

1 SENATE BILL 270

2 **54TH LEGISLATURE - STATE OF NEW MEXICO - SECOND SESSION, 2020**

3 INTRODUCED BY

4 Daniel A. Ivey-Soto and Gail Chasey

5  
6  
7  
8  
9  
10 AN ACT

11 RELATING TO ELECTRONIC COMMUNICATIONS; AMENDING THE ELECTRONIC  
12 COMMUNICATIONS PRIVACY ACT; ADDRESSING THE REQUIREMENTS AND  
13 PROCEDURES FOR A WARRANT FOR THE SEARCH AND SEIZURE OF  
14 ELECTRONIC INFORMATION; PROVIDING FOR THE DESTRUCTION OR  
15 SEALING OF INFORMATION IN CERTAIN SITUATIONS; AMENDING  
16 REQUIREMENTS FOR REPORTING ACTIONS TO THE ATTORNEY GENERAL.

17  
18 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

19 SECTION 1. Section 10-16F-3 NMSA 1978 (being Laws 2019,  
20 Chapter 39, Section 3) is amended to read:

21 "10-16F-3. GOVERNMENT ENTITY--PROSCRIBED ACTS--PERMITTED  
22 ACTS--WARRANTS--INFORMATION RETENTION--EMERGENCY.--

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

25 (1) compel or incentivize the production of or

.217076.2

underscored material = new  
[bracketed material] = delete

1 access to electronic communication information from a service  
2 provider;

3 (2) compel the production of or access to  
4 electronic device information from a person other than the  
5 device's authorized possessor; or

6 (3) access electronic device information by  
7 means of physical interaction or electronic communication with  
8 the electronic device.

9 B. A government entity may compel the production of  
10 or access to electronic communication information from a  
11 service provider or compel the production of or access to  
12 electronic device information from a person other than the  
13 authorized possessor of the device only if the production or  
14 access is made under a:

15 (1) warrant that complies with the  
16 requirements in Subsection D of this section; or

17 (2) wiretap order.

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

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

23 (2) under a wiretap order;

24 (3) with the specific consent of the device's  
25 authorized possessor;

underscored material = new  
[bracketed material] = delete

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

3 (5) because the government entity believes in  
4 good faith that the device is lost, stolen or abandoned, in  
5 which case, the government entity may access that information  
6 only as necessary and for the purpose of attempting to  
7 identify, verify or contact the device's authorized possessor;  
8 or

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

13 D. A warrant for the search and seizure of  
14 electronic information shall:

15 (1) describe with particularity the  
16 information to be seized by specifying the time periods covered  
17 and, as appropriate and reasonable, the natural persons or  
18 accounts targeted, the applications or services covered and the  
19 types of information sought;

20 (2) ~~[except when the information obtained is~~  
21 ~~exculpatory with respect to the natural person targeted,~~  
22 ~~require that any information obtained through the execution of~~  
23 ~~the warrant that is unrelated to the objective of the warrant~~  
24 ~~be destroyed within thirty days after the information is seized~~  
25 ~~and be not subject to further review, use or disclosure]~~

.217076.2

1 require that information obtained through the execution of the  
2 warrant that is unrelated to the objective of the warrant or is  
3 not exculpatory to the target of the warrant shall be sealed  
4 and shall not be subject to further review, use or disclosure  
5 except pursuant to a court order or to comply with discovery as  
6 required. A court shall issue such an order upon a finding  
7 that there is probable cause to believe that the information is  
8 relevant to an active investigation or review, use or  
9 disclosure is required by state or federal law; and

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

13 E. When issuing a warrant or order for electronic  
14 information or upon a petition of the target or recipient of  
15 the warrant or order, a court may appoint a special master  
16 charged with ensuring that only the information necessary to  
17 achieve the objective of the warrant or order is produced or  
18 accessed.

19 F. A service provider may voluntarily disclose  
20 electronic communication information or subscriber information  
21 if the law otherwise permits that disclosure.

22 G. Information obtained through the execution of a  
23 warrant or order that is unrelated to the objective of the  
24 warrant shall be destroyed as soon as feasible after the  
25 termination of the current investigation and related

underscoring material = new  
[bracketed material] = delete

1 investigations or proceedings.

2           H. If a government entity receives electronic  
3 communication information as provided in Subsection F of this  
4 section, the government entity shall ~~[destroy]~~ seal that  
5 information, which shall not be subject to further review, use  
6 or disclosure except pursuant to a court order upon a finding  
7 that there is probable cause to believe that the information is  
8 relevant to an active investigation or review, use or  
9 disclosure is required by state or federal law or to comply  
10 with discovery as required, within ninety days after the  
11 disclosure unless the government entity:

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

15                   (2) obtains a court order under Subsection ~~[H]~~  
16 I of this section.

17           ~~[H.]~~ I. A court may issue an order authorizing the  
18 retention of electronic communication information:

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

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

24           ~~[I.]~~ J. Information retained as provided in  
25 Subsection ~~[H]~~ I of this section shall be shared only with a

.217076.2

underscored material = new  
[bracketed material] = delete

1 person that agrees to limit the person's use of the information  
2 to the purposes identified in the court order and that:

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

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

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

15 (1) an application for a warrant or order  
16 authorizing the production of electronic information and, if  
17 applicable, a request supported by a sworn affidavit for an  
18 order delaying notification as provided in Subsection B of  
19 Section [~~4 of the Electronic Communications Privacy Act]~~  
20 10-16F-4 NMSA 1978; 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~~

.217076.2

underscored material = new  
[bracketed material] = delete

1 ~~Privacy Act]~~ 10-16F-4 NMSA 1978.

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

8                   (1) the immediate ~~[destruction]~~ sealing of all  
9 information obtained, which shall not be subject to further  
10 review, use or disclosure except pursuant to a court order upon  
11 a finding that there is probable cause to believe that the  
12 information is relevant to an active investigation or review,  
13 use or disclosure is required by state or federal law or to  
14 comply with discovery as required; and

15                   (2) the immediate notification provided in  
16 Subsection A of Section ~~[4 of the Electronic Communications~~  
17 ~~Privacy Act]~~ 10-16F-4 NMSA 1978 if that notice has not already  
18 been given.

19           ~~[L.]~~ M. This section does not limit the authority  
20 of a government entity to use an administrative, grand jury,  
21 trial or civil discovery subpoena to require:

22                   (1) an originator, addressee or intended  
23 recipient of an electronic communication to disclose any  
24 electronic communication information associated with that  
25 communication;

.217076.2

underscored material = new  
[bracketed material] = delete

1 (2) when a person that provides electronic  
2 communications services to its officers, directors, employees  
3 or agents for those officers, directors, employees or agents to  
4 carry out their duties, the person to disclose the electronic  
5 communication information associated with an electronic  
6 communication to or from the officer, director, employee or  
7 agent; or

8 (3) a service provider to provide subscriber  
9 information.

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

14 [~~N.~~] O. Nothing in this section shall be construed  
15 to expand any authority under New Mexico law to compel the  
16 production of or access to electronic information.

17 P. This section shall not be construed to alter the  
18 authority of a government entity that owns an electronic device  
19 to compel an employee who is authorized to possess the device  
20 to return the device to the government entity's possession."

21 SECTION 2. Section 10-16F-4 NMSA 1978 (being Laws 2019,  
22 Chapter 39, Section 4) is amended to read:

23 "10-16F-4. WARRANT--EMERGENCY--GOVERNMENT DUTIES--  
24 NOTIFICATION.--

25 A. Except as otherwise provided in this section, a

.217076.2



underscored material = new  
[bracketed material] = delete

1 government entity that executes a warrant or obtains electronic  
2 information in an emergency as provided in Section [~~3 of the~~  
3 ~~Electronic Communications Privacy Act~~] 10-16F-3 NMSA 1978  
4 shall:

5 (1) serve upon or deliver, by registered or  
6 first-class mail, electronic mail or other means reasonably  
7 calculated to be effective, to the identified targets of the  
8 warrant or emergency request, a notice that informs the  
9 recipient that information about the recipient has been  
10 compelled or requested and that states with reasonable  
11 specificity the nature of the government investigation under  
12 which the information is sought;

13 (2) serve or deliver the notice:

14 (a) contemporaneously with the execution  
15 of a warrant; or

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

18 (3) include with the notice:

19 (a) a copy of the warrant; or  
20 (b) a written statement setting forth  
21 the facts giving rise to the emergency.

22 B. When a government entity seeks a warrant or  
23 obtains electronic information in an emergency as provided in  
24 Section [~~3 of the Electronic Communications Privacy Act~~]  
25 10-16F-3 NMSA 1978, the government entity may request from a

.217076.2

1 court an order delaying notification and prohibiting any party  
2 providing information from notifying any other party that  
3 information has been sought. The government entity shall  
4 support the request with a sworn affidavit. The court:

5 (1) shall issue the order if the court  
6 determines that there is reason to believe that notification  
7 may have an adverse result, but for no more than ninety days  
8 and only for the period that the court finds there is reason to  
9 believe that the notification may have that adverse result; and

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

13 C. When the period of delay of a notification  
14 ordered by a court as provided in Subsection B of this section  
15 expires, the government entity that requested the order shall  
16 serve upon or deliver, by registered or first-class mail,  
17 electronic mail or other means reasonably calculated to be  
18 effective, as specified by the court issuing the order, to the  
19 identified targets of the warrant:

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

22 (2) a copy of all electronic information  
23 obtained or a summary of that information, including, at a  
24 minimum:

25 (a) the number and types of records

underscoring material = new  
[bracketed material] = delete

1 disclosed; and

2 ~~[(b) the date and time when the earliest~~  
3 ~~and latest records were created; and~~

4 ~~(e)]~~ (b) a statement of the grounds for  
5 the court's determination to grant a delay in notifying the  
6 targeted person.

7 D. If there is no identified target of a warrant or  
8 emergency request at the time of the warrant's or request's  
9 issuance, the government entity shall submit to the attorney  
10 general within three days after the execution of the warrant or  
11 request issuance the information described in Paragraph (1) of  
12 Subsection A of this section. If an order delaying notice is  
13 obtained under Subsection B of this section, the government  
14 entity shall submit to the attorney general when the period of  
15 delay of the notification expires the information described in  
16 Paragraph (2) of Subsection C of this section and the  
17 information required by this subsection. The attorney general  
18 shall publish all those reports on the attorney general's  
19 website ~~[within ninety days after receipt. The attorney~~  
20 ~~general shall redact names and other personal identifying~~  
21 ~~information from the reports]~~ as provided in Section 10-16F-6  
22 NMSA 1978.

23 E. Except as otherwise provided in this section,  
24 nothing in the Electronic Communications Privacy Act prohibits  
25 or limits a service provider or any other party from disclosing

.217076.2

underscored material = new  
[bracketed material] = delete

1 information about a request or demand for electronic  
2 information."

3 SECTION 3. Section 10-16F-6 NMSA 1978 (being Laws 2019,  
4 Chapter 39, Section 6) is amended to read:

5 "10-16F-6. 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 [2020] 2021 and every year thereafter on or before February 1.  
10 The 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

.217076.2

underscored material = new  
[bracketed material] = delete

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] K of Section [~~3 of the Electronic Communications~~  
6 ~~Privacy Act~~] 10-16F-3 NMSA 1978;

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

9 ~~(e)]~~ (b) the number of instances in  
10 which information sought or obtained did not specify a target  
11 natural person; and

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)]~~ (c) 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~~

.217076.2

underscored material = new  
[bracketed material] = delete

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

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

B. Beginning in [2020] 2021 and every year thereafter, on or before April 1, the attorney general shall publish on the attorney general's website

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

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

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