Cell phone search warrant language

Search Warrant Language For Cellular Phones[1/] (5/06)

Cellular phones have become the virtual biographer of our daily activities. It tracks who we talk to and where we are. It will log calls, take pictures, and keep our contact list close at hand. In short it has become an indispensable piece of evidence in a criminal investigation.

Want to know where your suspect was last Saturday? The cellular service provider can provide you the location information of the cellular phone as it relates to the provider's network. What about the last person your victim called? Both the cellular phone and the cellular provider will keep a record of this. How about finding gang member photos associated with their gang moniker? It will be located within their cellular phones.

Information relating to a cellular phone will be found in two places. In the phone itself and in the records possessed by the cellular service provider. The following is offered to provide guidance on drafting a search warrant for the production of records maintained by the cellular provider.

The first step in obtaining records from a cellular service provider is to identify the provider. A cellular phone carrier can be queried directly to ascertain if they provide service to a known number. The North American Numbering Plan Administration also tracks the numbers that have been assigned to service providers. (http://www.nationalnanpa.com) Since a cellular phone number may now be ported (transferred) by a consumer to another cellular service provider, law enforcement should make a number porting check. Law enforcement may sign up for the service at (http://www.nationalpooling.com/forms/law/index.htm)

The second step in obtaining records from a cellular service provider is a preservation request to "freeze" stored records and communications pursuant to 18 U.S.C. § 2703(f). Many cellular service providers maintain records for only a short period of time. This requests can be used as a directive to third-party providers to preserve records and not disclose the investigation to the suspect. This is an important tool to use to prevent third-party providers from writing over or deleting data you need while you obtain a warrant. Currently there are no laws which govern how long a third-party provider must retain log

---

1. The following search warrant language was complied by California Deputy Attorney General Robert Morgester for use by law enforcement. Source material was derived from law enforcement training programs provided by Air Touch Cellular and AT&T Wireless Service; investigators of the Sacramento Valley High Tech Crime Task Force, with special thanks to Turlock Police Department Detective Kip Loving and California Highway Patrol Officer Bill McDonald; Deputy Attorney General Keith Lyon; Karl Dunnagan of Mobile Forensics, Inc.; Bill Napieralski, and many others. Suggestions or other information relating to cellular search warrant language would be appreciated. Comments may be sent to Robert.Morgester@doj.ca.gov.

or other information. Sample preservation orders can be found at http://www.cybercrime.gov./s&sappendix2002.htm (Appendix C) or http://mobileforensics.info/

It is also recommended that you contact the cellular service provider to ascertain the type and nature of records kept and any special terms or definitions that the carrier uses to describe those records. Any request for records should be limited to only the records that are needed. Do not request all of the categories of records listed unless it is truly needed for your case. Cellular phone records can be described in the warrant as follows:

A.) Subscriber information

Note: This should give you the name, address, phone numbers, and other personal identifying information relating to the subscriber.

B.) Account comments

Note: Anytime the provider has contact with the customer or modifies the customer's account a notation will be made by a service representative on the account.

C.) Credit information

Note: Most providers run a credit report on customer prior to activating the account

D.) Billing records

Note: Do not ask for toll information; that is a landline term for long distance. Specify period desired.

E.) Outbound and inbound call detail

Note: This is the real time, current activity that is not yet on the customer's bill. "Inbound" is usually available for only a limited time (45 days) which gives other cellular phones calling the target number.

F.) Call origination / termination location

Note: Available for a limited time (45 days) and gives location information on cell sites used, length of call, date, time, numbers dialed. With a GPS enabled phone it gives location of phone.

G.) Physical address of cell sites and RF coverage map

Note: Needed to determine where cell site is located when you receive inbound & outbound or call origination & termination location. The RF coverage map models

the theoretical radio frequency coverage of the towers in the system. You will want to limit this request to a specified geographical area.

H.) Any other cellular telephone numbers that dial the same numbers as (xxx) xxx-xxxx

Note: If you want to know who calls the same number the target calls (for example a pager or landline number). Available for only a limited time (45 days).

I.) Subscriber information on any cellular numbers that (xxx) xxx-xxxx dials

Note: Subscriber information on the carrier's network that is dialing the target.

J.) All of the above records whether possessed by cellular service provider [target of warrant] or any other cellular service provider

Note: If you anticipate the suspect may be roaming or if the number is roaming in the providers market, you may be able to obtain information from other cellular carriers if you include this language in your description of records.

K.) All stored communications or files, including voice mail, email, digital images, buddy lists, and any other files associated with user accounts identified as: account(s) xxxxxx, mobile numbers (xxx) xxx-xxxx, or e-mail account roe1234@sprint.net.

Note: Cellular service providers now offer similar services to an internet service provider (ISP)and maintain the same type of records such as text messaging, e-mail, and file storage for the transfer of data including digital pictures. Limit your request to what you need.

L.) All connection logs and records of user activity for each such account including:

1. Connection dates and times.
2. Disconnect dates and times.
3. Method of connection (e.g., telnet, ftp, http)
4. Data transfer volume.
5. User name associated with the connections.
6. Telephone caller identification records.
7. Any other connection information, such as the Internet Protocol address of the source of the connection.
8. Connection information for the other computer to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, and all other information related to the connection from cellular service provider.

Note: The above is a standard request made to ISP to track connection information. Remember with the type of cellular service offered today the user can send a

message from the phone or from the associated account via a computer or other access device.

M.) Any other records or accounts, including archived records related or associated to the above-referenced names, user names, or accounts and any data field name definitions that describe these records.

Note: This is the catch all to use when you want everything. This request also includes "archived" information. Many companies now "archive" records thus allowing for the preservation of subscriber records for a significant time. Archived records are usually stored in a spread sheet format encompassing a variety of data fields. You must request the data field name definitions in order to understand the spreadsheet.

N.) PUK for SIM card # _____

Subscriber Identity Module (SIM) is a smart card inside of a GSM cellular phone that encrypts voice and data transmissions and stores data about the specific user so that the user can be identified and authenticated to the network supplying the service. The SIM also stores data such as personal phone settings specific to the user and phone numbers.

SIM cards can be password protected by the user. Even with this protection SIM cards may still be unlocked with a personal unlock key (PUK) that is available from the service provider. Note that after ten wrong PUK codes, the SIM card locks forever.

A search warrant for the production of records held by a cellular service provider should always include an order for non-disclosure. The cellular service provider will notify the customer of the search warrant unless there is a non-disclosure order. This order will delay notification for 90 days and can be extended for an additional 90 days. (See California Public Utilities Commission decision No. 93361 (7/21/1981).) A non-disclosure order may be phrased as follows:

ORDER FOR NON-DISCLOSURE OF SEARCH WARRANT

It is further ordered that cellular service provider not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this order for 90 days in that such a disclosure could give the subscriber an opportunity to destroy evidence, notify confederates, or flee or continue his flight from prosecution

Now that we have listed what records we are seeking, probable cause must be shown in the affidavit for each of the listed items. The following is sample language justifying the need for the production of specified records that can be used as a starting point for drafting the search warrant affidavit:

A.) Through experience and training, your affiant knows cellular service providers maintain records related to subscriber information, account registration, credit information, billing and airtime records, outbound and inbound call detail, connection time and dates, Internet routing information (Internet Protocol numbers), and message content, that may assist in the identification of person/s accessing and utilizing the account.

B.) Through experience and training, your affiant knows that the cellular service provider maintains records that include cell site information and GPS location. Cell site information shows which cell site a particular cellular telephone was within at the time of the cellular phone's usage. Some model cellular phone are GPS enabled which allows the provider and user to determine the exact geographic position of the phone. Further, the cellular service provider maintains cell site maps that show the geographical location of all cell sites within its service area. Using the cell site geographical information or GPS information, officers would be able to determine the physical location of the individual using the cell phone number (xxx) xxx-xxxx, which according to corroborating sources listed above was/is in use by the suspect. That information is necessary to the investigating officers in order to

---

It is also recommended that you include within the affidavit the authority which allows a search warrant to be served by facsimile (fax) for the production of records maintained outside of California.

A.) Your affiant is aware that cellular service provider is located within the State of _____. Pursuant to Penal Code section 1524.2 and Corporations Code section 2105 a California search warrant may be served upon them and they have requested that this warrant be served by facsimile to the attention of _____ at (xxx) xxx-xxxx.

Finally, a word of caution. If you use the cellular subscriber records to attempt to determine the physical location of an individual's position there are a couple of questions that must be answered.

First question is call overloading. When the maximum call processing capacity of a specified cell tower is reached it may be designed to hand off calls to other cell towers. Thus, a tower that the records reflect handled a call may have off-loaded the call to another cellular tower. The cellular provider will be able to check the cellular traffic on a specified cellular tower to determine whether or not any calls were off loaded.

Second question is whether the records reflecting the placement of a specified cellular tower's directional antenna is accurate. Occasionally the cellular provider may make adjustments to the cellular towers directional antenna that are not reflected in the records. Since the physical location of an individual's position will be based upon this directional antenna, its placement should be confirmed prior to trial.