

STATE OF OKLAHOMA

1st Session of the 59th Legislature (2023)

SENATE BILL 35

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 provider 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 BE IT ENACTED BY THE PEOPLE OF THE STATE OF OKLAHOMA:

5 SECTION 1. NEW LAW A new section of law to be codified  
6 in the Oklahoma Statutes as Section 1251 of Title 22, unless there  
7 is created a duplication in numbering, reads as follows:

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

10 SECTION 2. NEW LAW A new section of law to be codified  
11 in the Oklahoma Statutes as Section 1252 of Title 22, unless there  
12 is created a duplication in numbering, reads as follows:

13 As used in this act:

14 1. "Adverse result" means:

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

22 2. "Authorized possessor" means the possessor of an electronic  
23 device when such person is the owner of the device or has been  
24 authorized to possess the device by the owner of the device;

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

5           4. "Electronic communication information" means any information  
6 about an electronic communication or the use of an electronic  
7 communication service including, but not limited to, the contents,  
8 sender, recipients, format, or location of the sender or recipients  
9 at any point during the communication, the time or date the  
10 communication was created, sent, or received or any information  
11 pertaining to any individual or device participating in the  
12 communication including, but not limited to, an IP address.

13 Electronic communication information does not include subscriber  
14 information as defined in this act;

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

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

22           7. "Electronic device information" means any information stored  
23 on or generated through the operation of an electronic device  
24 including the current and prior locations of the device;

1 8. "Electronic information" means electronic communication  
2 information or electronic device information;

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

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

8 11. "Specific consent" means consent provided directly to the  
9 government entity seeking information including but not limited to  
10 when the government entity is the addressee or intended recipient or  
11 a member of the intended audience of an electronic communication.  
12 Specific consent does not require that the originator of the  
13 communication have actual knowledge that an addressee, intended  
14 recipient, or member of the specific audience is a government  
15 entity; and

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

22 SECTION 3. NEW LAW A new section of law to be codified  
23 in the Oklahoma Statutes as Section 1253 of Title 22, unless there  
24 is created a duplication in numbering, reads as follows:

1 A. Except as provided in this section, a government entity  
2 shall not:

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

5 2. Compel the production of or access to electronic device  
6 information from any person or entity other than the authorized  
7 possessor of the device; or

8 3. Access electronic device information by means of physical  
9 interaction or electronic communication with the electronic device.

10 This section does not prohibit the intended recipient of an  
11 electronic communication from voluntarily disclosing electronic  
12 communication information concerning that communication to a  
13 government entity.

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

19 1. Pursuant to a lawful warrant issued pursuant to federal law  
20 or the laws of this state and subject to subsection D of this  
21 section;

22 2. Pursuant to a wiretap order issued pursuant to federal law  
23 or the laws of this state;

1           3. Pursuant to an order for electronic reader records issued  
2 pursuant to federal law or the laws of this state; or

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

10           C. A government entity may access electronic device information  
11 by means of physical interaction or electronic communication with  
12 the device only:

13           1. Pursuant to a warrant issued pursuant to federal law or the  
14 laws of this state and subject to subsection D of this section;

15           2. Pursuant to a wiretap order issued pursuant to federal law  
16 or the laws of this state;

17           3. With the specific consent of the authorized possessor of the  
18 device;

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

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

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

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

15           D. Any warrant for electronic information shall comply with the  
16 following:

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

22           2. The warrant shall require that any information obtained  
23 through the execution of the warrant that is unrelated to the  
24 objective of the warrant shall be sealed and not subject to further

1 review, use, or disclosure without a court order. A court shall  
2 issue such an order upon a finding that there is probable cause to  
3 believe that the information is relevant to an active investigation,  
4 or if its review, use, or disclosure is required by state or federal  
5 law; and

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

15 E. When issuing any warrant or order for electronic  
16 information, or upon the petition from the target or recipient of  
17 the warrant or order, a court may do one or both of the following:

18 1. Appoint a special master charged with ensuring that only  
19 information necessary to achieve the objective of the warrant or  
20 order is produced or accessed; or

21 2. Require that any information obtained through the execution  
22 of the warrant or order that is unrelated to the objective of the  
23 warrant be destroyed as soon as feasible after the termination of  
24



1 the current investigation and any related investigations or  
2 proceedings.

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

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

10 1. The entity has or obtains the specific consent of the sender  
11 or recipient of the electronic communications about which  
12 information was disclosed;

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

20 3. The entity reasonably believes that the information relates  
21 to child pornography and the information is retained as part of a  
22 multiagency database used in the investigation of child pornography  
23 and related crimes.

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

18 I. This section shall not be construed to limit the authority  
19 of a government entity to use an administrative, grand jury, trial,  
20 or civil discovery subpoena to:

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

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

7           3. Require a service provider to provide subscriber  
8 information.

9           SECTION 4.       NEW LAW       A new section of law to be codified  
10 in the Oklahoma Statutes as Section 1254 of Title 22, unless there  
11 is created a duplication in numbering, reads as follows:

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

1 a warrant, or in the case of an emergency, within three (3) days  
2 after obtaining the electronic information.

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

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

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

1 the earliest and latest records were created, and a statement of the  
2 grounds for the court's determination to grant a delay in notifying  
3 the individual.

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

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

20 SECTION 5. NEW LAW A new section of law to be codified  
21 in the Oklahoma Statutes as Section 1255 of Title 22, unless there  
22 is created a duplication in numbering, reads as follows:

23 A. Any person in a trial, hearing, or proceeding may move to  
24 suppress any electronic information obtained or retained in

1 violation of the Fourth Amendment to the United States Constitution  
2 or of this act. The motion shall be made, determined, and be  
3 subject to review in accordance with the procedures set forth in the  
4 laws of this state.

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

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

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

20 SECTION 6. This act shall become effective November 1, 2023.

21  
22 59-1-421 TEK 12/14/2022 11:50:54 AM  
23  
24  
25