INTEROFFICE MEMORANDUM

TO: CHRISTINA MILLER

FROM: ED BEAGAN

SUBJECT: ADMIN SUBPOENA GUIDELINES

DATE: MARCH 2009

With the passage of legislation in October of 2008, prosecutors now have enhanced administrative subpoena power to seek subscriber records held by information service providers, telecommunications companies and other sources of digital evidence. The new legislation amended M.G.L. c. 271 sec. 17B by significantly expanding the types entities which must respond to an administrative subpoena under sec. 17B, and lowering the applicable legal standard.

District court prosecutors in particular should familiarize themselves with this tool, as they can expect that detectives will be approaching them for assistance in issuing subpoenas for these records. Subscriber information can be a source of and/or a starting point for important evidence in a wide variety of cases.

Here are some typical scenarios that you will encounter, where using a subpoena may be appropriate:

Detective has a cell phone number provided by a victim of a threatening phone call, text message or communication, and wants to establish the identity of the sender.

Detective is given an email/ip addresss/screen name of a target by a victim of a threatening or harassing communication, or a fraudulent transaction.

Detective recovers a cell phone from the scene of a shooting/stabbing or other event, and wants to establish ownership of the phone.

Also, you may use this subpoena power to obtain subscriber information *after* issuance of a complaint, but see the business records materials soon to be posted on the **S: Drive/District Court Forms & Guidelines** for more information on admitting such records.

What is subscriber information?

Subscriber information is generally user account registration information, some transactional information and other types of information associated with an email account, phone number or other service provided by an ISP or communications provider. 18 U.S.C. § 2703 et seq. draws an **important distinction between content-related information**, such as the content of text messages and emails, multimedia files - and transactional information, such as the ip address used by a subscriber when they sign up for a gmail account. The administrative subpoena power authorizes access only to **subscriber information, and should not be used to request the contents of any communications - a search warrant or court order is needed to gain access to content-related records.**

Here are some examples of subscriber information that may be available from providers:

a. cell phones
    1. name, address, phone number, instrument id #
    2. billing or payment information, i.e. credit card or bank account billed.
    3. incoming and outgoing calls, dates, duration

b. email addresses
    1. ip address used by the subscriber upon registering this email address, and "ip address logs" used more recently by subscriber when accessing email. (this can lead you to a residential address of the user, with a separate subpoena to the ISP).
    2. billing or payment information, if any

c. Facebook/myspace
    1. name, address, alternate email addresses, billing information
    2. ip address logs of certain activity, e.g. uploads of photos or other events

Different service providers will maintain different types of subscriber information, so you may have to contact a service provider directly to ascertain exactly what is available to you.

Please be sure to reference the **S: Drive/District Court Forms & Guidelines\Admin Subpoenas** folder for more information and administrative subpoena templates.

These are the basic steps required for an admin subpoena, with additional detail following:

1. Ask your requestor to fill out a request form and attach a police report.
2. Determine whether the request meets the material & relevant standard of 217 sec. 17B.
3. Identify the provider/holder of subscriber records and their contact information.

4. Prepare your subpoena, and specifically request the appropriate subscriber information.
5. Assign a case number to your subpoena, arrange for entry into the Excel Spreadsheet.
6. Send out the subpoena
7. Forward subpoena response to the requesting agency.

1. Use the sample "**admin subpoena request form**" from the S: Drive. **Make sure to obtain a legitimate police report**, which you will review to determine the appropriateness of the request, bearing in mind the potential civil and criminal penalties under the Electronic Communications Privacy Act.

2. M.G.L. 217 sec. 17B now requires that the ADA issuing the subpoena have "*reasonable grounds* to believe that records in the possession of . . . [certain types of providers] . . . are *relevant and material* to an ongoing criminal investigation . . . ."

Review your police report and determine whether the information sought is relevant and material to the investigation. Normally, the records will be relevant to establishing identification, but other legitimate aims exist as well. As the ADA issuing the subpoena, **you are the entity responsible** for ensuring that this authority is used appropriately, so do not hesitate to question or seek clarification and/or further documentation from the requestor.

3. Normally your requestor will have little or no information on the company holding the records. Use the following link to identify contact information for entities like ISPs, and other providers of electronic and remote computing services, as described in the statute. http://www.search.org/programs/hightech/isp/default.asp. Bear in mind that a single entity may have subsidiaries with different subpoena processing locations, e.g. Verizon Online, Verizon Wireless and Verizon-Bell Atlantic. (There may be a template available on the S: Drive that contains a valid address/fax# for your service provider).

To determine the cell phone company of a particular cell phone #, use www.fonefinder.net. To determine the internet service provider of a particular IP address, use www.arin.net, or contact Bill Durette at SPU.

4. On the S: Drive, you will find **several read-only sample admin subpoenas, for cell phone, email address and ip address requests**. Be sure to include the latter 2 paragraphs, as they track the federal statute referenced by sec. 17B.

a. **Be as thorough as possible in requesting the information sought.** You cannot simply put in a cell phone number and expect to receive call

detail (incoming/outgoing calls). The latter 2 paragraphs are helpful in this regard, but read them carefully to make sure that you've stated, in addition to those 2 paragraphs, exactly what you are looking for. Companies will generally only give you what you ask for, even if they have additional information. Remember, this subpoena does not authorize you to seek any content of any kind, just subscriber information as defined under 18 U.S.C. § 2703(c)(1)(C).

b. **It is permissible to request that the records be returned to the requesting agency**, as opposed to SCDAO. This may save the time/effort required to receive records and forward them appropriately. However, some companies will not honor this request and will simply return them to you. Also, you may want to be aware of a subpoena response for your own case management purposes.

c. In the last line, be sure to **specify the manner in which you wish to receive** your response. Bear in mind that call detail will often by sent by compact disc or other media. Generally, companies will respond quickly via fax responses, and mail a separate copy.

5. Be sure to put your **internal case number near the top of the subpoena**, so you recognize whatever it is that arrives pursuant to your request.

6. Forward the subpoena response to the appropriate agency. Be sure to keep a copy of the subpoena response for your own records.