**MDAO PROTOCOL FOR THE ISSUANCE OF ADMINISTRATIVE SUBPOENAS**

**Updated August 26, 2013**

**INTRODUCTION**

The Massachusetts Administrative Subpoena statute, G.L. c. 271, § 17B, provides law enforcement access to a critical tool, allowing the District Attorney’s Office to obtain certain types of records from companies, including telephone and Internet Service Providers (ISPs), even before charges have been brought or a suspect has been fully identified. But it is a complicated statute, with important limitations and hidden pitfalls for the unwary. This memorandum seeks to explain the process and provide guidance for the Assistant District Attorneys and paralegals who are asked to authorize, draft and serve these subpoenas.

**THE AUTHORIZING STATUTE**

**Chapter 271: Section 17B. Use of electronic communications records in ongoing criminal investigations; subpoena of records**

[W]henever . . . a district attorney has reasonable grounds to believe that records in the possession of: (i) a common carrier . . . or (ii) a provider of electronic communication service . . . or (iii) a provider of remote computing service . . . are relevant and material to an ongoing criminal investigation . . . the district attorney may issue an administrative subpoena demanding all such records in the possession of such common carrier or service, and such records shall be delivered to the . . . district attorney within 14 days of receipt of the subpoena.

**WHO CAN ISSUE AN ADMINISTRATIVE SUBPOENA?**

An administrative subpoena can only be issued by an Assistant District Attorney (or an Assistant Attorney General). While police officers and federal agents are authorized to issue *preservation letters* to providers on their own, see 18 U.S.C. §2703(f), they are barred from issuing an administrative subpoena, and the results of any subpoena that is wrongly issued by a non-attorney are subject to suppression. See Commonwealth v. Feodoroff, 43 Mass.App.Ct. 725 (1997) (police officers are not authorized on behalf of Attorney General or district attorney to demand telephone company records on ground that company's service is being used or may be used for unlawful purpose); Commonwealth v. Vinnie, 428 Mass. 161, 178 (1998) (“[W]e hold that a defendant may move to suppress telephone records acquired by administrative subpoena and a judge should allow such a motion if it is shown that a district attorney had no reasonable grounds for belief that the target was using the telephone for an unlawful purpose”), certiorari denied 525 U.S. 1007 (1998). In most cases, the impetus for an administrative subpoena begins with a request made to the District Attorney’s Office by a police officer. Such a request should be made *in writing* using one of MDAO’s forms, and should be accompanied by all relevant police reports and other documents.

The request must be made to an Assistant District Attorney. While an ADA can ask a paralegal or administrative assistant to type, fax and file the subpoena, the responsibility to review the legal merits of a law enforcement request, and the authority of an ADA to *issue* an administrative subpoena *cannot* be delegated, even to a highly experienced paralegal, administrative assistant or investigator. See Feodoroff, *supra* at 728 (“We think it would defeat the legislative limitation that the tool be used on demand of the Attorney General or a district attorney if that limitation were read as permitting police officers or staff investigators to make a demand under G.L. c.271, § 17B, on behalf of the Attorney General or a district attorney.”)

In practice, this rule requires not only that each and every subpoena be specifically authorized by an ADA prior to issue, but also that the ADA be personally in possession of sufficient information about the case to make an informed assessment of whether the requisite legal standard has been met. Defendants in cases have a right to file motions to suppress in cases involving administrative subpoenas, and the issuing ADAs can be called to testify about the basis for their decision to issue compulsory process. We cannot expect to benefit from the “knowledge of one is the knowledge of all” doctrine enjoyed by police officers in a street-level Probable Cause analysis; the law requires the ADA in these situations to act in a quasi-judicial gatekeeper capacity, and the failure to do so can be fatal to the legality of the subpoena.

While the statute allows any ADA, including one assigned to the District Court, to issue such a subpoena, it is the policy of the Middlesex District Attorney’s Office, except in emergency circumstances, to funnel all requests for Administrative Subpoenas through the SIU and Cyber Protection Units. In general, requests for administrative subpoenas relating to telephone providers should be submitted to the Chief of the SIU Unit; requests for administrative subpoenas relating to Internet Service Providers and web-based businesses should be directed to the Chief of the Cyber Protection Unit. This practice will allow us to maintain consistency in our application of the statute, simplify our record-keeping responsibilities, and maintain consistent points of contact between MDAO and service providers.

**EMERGENCY CIRCUMSTANCES**

In some cases, the Chiefs of SIU and Cyber will not be available. In such a case, any ADA is legally capable of authorizing the subpoena on an expedited basis, so long as the statutory requirements described in this memo are otherwise met. In such circumstances, after the ADA has authorized the terms of administrative subpoena, the SIU and Cyber paralegals should be contacted to draft and serve the subpoenas upon the appropriate parties, and efforts should be made as soon as possible to document the basis for the emergency issuance and to notify the Chiefs of SIU and Cyber so that they can integrate the emergency request into their record-keeping protocol.

**WHAT RECORDS SHOULD BE KEPT WHEN A SUBPOENA IS ISSUED?**

In each case involving a request for an administrative subpoena, a file should be kept containing the basis for the request, including supporting documents such as police reports and emails. These documents can then be used to refresh the recollection of the issuing ADA or as evidence, if necessary, in a suppression hearing. MDAO has created request forms for police agencies to fill out when requesting that MDAO issue an administrative subpoena. Each time that a police request is evaluated, the reviewing ADA should indicate whether the request has been approved, note the crime or crimes that are implicated, and sign and date the approval. A copy of this signed form should be kept in the file, along with the records (whether in paper or electronic form) which are received in response to the subpoena. If the reviewing ADA needs to authorize the subpoena remotely, the paralegal should print and file the authorizing email, or make a contemporaneous note of the date and time that the ADA authorized issuance. This file will be kept by the Cyber paralegal; if you authorize a subpoena on emergency grounds, send all documentation to the Cyber paralegal, nor.admin.cyber@state.ma.us .

**WHAT SHOULD WE DO WITH THE RECORDS WE RECEIVE?**

When records are received from a service provider, a copy should be sent to the requesting police officer and any ADA assisting in the investigation (if one has been assigned). Because administrative subpoena records are part of mandatory discovery, it is critical that prosecutors receive and transmit all records obtained from providers through the administrative subpoena process.

**WHAT DOES AN ADA HAVE TO KNOW BEFORE ISSUING AN ADMINISTRATIVE SUBPOENA?**

An ADA does not need probable cause in order to issue an administrative subpoena. However, under the terms of the statue, he or she does need “reasonable grounds to believe records are relevant and material to an ongoing criminal investigation.” This requirement can be broken into several parts.

**“REASONABLE GROUNDS TO BELIEVE”**

“Reasonable grounds to believe” is not “proof beyond a reasonable doubt,” not “clear and convincing evidence,” not “preponderance,” or even “probable cause” - but more than mere guesswork.

For example, in Feodoroff, *supra*, police surveillance of the residence of a suspected drug dealer led them to conclude that he was using a particular telephone to facilitate his drug business. On this basis, the court held that the District Attorney was justified in issuing an administrative subpoena for telephone records, an act that produced records later used in support of a successful wiretap application. Where the ADA has no reasonable grounds to believe the target is using a telephone (or ISP, etc.) for an unlawful purpose, the defendant will be entitled to suppression of the results of the administrative subpoena, and presumably of any fruits that flow from the subpoena. See Vinnie, *supra* at 178.

To determine whether reasonable grounds exist to issue a subpoena, a prosecutor must first be able to make a determination that it is likely that a crime took place. Administrative subpoenas cannot be issued in non-criminal investigations (such as administrative investigations involving officer misconduct). As a rule of thumb, a prosecutor should be able to identify a particular Massachusetts statute that appears to have been violated before issuing an administrative subpoena.

Where the activity in question is plainly non-criminal, no administrative subpoena should be issued. For instance, where an anonymous email is rude, but non-threatening, and thus protected by the First Amendment, see O’Brien v. Borowski, 461 Mass. 415 (2012) (because of First Amendment constraints, Criminal Harassment statute reaches just two forms of purse speech, “fighting words” and “true threats”), it would not be reasonable to use an administrative subpoena to “unmask” the anonymous e-mailer, because there would be no “reasonable grounds to believe” that the identity is relevant to a “criminal investigation.” It is important to remember that a great deal of cruel and uncouth behavior, which is defined by state law as “Cyber Bullying,” see G.L. c. 71, § 37O, is insulated from criminal prosecution by the First Amendment.

**“RELEVANT AND MATERIAL”**

The “relevant and material” standard, the same standard used by 18 U.S.C. 2703(d), requires a nexus between the subject of the subpoena and the advancement of the criminal case.

To satisfy the “relevant and material” requirement, the prosecuting authority must be able to articulate how the records would be expected to help to advance the cause of the investigation – to provide some evidence of a given party’s guilt (or innocence, if it can help to eliminate a potential suspect). For instance, the IP address connected with a threatening email could be expected to aid in identifying the identity and location of the perpetrator; or the telephone records of a suspected drug dealer could be expected to help to identify his customers or suppliers.

**“ONGOING” CRIMINAL INVESTIGATION**

The authorizing statute specifically requires that the criminal investigation be “ongoing.” It would be contrary to the canons of statutory interpretation, see Halebian v. Berv, 457 Mass. 620, 628 (2010) (“We give effect to each word and phrase in a statute, and seek to avoid an interpretation that treats some words as meaningless”) to reason that an investigation is necessarily “ongoing” simply because the Commonwealth continues to seek records; this would tend to make the “ongoing” provision meaningless.

Thus, it is the view of the Middlesex District Attorney’s Office that for a “criminal investigation” to be “ongoing” requires that the case not yet be pending in court, or that the target be a fugitive, or that the investigation is continuing in uncharged aspects. For example, if an individual has been charged with Receiving Stolen Property that was taken in a housebreak, but the police are continuing to investigate whether the suspect was also involved in the break-in itself, it would still be appropriate to issue a subpoena that related to the break-in.

If a case has already been charged, the defendant has been apprehended, and there is no uncharged crime that remains under investigation, recourse for further investigation must be to a search warrant, or a subpoena pursuant to Rule 17.

**FUGITIVES AND RUNAWAYS**

In some situations, police agencies will ask for an administrative subpoena to assist in the location of a missing person. This may be appropriate under some circumstances, where the missing person is a) suspected to have been the victim of foul play; b) is a fugitive in active warrant status or c) is a runaway.

Because it is a crime for an adult to harbor a juvenile runaway, see G.L. c.119, § 63A,[[1]](#footnote-1) it may be appropriate to issue an administrative subpoena for IP records, for instance, if they would tend to show that the runaway was accessing Facebook from the home of an adult boyfriend.

Likewise, because the location of a criminal suspect is a necessary aspect of a criminal investigation, a subpoena for information tending to reveal that party’s whereabouts may be appropriate. C.f. G.L. c.276 § 1, authorizing issuance of search warrant for
“the body of a living person for whom a current arrest warrant is outstanding.”

**WHAT INFORMATION CAN WE OBTAIN WITH AN ADMINISTRATIVE SUBPOENA?**

“Subscriber information” is defined by 18 U.S.C. § 2703(c)(1)(C) as “the name; address; local and long distance telephone connection records [ANI or RADIUS logs], or records of session times and durations; length of service (including start date) and types of service utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number)” of a subscriber.

In many cases involving pre-paid cellular phones or free email services, the provider will conduct no independent verification of the subscriber information provided by a customer; thus, a purchaser of a telephone may call himself “Mickey Mouse,” or a user of an email account may list his account in the name of his ex-wife in an effort to conceal his true identity.

In these situations, it will often be necessary to search for an alternate means of identifying the user of the account, such as an analysis of the toll history, or the Internet Protocol log-in history.

**IP LOG-IN INFORMATION**

Every device that accesses the Internet must do so using a unique identifying number, called an IP Address. A typical IP address looks like this: 216.27.61.137

Some IP Addresses are static and some are dynamic. Both will change, but dynamic changes much more frequently. For example,Verizon Wireless phones use *dynamic* IP addresses for their wireless services. This means that the IP address changes often. Verizon Online, provides home internet services and those IP addresses are *static*.

Social media services like Facebook, or email providers like Gmail, will keep an IP log for each of their account holders. An IP log is a list of the IP address, the date and the time of the user logging into an email account, Facebook account, Ebay/Paypal account etc.

****

Once a list of IP addresses is obtained, follow-up subpoenas can be issued to the Internet Service Provider associated with a given IP address.

This can then reveal other information that can identify the user, such as: subscriber name, address, telephone, associated email addresses and their method of payment (i.e. credit card on file).

**PROHIBITION ON OBTAINING CONTENT**

Obtaining content is specifically prohibited by the authorizing statute, G.L. c. 271, § 17B:

No subpoena issued pursuant to this section shall demand records **that disclose the content of electronic communications or subscriber account records disclosing internet locations which have been accessed** including, but not limited to, websites, chat channels and newsgroups, but excluding servers used to initially access the internet. No recipient of a subpoena issued pursuant to this section shall provide any such content or records accessed, in response to such subpoena.

Content, for these purposes, would include the text of email communications or a Craigslist posting, or photographic images sent from one party to another, or a list of the web-addresses visited by a particular individual. In order to obtain content, resort must be made to a search warrant.

At times, providers will send content that we have not requested under the terms of our administrative subpoena. In such a case, the ADA receiving the erroneously delivered content should immediately cease review of such records upon recognizing them as inappropriately obtained, should seal them in an envelope, and make note of the date and time at which they were received. ADAs should not disseminate such content to police agencies, as this will create a risk that information derived from the erroneously delivered content will be deemed fruit of the poisonous tree and thus subject to suppression. However, ADAs should be free to make use of, and disseminate, non-content material that was obtained lawfully, as long as it has been properly segregated from the content material.

**WHICH PROVIDERS ARE ELIGIBLE TO RECEIVE AN ADMINISTRATIVE SUBPOENA?**

Not all businesses are eligible recipients of administrative subpoenas – only businesses that fall into one of three specific categories. The language here is complicated and makes reference to several other statutes. However, providers of telephone service, email or text service, or Internet communication services should all be susceptible to the administrative subpoena. If you have questions about whether a given provider is an eligible recipient of an administrative subpoena, please contact the Chief of the SIU or Cyber Protection Unit.

**CAN AN ADMINISTRATIVE SUBPOENA BE SERVED OUT OF STATE?**

Yes. G.L. c.276, § 1B,[[2]](#footnote-2) specifically gives the Commonwealth authority to serve search warrants and administrative subpoenas on so-called “foreign corporations.”

**WILL THE TARGET/ACCOUNT HOLDER BE NOTIFIED OF AN ADMINISTRATIVE SUBPOENA?**

It depends on the policy of the provider. If there is a concern that notice to the subscriber will interfere with the investigation, an administrative subpoena should not be sent; instead, an order of non-disclosure can be obtained to accompany a search warrant or grand jury subpoena, as appropriate to the investigation.

1. G.L. c.119, Section 63A. Whoever is 19 years of age or older and: (i) knowingly and willfully aids or abets a child under the age of 17, or under the age of 18 and in state custody, to violate an order of a juvenile court; or (ii) knowingly and willfully conceals or harbors a child who has taken flight from the custody of the court, a parent, a legal guardian, the department of children and families or the department of youth services shall be punished by a fine of not more than $500 or by imprisonment in the house of correction for not more than 1 year, or by both such fine and imprisonment. [↑](#footnote-ref-1)
2. G.L. c.276, § 1B defines “Foreign corporation” as follows: “any corporation or other entity that makes a contract or engages in a terms of service agreement with a resident of the commonwealth to be performed in whole or in part by either party in the commonwealth. The making of the contract or terms of service agreement shall be considered to be the agreement of the foreign corporation that a search warrant or subpoena which has been properly served on it has the same legal force and effect as if served personally within the commonwealth.” [↑](#footnote-ref-2)