1.0 PURPOSE

The purpose of this policy is to establish procedures and guidelines to conform to the Electronic Communications Privacy Act (ECPA).

2.0 POLICY

It is the policy of the DPS to preserve evidence and property in such a manner as to ensure its actual and evidentiary value. It is also departmental policy to dispose of evidence and property promptly and lawfully when such items are no longer required for departmental purposes, or not permitted to be retained under the ECPA.

3.0 APPLICABILITY

This policy applies to all employees of the Department of Public Safety.

4.0 REFERENCES

A. CALEA Chapter 12 - Direction

B. Electronic Communications Privacy Act; NMSA 1978, 10-16F-1 through 10-16F-6.

5.0 DEFINITIONS

A. Adverse Result - danger to the life or physical safety of a natural person, flight from prosecution, destruction of or tampering with evidence intimidation of a potential witness, or serious jeopardy to an investigation.

B. Authorized Processor - 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. Contemporaneously - as close as practicable to the same time and the same date.

D. Electronic Communication - 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.

E. Electronic Communication Information - information about electronic communication or the use of an electronic communication service, including the contents, sender, recipients, format or the sender's or recipients' precise or approximate location at any point during the communication; the time or date the communication was created, sent or received; and any information, including an

internet protocol address, pertaining to a person or device participating in the communication; and excludes subscriber information.

F. Electronic Communication Service - 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.

G. Electronic Device - a device that stores, generates, or transmits information in electronic form.

H. Electronic Device Information - information stored on or generated through the operation of an electronic device; and includes the current and prior locations of the device.

I. Electronic information - electronic communication information or electronic device information;

J. Government Entity - means a department, agency, or political subdivision of the state, or a natural person acting for or on behalf of the state or a political subdivision of the state.

K. Service Provider - means a person offering an electronic communication service;

L. Specific Consent - consent provided directly to a government entity seeking information; and includes consent provided when the government entity is the addressee, the intended recipient, or a member of the intended audience of 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.

M. Subscriber Information - the name, street address, telephone number, email address, or other similar types of contact information provided by a subscriber to a service provider to establish or maintain an account or communication channel, a subscriber or account number or identifier; or the length and type of service used by a user or a service-provider subscriber.

6.0 PROCEDURE

A. Obtaining electronic information.

1. An NMSP officer may only obtain electronic information from a service provider or from a person other than the authorized possessor of the device with a:

   a. Warrant that complies with the requirements in section A-3. below; or

   b. Wiretap order.

2. An NMSP officer may only access information directly from an electronic device:

   a. Under a warrant that complies with the requirements in section A(3);

b. Under a wiretap order;

c. With the consent of the device's authorized possessor;

d. With the consent of the device's owner if the device has been reported lost or stolen.

e. If the officer has a reasonable belief that the device is lost, stolen, or abandoned. The officer may only access information to identify, verify or contact the device's authorized possessor;

f. If the officer has a reasonable belief that an emergency involving danger of death or serious physical injury requires access to the electronic device information.

3. A warrant for the search and seizure of electronic information in criminal investigations shall:

a. Describe the specific information to be seized, as well the specific time periods covered and, the persons or accounts targeted, the applications or services covered, and the types of information sought;

b. The electronic information to be seized will be limited to the objective of the warrant and to any exculpatory information.

c. Require that any information unrelated to the objective of the warrant be sealed. It cannot be accessed again without a court order.

4. If service provider voluntarily provides electronic communication information or subscriber information to an NMSP officer without a warrant or court order as in the case of an exigent circumstances disclosure (e.g., search and rescue or life-threatening circumstance, e.g., kidnapping):

a. The information shall be sealed within ninety (90) days, and can only be accessed again with:

i. A court order or search warrant showing probable cause to believe that the information is relevant to an active criminal investigation,

ii. With the consent of the sender or recipient of the electronic communication.

b. Electronic information retained pursuant to a court order shall be shared only with a person who agrees to limit its use to purposes identified in the court order, and agrees to, or is legally obligated to, destroy the information upon expiration or rescindment of the order. This should generally be limited

to a government agency involved in the investigation or prosecution of the criminal case. No non-criminal cases will have their data shared;

i. Orders issued by the court which identify others with whom the information will be shared will set the terms by which those receiving ECI from NMSP must abide.

5. Court Orders: for cases that do not require search warrants (SAR and exigent circumstances), an officer may get a court order authorizing the retention of electronic communication information:

a. If the officer can show that the conditions justifying the initial voluntary disclosure persist, as in the case of an ongoing search and rescue mission; and/or

b. Lasting only for the time those conditions persist or there is probable cause to believe that the information constitutes criminal evidence in which case, a search warrant will be obtained to retain that evidence.

c. If an NMSP officer obtains electronic information because of an emergency that involves danger of death or serious physical injury, and that requires access to the electronic information without delay, the officer shall file an order in the appropriate court within three days after obtaining the electronic information. That information shall include the facts giving rise to the emergency.

6. The ECPA does not apply to someone who receives an electronic communication and voluntarily gives that information to an officer.

7. The ECPA does not cover department phones or other electronic equipment. There is no expectation of privacy on department phones or other electronic equipment.

8. Destruction of data as required by ECPA: This data will be destroyed as soon as practical upon the complete adjudication of the criminal case along with all evidence gathered in the course of the investigation and in compliance with NMSP evidence destruction policy and procedure established in OPR: 17.

B Notification Requirements

1. An officer that executes a warrant in a criminal investigation or obtains a court order for electronic information obtained in an emergency shall,

a. Deliver to the identified target of the warrant or court order, by registered mail, first-class mail, electronic mail, or by other reasonable means, a notice that informs the target of the warrant or court order, including the

nature of the government investigation under which the information is sought with reasonable specificity.

b. Serve or deliver the notice,

i. Contemporaneously with the execution of a warrant at the point which a return of inventory can be completed, unless a court order for delayed notification is obtained.

ii. In case of a court order for an emergency, within three days after obtaining the electronic information.

c. Included with the notice:

i. A copy of the warrant, or;

ii. In the case of an emergency disclosure, a written statement setting forth the facts giving rise to the emergency.

2. Delay of Notification: An officer may request a court order delaying notification and prohibiting any other party from notifying the target of a warrant for no more than 90 days.

a. The officer shall support the request with a sworn affidavit stating facts showing that notification may have an adverse result on the criminal investigation

b. The officer may request one or more extensions of the delay up to ninety days each.

c. When the delay of notification expires, the officer shall deliver to the identified target of the warrant, by registered mail, first-class mail, electronic mail, or by other reasonable means, a notice that informs the target of the warrant, including the nature of the government investigation under which the information is sought with reasonable specificity.

d. The notice after a delay of notification shall also include a copy of all electronic information obtained or a summary of that information, including, at a minimum:

i. The number and types of records disclosed

ii. A statement of the grounds for the court's determination to grant a delay in notifying the targeted person.

e. See below for delayed notifications for cases with no identified targets.

3. Notification requirements for no identified targets: If there is no identified target of an investigation or the authorized possessor is unknown at the time the officer obtains the warrant or court order, the officer shall submit the information to the Attorney General's office that would have been sent to the target of the warrant or court order within 3 days.

   a. If an order delaying notice is obtained when there is no identified target, the officer shall submit the same information to the Attorney General's office that would have been sent to the target of the warrant when the period of delay expires.

C. Penalties for Violations of ECPA

Any electronic information obtained or retained in violation of the Electronic Communications Privacy Act may be suppressed.

D. Annual reporting

1. Beginning in 2021, NMSP must annually report to the Attorney General's Office on or before February 1, the electronic communication information obtained pursuant to the Electronic Communications Privacy Act. The report shall include, to the extent it reasonably can be determined:

   a. The number of times electronic information was sought or obtained under the Electronic Communications Privacy Act

   b. The number of times each of the following were sought and for each, the number of records obtained:

      i. Electronic communication content

      ii. Location information

      iii. Electronic device information excluding location information,

      iv. Other electronic communication information

   c. For each type of information listed in paragraph b of this subsection the number of times that type of information was sought or obtained under:

      i. A wiretap order issued under the Electronic Communications Privacy Act

      ii. A search warrant issued under the Electronic CommunicationPrivacy Act

      iii. An emergency request as allowed under the Electronic Communications Privacy Act

d. The number of instances in which information sought or obtained did not specify a target natural person, and the number of times notice to targeted persons was delayed.

7.0 ATTACHMENTS

A. Cell Phone Extraction Procedure

B. Electronic Device Consent to Search Form

C. Emergency Cell Phone Ping Template

D. How-To-Guide to seal in the ECPA Retention folder in the Z-Drive

E. ECPA Search Warrant Flow Chart

F. ECPA Tracking Form

G. Cell Phone Download Search Warrant Template

H. Cellular Ping Search Warrant Template

I. ECPA Notification Guide

8.0 APPROVAL

APPROVED BY:_____Jason R. Bowie_____DATE:___10-07-21_____
DPS Cabinet Secretary