known or believed
14 to be the possession of an authorized visitor. Nothing in this
15 paragraph shall be construed to supersede or override the Oklahoma
16 Statutes or rules promulgated by the Department of Corrections for
17 electronic devices.

18 D. Any warrant for electronic information shall comply with the
19 following:

20 1. The warrant shall describe with particularity the
21 information to be seized by specifying the time periods covered and,
22 as appropriate and reasonable, the target individuals or accounts,
23 the applications or services covered, and the types of information
24 sought;

1 2. The warrant shall require that any information obtained
2 through the execution of the warrant that is unrelated to the
3 objective of the warrant shall be sealed and not subject to further
4 review, use or disclosure without a court order. A court shall
5 issue such an order upon a finding that there is probable cause to
6 believe that the information is relevant to an active investigation,
7 or review, use or disclosure is required by state or federal law;
8 and

9 3. The warrant shall comply with all other provisions of state
10 and federal law including any provisions prohibiting, limiting or
11 imposing additional requirements on the use of search warrants. If
12 directed to a service provider, the warrant shall be accompanied by
13 an order requiring the service provider to verify the authenticity
14 of electronic information that it produces by providing an affidavit
15 that complies with the requirements set forth in the Oklahoma
16 Evidence Code. Admission of that information into evidence shall be
17 subject to the Oklahoma Evidence Code.

18 E. When issuing any warrant or order for electronic
19 information, or upon the petition from the target or recipient of
20 the warrant or order, a court may, at its discretion, do any or all
21 of the following:

22 1. Appoint a special master charged with ensuring that only
23 information necessary to achieve the objective of the warrant or
24 order is produced or accessed; and

1 2. Require that any information obtained through the execution
2 of the warrant or order that is unrelated to the objective of the
3 warrant be destroyed as soon as feasible after the termination of
4 the current investigation and any related investigations or
5 proceedings.

6 F. A service provider may voluntarily disclose electronic
7 communication information or subscriber information when that
8 disclosure is not otherwise prohibited by state or federal law.

9 G. If a government entity receives electronic communication
10 information voluntarily provided pursuant to subsection F of this
11 section, it shall destroy that information within ninety (90) days
12 unless one or more of the following circumstances apply:

13 1. The entity has or obtains the specific consent of the sender
14 or recipient of the electronic communications about which
15 information was disclosed;

16 2. The entity obtains a court order authorizing the retention
17 of the information. A court shall issue a retention order upon a
18 finding that the conditions justifying the initial voluntary
19 disclosure persist, in which case the court shall authorize the
20 retention of the information only for so long as those conditions
21 persist, or there is probable cause to believe that the information
22 constitutes evidence that a crime has been committed; or

23 3. The entity reasonably believes that the information relates
24 to child pornography and the information is retained as part of a

1 multiagency database used in the investigation of child pornography
2 and related crimes.

3 H. If a government entity obtains electronic information
4 pursuant to an emergency involving danger of death or serious
5 physical injury to a person that requires access to the electronic
6 information without delay, the entity shall, within three (3) days
7 after obtaining the electronic information, file with the
8 appropriate court an application for a warrant or order authorizing
9 obtaining the electronic information or a motion seeking approval of
10 the emergency disclosure that shall set forth the facts giving rise
11 to the emergency, and if applicable, a request supported by a sworn
12 affidavit for an order delaying notification under paragraph 1 of
13 subsection B of Section 4 of this act. The court shall promptly
14 rule on the application or motion. Upon a finding that the facts
15 did not give rise to an emergency or upon rejecting the warrant or
16 order application on any other ground, the court shall order the
17 immediate destruction of all information obtained, and immediate
18 notification pursuant to subsection A of Section 4 of this act, if
19 such notice has not already been given.

20 I. This section does not limit the authority of a government
21 entity to use an administrative, grand jury, trial, or civil
22 discovery subpoena to do any of the following:
23
24
25

1 1. Require an originator, addressee, or intended recipient of
2 an electronic communication to disclose any electronic communication
3 information associated with that communication;

4 2. Require an entity that provides electronic communications
5 services to its officers, directors, employees or agents for the
6 purpose of carrying out their duties, to disclose electronic
7 communication information associated with an electronic
8 communication to or from an officer, director, employee or agent of
9 the entity; or

10 3. Require a service provider to provide subscriber
11 information.

12 SECTION 4. NEW LAW A new section of law to be codified
13 in the Oklahoma Statutes as Section 1265.3 of Title 22, unless there
14 is created a duplication in numbering, reads as follows:

15 A. Except as otherwise provided in this section, any government
16 entity that executes a warrant, or obtains electronic information in
17 an emergency pursuant to Section 3 of this act, shall serve upon, or
18 deliver to by registered or first-class mail, electronic mail or
19 other means reasonably calculated to be effective, the identified
20 targets of the warrant or emergency request, a notice that informs
21 the recipient that information about the recipient has been
22 compelled or requested, and states with reasonable specificity the
23 nature of the government investigation under which the information
24 is sought. The notice shall include a copy of the warrant or a

1 written statement setting forth facts giving rise to the emergency.
2 The notice shall be provided contemporaneously with the execution of
3 a warrant, or, in the case of an emergency, within three (3) days
4 after obtaining the electronic information.

5 B. 1. When a warrant is sought or electronic information is
6 obtained in an emergency under Section 3 of this act, the government
7 entity may submit a request supported by a sworn affidavit for an
8 order delaying notification and prohibiting any party providing
9 information from notifying any other party that information has been
10 sought. The court shall issue the order if the court determines
11 that there is reason to believe that notification may have an
12 adverse result, but only for the period of time that the court finds
13 there is reason to believe that the notification may have that
14 adverse result, and not to exceed ninety (90) days.

15 2. The court may grant extensions of the delay of up to ninety
16 (90) days each on the same grounds as provided in paragraph 1 of
17 this subsection.

18 3. Upon expiration of the period of delay of the notification,
19 the government entity shall serve upon, or deliver to by registered
20 or first-class mail, electronic mail, or other means reasonably
21 calculated to be effective as specified by the court issuing the
22 order authorizing delayed notification, the identified targets of
23 the warrant, a document that includes the information described in
24 subsection A of this section, a copy of all electronic information

1 obtained or a summary of that information including, at a minimum,
2 the number and types of records disclosed, the date and time when
3 the earliest and latest records were created, and a statement of the
4 grounds for the court's determination to grant a delay in notifying
5 the individual.

6 C. If there is no identified target of a warrant or emergency
7 request at the time of its issuance, the government entity shall
8 submit to the Department of Public Safety within three (3) days of
9 the execution of the warrant or issuance of the request all of the
10 information required in subsection A of this section. If an order
11 delaying notice is obtained pursuant to subsection B of this
12 section, the government entity shall submit to the Department upon
13 the expiration of the period of delay of the notification all of the
14 information required in paragraph 3 of subsection B of this section.
15 The Department shall publish all those reports on its website within
16 ninety (90) days of receipt. The Department may redact names or
17 other personal identifying information from the reports.

18 D. Except as otherwise provided in this section, nothing in
19 this act shall prohibit or limit a service provider or any other
20 party from disclosing information about any request or demand for
21 electronic information.

22 SECTION 5. NEW LAW A new section of law to be codified
23 in the Oklahoma Statutes as Section 1265.4 of Title 22, unless there
24 is created a duplication in numbering, reads as follows:

1 A. Any person in a trial, hearing or proceeding may move to
2 suppress any electronic information obtained or retained in
3 violation of the Fourth Amendment to the United States Constitution
4 or of this act. The motion shall be made, determined, and be
5 subject to review in accordance with the procedures set forth in the
6 Oklahoma Statutes.

7 B. The Attorney General may commence a civil action to compel
8 any government entity to comply with the provisions of this act.

9 C. An individual whose information is targeted by a warrant,
10 order or other legal process that is inconsistent with this act or
11 the United States Constitution, or a service provider or any other
12 recipient of the warrant, order or other legal process may petition
13 the issuing court to void or modify the warrant, order or process,
14 or to order the destruction of any information obtained in violation
15 of this act or the United States Constitution.

16 D. An Oklahoma or foreign corporation, and its officers,
17 employees and agents are not subject to any cause of action for
18 providing records, information, facilities or assistance in
19 accordance with the terms of a warrant, court order, statutory
20 authorization, emergency certification or wiretap order issued
21 pursuant to this act.

22 SECTION 6. This act shall become effective November 1, 2021.
23

24 58-1-1325 NP 1/21/2021 3:49:20 PM
25