**EXHIBIT A**

**LOCATIONS TO BE SEARCHED**

Located at (list current location of the device)

*Note: This may be your agency*

**EXHIBIT B**

**FOR THE FOLLOWING PROPERTY:**

One (describe cellular device), Model #\_\_\_\_\_\_\_, on the \_\_\_\_\_\_\_ network with access number \_\_\_\_\_\_\_\_\_, ESN/IMEI number \_\_\_\_\_\_\_\_\_\_ and all memory cards immediately associated/attached with the cellular telephone such as SIM cards and memory cards. (the "Cellular Device").

*Note: The above language assumes that you are in possession of the cellular device. When you have the device it only needs to be described with sufficient particularity that anyone would recognize it. This can be as simple as one black iPhone identified as Item # 4 placed into evidence under Agency Report No. 14-12345. (See Pen. Code, § 1529; People v. Duncan (1981) 115 Cal.App.3d 418, 426.)*

**FOR THE FOLLOWING ITEMS LOCATED ON THE PROPERTY:**

All data that constitute evidence and instrumentalities of [SPECIFIED CRIMES] occurring between [DATES SOUGHT], including communications referring or relating to a this investigation involving any or all of the following: [SPECIFIED INDIVIDUALS AND ENTITIES] including:

1. All communications content, including email, text (SMS/MMS or app chats), notes, or voicemail. This data will also include attachments, source and destination addresses, and time and date information, and connection logs, images and any other records that constitute evidence and instrumentalities of [SPECIFIED CRIMES] for the dates above, including communications referring or relating to this investigation involving any or all of the following: [SPECIFIED INDIVIDUALS AND ENTITIES] together with indicia of use, ownership, possession, or control of such communications or information found.

2. All location data for the dates above. Location data may be stored as GPS locations or cellular tower connection data. Location data may be found in the metadata of photos and social networking posts, wi-fi logs, and data associated with installed applications

3. All photographic/video/audio data and associated metadata

4. All internet history for the dates above, including cookies, bookmarks, web history, search terms

5. All financial information.

6. All indicia of ownership and control for both the data and the cellular device, such as device identification and settings data, address book/contacts, social network posts/updates/tags, wi-fi network tables, associated wireless devices (such as known wi-fi networks and Bluetooth devices), associated connected devices (such as for backup and syncing), stored passwords, user dictionaries.

Investigating officers are authorized, at their discretion, to conduct an offsite search of the seized items for the property described. Investigating officers and those agents acting under the direction of the investigating officers are authorized to access all data on the cellular device to determine if the data contains the items as described above. If necessary, investigating officers are authorized to employ the use of outside experts, acting under the direction of the investigating officers, to access and preserve data on the cellular device. Those items that are within the scope of this warrant may be copied and retained by investigative officers.

As required by California Penal Code § 1524.1 (d); any information obtained through the execution of this warrant that is unrelated to the objective of the warrant shall be sealed and shall not be subject further review, use, or disclosure absent an order from the Court.

If no evidence of criminal activity is discovered relating to the seized property and associated peripherals, the system will be returned promptly.

*Note: Describe the records that you have probable cause to believe will be recovered from the cellular phone.* *Description of records must describe with particularity the information to be seized by specifying the time periods covered and, as appropriate and reasonable, the target individuals or accounts, the application of services covered, and the types of information sought. (Pen. Code, §§ 1546.1 (d)(1), 1525, 1529.)*

*As opposed to trying to describe the record by its type, describe the item as it pertains to a specified person or between specified dates. For example, records showing communication between suspect John Doe and any other party relating to the sale of methamphetamine occurring between July 1, 2014 and December 30, 2014. Remember not all of the above listed data sets may be relevant to your case; investigators should edit the affidavit and attachments to remove requests for information that will not be needed in a particular case.*