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,

radio, electromagnetic, photoelectric or photo-optical system;

D. "electronic communication information":

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

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

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

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

(2) excludes subscriber information;

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

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

(2) stores electronic communication information;

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

G. "electronic device information":

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

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

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

I. "government entity" means:

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

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

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

K. "specific consent":

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

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

government association; and

L. "subscriber information" means:

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

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

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

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

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

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

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

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

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

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

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

(2) wiretap order.

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

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

(2) under a wiretap order;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

purposes identified in the court order and that:

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

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

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

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

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

K. A court that receives an application or motion

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

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

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

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

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

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

(3) a service provider to provide subscriber

information.

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

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

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

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

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

(2) serve or deliver the notice:

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

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

(3) include with the notice:

(a) a copy of the warrant; or

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

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

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

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

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

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

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

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

(a) the number and types of records disclosed;

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

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

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

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

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

SECTION 5. VIOLATIONS OF LAW.--

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

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

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

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

SECTION 6. ANNUAL REPORTING.--

A. A government entity that obtains electronic communication information under the Electronic Communications Privacy Act shall report to the attorney general beginning in 2020 and every year thereafter on or before February 1. The report shall include, to the extent it reasonably can be determined:

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

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

(a) electronic communication content;

(b) location information;

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

(d) other electronic communication information; and

(3) for each type of information listed in

Paragraph (2) of this subsection:

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

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

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

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

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

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

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

(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 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.