

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

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. SHORT TITLE.--This act may be cited as the  
"Electronic Communications Privacy Act".

SECTION 2. 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
  - (5) serious jeopardy to an investigation;

B. "authorized possessor" means a natural person who owns and possesses an electronic device or a natural person who, with the owner's consent, possesses an electronic device;

C. "electronic communication" means the transfer of a sign, a signal, a writing, an image, a sound, a datum or intelligence of any nature in whole or in part by a wire,

1 radio, electromagnetic, photoelectric or photo-optical  
2 system;

3 D. "electronic communication information":

4 (1) means information about an electronic  
5 communication or the use of an electronic communication  
6 service, including:

7 (a) the contents, sender, recipients,  
8 format or the sender's or recipients' precise or approximate  
9 location at any point during the communication;

10 (b) the time or date the communication  
11 was created, sent or received; and

12 (c) any information, including an  
13 internet protocol address, pertaining to a person or device  
14 participating in the communication; and

15 (2) excludes subscriber information;

16 E. "electronic communication service" means a  
17 service that:

18 (1) allows its subscribers or users to send  
19 or receive electronic communications, including by acting as  
20 an intermediary in the transmission of electronic  
21 communications; or

22 (2) stores electronic communication  
23 information;

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

1 G. "electronic device information":

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

4 (2) includes the current and prior locations  
5 of the device;

6 H. "electronic information" means electronic  
7 communication information or electronic device information;

8 I. "government entity" means:

9 (1) a department, agency or political  
10 subdivision of the state; or

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

13 J. "service provider" means a person offering an  
14 electronic communication service;

15 K. "specific consent":

16 (1) means consent provided directly to a  
17 government entity seeking information; and

18 (2) includes consent provided when the  
19 government entity is the addressee, the intended recipient or  
20 a member of the intended audience of an electronic  
21 communication, regardless of whether the originator of the  
22 communication had actual knowledge that the addressee,  
23 intended recipient or member of the specific audience is a  
24 government entity, except where the government entity has  
25 taken deliberate steps to hide the government entity's

1 government association; and

2 L. "subscriber information" means:

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

7 (2) a subscriber or account number or  
8 identifier; or

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

11 SECTION 3. GOVERNMENT ENTITY--PROSCRIBED ACTS--  
12 PERMITTED ACTS--WARRANTS--INFORMATION RETENTION--EMERGENCY.--

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

15 (1) compel or incentivize the production of  
16 or access to electronic communication information from a  
17 service provider;

18 (2) compel the production of or access to  
19 electronic device information from a person other than the  
20 device's authorized possessor; or

21 (3) access electronic device information by  
22 means of physical interaction or electronic communication  
23 with the electronic device.

24 B. A government entity may compel the production  
25 of or access to electronic communication information from a

1 service provider or compel the production of or access to  
2 electronic device information from a person other than the  
3 authorized possessor of the device only if the production or  
4 access is made:

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

7 (2) under a wiretap order.

8 C. A government entity may access electronic  
9 device information by means of physical interaction or  
10 electronic communication with the device only if that access  
11 is made:

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

14 (2) under a wiretap order;

15 (3) with the specific consent of the  
16 device's authorized possessor;

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

20 (5) because the government entity believes  
21 in good faith that the device is lost, stolen or abandoned,  
22 in which case, the government entity may access that  
23 information only as necessary and for the purpose of  
24 attempting to identify, verify or contact the device's  
25 authorized possessor; or

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

5 D. A warrant for the search and seizure of  
6 electronic information shall:

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

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

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

22 E. When issuing a warrant or order for electronic  
23 information or upon a petition of the target or recipient of  
24 the warrant or order, a court may appoint a special master  
25 charged with ensuring that only the information necessary to

1 achieve the objective of the warrant or order is produced or  
2 accessed.

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

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

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

14 (2) obtains a court order under Subsection H  
15 of this section.

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

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

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

23 I. Information retained as provided in Subsection  
24 H of this section shall be shared only with a person that  
25 agrees to limit the person's use of the information to the

1 purposes identified in the court order and that:

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

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

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

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

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

25 K. A court that receives an application or motion

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

6 (1) the immediate destruction of all  
7 information obtained; and

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

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

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

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

25 (3) a service provider to provide subscriber

1 information.

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

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

9 SECTION 4. WARRANT--EMERGENCY--GOVERNMENT  
10 DUTIES--NOTIFICATION.--

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

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

23 (2) serve or deliver the notice:

24 (a) contemporaneously with the  
25 execution of a warrant; or

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

3 (3) include with the notice:

4 (a) a copy of the warrant; or

5 (b) a written statement setting forth  
6 the facts giving rise to the emergency.

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

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

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

24 C. When the period of delay of a notification  
25 ordered by a court as provided in Subsection B of this

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

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

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

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

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

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

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

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

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

12 SECTION 5. 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  
18 subject to review in accordance with the procedures provided  
19 in law.

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

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

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

6 SECTION 6. ANNUAL REPORTING.--

7 A. A government entity that obtains electronic  
8 communication information under the Electronic Communications  
9 Privacy Act shall report to the attorney general beginning in  
10 2019 and every year thereafter on or before February 1. The  
11 report shall include, to the extent it reasonably can be  
12 determined:

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

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

19 (a) electronic communication content;

20 (b) location information;

21 (c) electronic device information,  
22 excluding location information; and

23 (d) other electronic communication  
24 information; and

25 (3) for each type of information listed in

1 Paragraph (2) of this subsection:

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

9 (b) the number of persons whose  
10 information was sought or obtained;

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

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

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

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

1 (g) for location information, the  
2 average period for which location information was obtained or  
3 received; and

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

10 B. Beginning in 2019 and every year thereafter, on  
11 or before April 1, the attorney general shall publish on the  
12 attorney general's website:

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

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

19 C. Nothing in the Electronic Communications  
20 Privacy Act prohibits or restricts a service provider from  
21 producing an annual report summarizing the demands or requests  
22 it receives under the Electronic Communications Privacy  
23 Act.