

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

SENATE BILL 154

**52ND LEGISLATURE - STATE OF NEW MEXICO - SECOND SESSION, 2016**

INTRODUCED BY

Peter Wirth and Jim Dines

AN ACT

RELATING TO CIVIL LIBERTIES; ENACTING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT; PROVIDING PERSONAL PROTECTIONS FROM GOVERNMENT ACCESS TO ELECTRONIC COMMUNICATIONS.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

SECTION 1. [NEW MATERIAL] SHORT TITLE.--This act may be cited as the "Electronic Communications Privacy Act".

SECTION 2. [NEW MATERIAL] DEFINITIONS.--As used in the Electronic Communications Privacy Act:

A. "adverse result" means:

- (1) danger to the life or physical safety of a natural person;
- (2) flight from prosecution;
- (3) destruction of or tampering with evidence;
- (4) intimidation of a potential witness; or

underscoring material = new  
[bracketed material] = delete

underscoring material = new  
~~[bracketed material] = delete~~

- 1 (5) serious jeopardy to an investigation;
- 2 B. "authorized possessor" means a natural person
- 3 who owns and possesses an electronic device or a natural person
- 4 who, with the owner's consent, possesses an electronic device;
- 5 C. "electronic communication" means the transfer of
- 6 a sign, a signal, a writing, an image, a sound, a datum or
- 7 intelligence of any nature in whole or in part by a wire,
- 8 radio, electromagnetic, photoelectric or photo-optical system;
- 9 D. "electronic communication information":
- 10 (1) means information about an electronic
- 11 communication or the use of an electronic communication
- 12 service, including:
- 13 (a) the contents, sender, recipients,
- 14 format or the sender's or recipients' precise or approximate
- 15 location at any point during the communication;
- 16 (b) the time or date the communication
- 17 was created, sent or received; and
- 18 (c) any information, including an
- 19 internet protocol address, pertaining to a person or device
- 20 participating in the communication; and
- 21 (2) excludes subscriber information;
- 22 E. "electronic communication service" means a
- 23 service that:
- 24 (1) allows its subscribers or users to send or
- 25 receive electronic communications, including by acting as an

1 intermediary in the transmission of electronic communications;  
2 or

3 (2) stores electronic communication  
4 information;

5 F. "electronic device" means a device that stores,  
6 generates or transmits information in electronic form;

7 G. "electronic device information":

8 (1) means information stored on or generated  
9 through the operation of an electronic device; and

10 (2) includes the current and prior locations  
11 of the device;

12 H. "electronic information" means electronic  
13 communication information or electronic device information;

14 I. "government entity" means:

15 (1) a department, agency or political  
16 subdivision of the state; or

17 (2) a natural person acting for or on behalf  
18 of the state or a political subdivision of the state;

19 J. "service provider" means a person offering an  
20 electronic communication service;

21 K. "specific consent":

22 (1) means consent provided directly to a  
23 government entity seeking information; and

24 (2) includes consent provided when the  
25 government entity is the addressee, the intended recipient or a

underscoring material = new  
[bracketed material] = delete

1 member of the intended audience of an electronic communication,  
2 regardless of whether the originator of the communication had  
3 actual knowledge that the addressee, intended recipient or  
4 member of the specific audience is a government entity, except  
5 where the government entity has taken deliberate steps to hide  
6 the government entity's government association; and

7 L. "subscriber information" means:

8 (1) the name, street address, telephone  
9 number, email address or other similar type of contact  
10 information provided by a subscriber to a service provider to  
11 establish or maintain an account or communication channel;

12 (2) a subscriber or account number or  
13 identifier; or

14 (3) the length and type of service used by a  
15 user or a service-provider subscriber.

16 SECTION 3. [NEW MATERIAL] GOVERNMENT ENTITY--PROSCRIBED  
17 ACTS--PERMITTED ACTS--WARRANTS--INFORMATION RETENTION--  
18 EMERGENCY.--

19 A. Except as otherwise provided in this section, a  
20 government entity shall not:

21 (1) compel or incentivize the production of or  
22 access to electronic communication information from a service  
23 provider;

24 (2) compel the production of or access to  
25 electronic device information from a person other than the

.202613.5

1 device's authorized possessor; or

2 (3) access electronic device information by  
3 means of physical interaction or electronic communication with  
4 the electronic device.

5 B. A government entity may compel the production of  
6 or access to electronic communication information from a  
7 service provider or compel the production of or access to  
8 electronic device information from a person other than the  
9 authorized possessor of the device only if the production or  
10 access is made:

11 (1) under a warrant that complies with the  
12 requirements in Subsection D of this section; or

13 (2) under a wiretap order.

14 C. A government entity may access electronic device  
15 information by means of physical interaction or electronic  
16 communication with the device only if that access is made:

17 (1) under a warrant that complies with the  
18 requirements in Subsection D of this section;

19 (2) under a wiretap order;

20 (3) with the specific consent of the device's  
21 authorized possessor;

22 (4) with the specific consent of the device's  
23 owner if the device has been reported as lost or stolen;

24 (5) because the government entity believes in  
25 good faith that the device is lost, stolen or abandoned, in

1 which case the government entity may access that information  
2 only for the purpose of attempting to identify, verify or  
3 contact the device's authorized possessor; or

4 (6) because the government entity believes in  
5 good faith that an emergency involving danger of death or  
6 serious physical injury to a natural person requires access to  
7 the electronic device information.

8 D. A warrant for the search and seizure of  
9 electronic information shall:

10 (1) describe with particularity the  
11 information to be seized by specifying the time periods covered  
12 and, as appropriate and reasonable, the natural persons or  
13 accounts targeted, the applications or services covered and the  
14 types of information sought;

15 (2) except when the information obtained is  
16 exculpatory with respect to the natural person targeted,  
17 require that any information obtained through the execution of  
18 the warrant that is unrelated to the objective of the warrant  
19 be destroyed within thirty days after the information is seized  
20 and be not subject to further review, use or disclosure; and

21 (3) comply with all New Mexico and federal  
22 laws, including laws prohibiting, limiting or imposing  
23 additional requirements on the use of search warrants.

24 E. When issuing a warrant or order for electronic  
25 information or upon a petition of the target or recipient of

1 the warrant or order, a court may appoint a special master  
2 charged with ensuring that only the information necessary to  
3 achieve the objective of the warrant or order is produced or  
4 accessed.

5 F. A service provider may voluntarily disclose  
6 electronic communication information or subscriber information  
7 if the law otherwise permits that disclosure.

8 G. If a government entity receives electronic  
9 communication information as provided in Subsection F of this  
10 section, the government entity shall destroy that information  
11 within ninety days after the disclosure unless the government  
12 entity:

13 (1) has or obtains the specific consent of the  
14 sender or recipient of the electronic communication about which  
15 information was disclosed; or

16 (2) obtains a court order under Subsection H  
17 of this section.

18 H. A court may issue an order authorizing the  
19 retention of electronic communication information:

20 (1) only upon a finding that the conditions  
21 justifying the initial voluntary disclosure persist; and

22 (2) lasting only for the time those conditions  
23 persist or there is probable cause to believe that the  
24 information constitutes criminal evidence.

25 I. Information retained as provided in Subsection H

1 of this section shall be shared only with a person that agrees  
2 to limit the person's use of the information to the purposes  
3 identified in the court order and:

4 (1) is legally obligated to destroy the  
5 information upon the expiration or rescindment of the court  
6 order; or

7 (2) voluntarily agrees to destroy the  
8 information upon the expiration or rescindment of the court  
9 order.

10 J. If a government entity obtains electronic  
11 information because of an emergency that involves danger of  
12 death or serious physical injury to a natural person and that  
13 requires access to the electronic information without delay,  
14 the government entity shall file with the appropriate court  
15 within three days after obtaining the electronic information:

16 (1) an application for a warrant or order  
17 authorizing the production of electronic information and, if  
18 applicable, a request supported by a sworn affidavit for an  
19 order delaying notification as provided in Subsection B of  
20 Section 4 of the Electronic Communications Privacy Act; or

21 (2) a motion seeking approval of the emergency  
22 disclosures that sets forth the facts giving rise to the  
23 emergency and, if applicable, a request supported by a sworn  
24 affidavit for an order delaying notification as provided in  
25 Subsection B of Section 4 of the Electronic Communications



underscoring material = new  
~~[bracketed material] = delete~~

1 Privacy Act.

2 K. A court that receives an application or motion  
3 as provided in Subsection J of this section shall promptly rule  
4 on the application or motion. If the court finds that the  
5 facts did not give rise to an emergency or if the court rejects  
6 the application for a warrant or order on any other ground, the  
7 court shall order:

8 (1) the immediate destruction of all  
9 information obtained; and

10 (2) the immediate notification provided in  
11 Subsection A of Section 4 of the Electronic Communications  
12 Privacy Act if that notice has not already been given.

13 L. This section does not limit the authority of a  
14 government entity to use an administrative, grand jury, trial  
15 or civil discovery subpoena to require:

16 (1) an originator, addressee or intended  
17 recipient of an electronic communication to disclose any  
18 electronic communication information associated with that  
19 communication;

20 (2) when a person that provides electronic  
21 communications services to its officers, directors, employees  
22 or agents for those officers, directors, employees or agents to  
23 carry out their duties, the person to disclose the electronic  
24 communication information associated with an electronic  
25 communication to or from the officer, director, employee or

.202613.5

underscored material = new  
[bracketed material] = delete

1 agent; or

2 (3) a service provider to provide subscriber  
3 information.

4 M. This section does not prohibit the intended  
5 recipient of an electronic communication from voluntarily  
6 disclosing electronic communication information concerning that  
7 communication to a government entity.

8 N. Nothing in this section shall be construed to  
9 expand any authority under New Mexico law to compel the  
10 production of or access to electronic information.

11 SECTION 4. [NEW MATERIAL] WARRANT--EMERGENCY--GOVERNMENT  
12 DUTIES--NOTIFICATION.--

13 A. Except as otherwise provided in this section, a  
14 government entity that executes a warrant or obtains electronic  
15 information in an emergency as provided in Section 3 of the  
16 Electronic Communications Privacy Act shall:

17 (1) serve upon or deliver, by registered or  
18 first-class mail, electronic mail or other means reasonably  
19 calculated to be effective, to the identified targets of the  
20 warrant or emergency request, a notice that informs the  
21 recipient that information about the recipient has been  
22 compelled or requested and that states with reasonable  
23 specificity the nature of the government investigation under  
24 which the information is sought;

25 (2) serve or deliver the notice:

.202613.5

1 (a) contemporaneously with the execution  
2 of a warrant; or

3 (b) in the case of an emergency, within  
4 three days after obtaining the electronic information; and

5 (3) include with the notice:

6 (a) a copy of the warrant; or

7 (b) a written statement setting forth  
8 the facts giving rise to the emergency.

9 B. When a government entity seeks a warrant or  
10 obtains electronic information in an emergency as provided in  
11 Section 3 of the Electronic Communications Privacy Act, the  
12 government entity may request from a court an order delaying  
13 notification and prohibiting any party providing information  
14 from notifying any other party that information has been  
15 sought. The government entity shall support the request with a  
16 sworn affidavit. The court:

17 (1) shall issue the order if the court  
18 determines that there is reason to believe that notification  
19 may have an adverse result, but for no more than ninety days  
20 and only for the period that the court finds there is reason to  
21 believe that the notification may have that adverse result; and

22 (2) may grant one or more extensions of the  
23 delay of up to ninety days each on the grounds provided in  
24 Paragraph (1) of this subsection.

25 C. When the period of delay of a notification

underscoring material = new  
~~[bracketed material] = delete~~

1 ordered by a court as provided in Subsection B of this section  
2 expires, the government entity that requested the order shall  
3 serve upon or deliver, by registered or first-class mail,  
4 electronic mail or other means reasonably calculated to be  
5 effective, as specified by the court issuing the order, to the  
6 identified targets of the warrant:

7 (1) a document that includes the information  
8 described in Subsection A of this section; and

9 (2) a copy of all electronic information  
10 obtained or a summary of that information, including, at a  
11 minimum:

12 (a) the number and types of records  
13 disclosed;

14 (b) the date and time when the earliest  
15 and latest records were created; and

16 (c) a statement of the grounds for the  
17 court's determination to grant a delay in notifying the  
18 targeted person.

19 D. If there is no identified target of a warrant or  
20 emergency request at the time of the warrant's or request's  
21 issuance, the government entity shall submit to the attorney  
22 general within three days after the execution of the warrant or  
23 request issuance the information described in Subsection A of  
24 this section. If an order delaying notice is obtained under  
25 Subsection B of this section, the government entity shall

.202613.5

underscored material = new  
[bracketed material] = delete

1 submit to the attorney general when the period of delay of the  
2 notification expires the information described in Subsection C  
3 of this section. The attorney general shall publish all those  
4 reports on the attorney general's website within ninety days  
5 after receipt. The attorney general shall redact names and  
6 other personal identifying information from the reports.

7 E. Except as otherwise provided in this section,  
8 nothing in the Electronic Communications Privacy Act prohibits  
9 or limits a service provider or any other party from disclosing  
10 information about a request or demand for electronic  
11 information.

12 SECTION 5. [NEW MATERIAL] VIOLATIONS OF LAW.--

13 A. A person in a trial, hearing or proceeding may  
14 move to suppress any electronic information obtained or  
15 retained in violation of the United States constitution, the  
16 constitution of New Mexico or the Electronic Communications  
17 Privacy Act. The motion shall be made, determined and subject  
18 to review in accordance with the procedures provided in law.

19 B. The attorney general may commence a civil action  
20 to compel a government entity to comply with the Electronic  
21 Communications Privacy Act.

22 C. A natural person, service provider or other  
23 recipient of a warrant, order or other legal process obtained  
24 in violation of the United States constitution, the  
25 constitution of New Mexico or the Electronic Communications

.202613.5

underscored material = new  
[bracketed material] = delete

1 Privacy Act may petition the court that issued the warrant,  
2 order or process to void or modify it or order the destruction  
3 of any information obtained in violation of those sources of  
4 law.

5 SECTION 6. [NEW MATERIAL] ANNUAL REPORTING.--

6 A. A government entity that obtains electronic  
7 communication information under the Electronic Communications  
8 Privacy Act shall report to the attorney general beginning in  
9 2018 and every year thereafter on or before February 1. The  
10 report shall include, to the extent it reasonably can be  
11 determined:

12 (1) the number of times electronic information  
13 was sought or obtained under the Electronic Communications  
14 Privacy Act;

15 (2) the number of times each of the following  
16 were sought and, for each, the number of records obtained:

17 (a) electronic communication content;

18 (b) location information;

19 (c) electronic device information,  
20 excluding location information; and

21 (d) other electronic communication  
22 information; and

23 (3) for each type of information listed in  
24 Paragraph (2) of this subsection:

25 (a) the number of times that type of

1 information was sought or obtained under: 1) a wiretap order  
2 issued under the Electronic Communications Privacy Act; 2) a  
3 search warrant issued under the Electronic Communications  
4 Privacy Act; and 3) an emergency request as provided in  
5 Subsection J of Section 3 of the Electronic Communications  
6 Privacy Act;

7 (b) the number of persons whose  
8 information was sought or obtained;

9 (c) the number of instances in which  
10 information sought or obtained did not specify a target natural  
11 person;

12 (d) for demands or requests issued upon  
13 a service provider, the number of those demands or requests  
14 that were fully complied with, partially complied with and  
15 refused;

16 (e) the number of times notice to  
17 targeted persons was delayed and the average length of the  
18 delay;

19 (f) the number of times records were  
20 shared with other government entities or any department or  
21 agency of the federal government and the government entity,  
22 department or agency names with which the records were shared;

23 (g) for location information, the  
24 average period for which location information was obtained or  
25 received; and

1 (h) the number of times electronic  
2 information obtained under the Electronic Communications  
3 Privacy Act led to a conviction and the number of instances in  
4 which electronic information was sought or obtained that were  
5 relevant to the criminal proceedings leading to those  
6 convictions.

7 B. Beginning in 2018 and every year thereafter, on  
8 or before April 1, the attorney general shall publish on the  
9 attorney general's website:

10 (1) the individual reports from each  
11 government entity that requests or compels the production of  
12 contents or records pertaining to an electronic communication  
13 or location information; and

14 (2) a summary aggregating each of the items in  
15 Subsection A of this section.

16 C. Nothing in the Electronic Communications Privacy  
17 Act prohibits or restricts a service provider from producing an  
18 annual report summarizing the demands or requests it receives  
19 under the Electronic Communications Privacy Act.