It is also worth noting that the requirements of ECPA typically do not apply to a private business that provides for the storage of email sent by a subject over the business network. Thus, an Assistant may subpoena all electronic records from businesses not offering Internet service to the general public, except for the contents of unopened email less than 180 days old (which must still be obtained by a search warrant as described below). In addition, if the investigation has become overt, such as after the arrest of the defendant, an Assistant may again subpoena all electronic records from an ISP, except for the contents of unopened email less than 180 days old (which must still be obtained by a search warrant as described below).

3. Court Orders (2703(d) Orders)

In addition to the limited class of information obtainable by subpoena, ECPA also provides for law enforcement to compel greater disclosure of electronic data from an ISP by court order, pursuant to 18 U.S.C. § 2703(d). A § 2703(d) order compels the ISP to provide all information obtainable by subpoena, all other records relating to a subscriber other than the contents of communications (§ 2703(c)), and, with delayed notice, the contents of opened email or unopened email older than 180 days. As a practical matter, a 2703(d) order permits the Government to compel the disclosure of all subscriber information, all transactional logs, the "to" and "from" of all email communications (a historical pen/trap and trace), buddy lists or other special services maintained on the ISP's computers, as well as opened electronic communications or extremely old unopened email.

Non-resp

Addendum to Attachment B

This warrant does not authorize the "seizure" of computers and related media within the meaning of Rule 41(c) of the Federal Rules of Criminal Procedure. Rather this warrant authorizes the removal of computers and related media so that they may be searched in a secure environment. The search shall be conducted pursuant to the following protocol:

With respect to the search of any computers or electronic storage devices seized from the residence in Attachment A hereto, the search procedure of electronic data contained in any such computer may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will be not returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth herein;

d. opening or reading portions of files in order to determine whether their contents fall within the items to be seized as set forth herein;

e. scanning storage areas to discover data falling within the list of items to be seized as set forth herein, to possibly recover any such recently deleted data, and to search for an recover deliberately hidden files falling within the list of items to be seized; and/or

f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B.

The government will return any computers or electronic storage devices seized from the residence described in Attachment B hereto within 30 days of the seizure thereof, unless contraband is found on the seized computer and/or electronic storage device.

ADDENDUM TO ATTACHMENT B

With respect to the search of any information and records stored within hand-held wireless communication devices, including cellular telephones, and any related memory cards or removable storage media, law enforcement personnel will locate the information to be seized according to the following protocol:

The search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. searching for and attempting to recover any hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein;

b. surveying various file directories, electronic mail, text messages, contact lists, address books, call logs, calendars, notes, appointments, task lists, voice mail, audio files, video files, or pictures, including attachments thereto, to determine whether they include data falling within the list of items to be seized as set forth herein;

c. opening or reading portions of electronic mail or text messages, and attachments thereto, in order to determine whether their contents fall within the items to be seized as set forth herein; and/or

d. performing key word searches through all electronic mail or text messages, and attachments thereto, to determine whether occurrences of language contained in such electronic mail or text messages, and attachments thereto, exist that are likely to appear in the information to be seized described in Attachment B.

Law enforcement personnel are not authorized to conduct additional searches on any information beyond the scope of the items to be seized by this warrant.

There is a cell phone search warrant protocol addendum contained on C_Network[Non-Resp

]It is mandatory that we use this addendum for all warrants where we are seeking to seize and search cell phones. This covers the search of all matter contained in the cell phone's memory and does not cover, for example, matter in which a phone links to the internet (i.e. stored e-mails accessible through a Treo) for which we would need a search warrant to the ISP. Additionally, to recover matter maintained by the carrier not contained within the physical phone (i.e. voice mails stored on the carrier) we would need to get a search warrant for the cell phone carrier[(

Non-Resp

Reminder: if you have already indicted a case and are seeking a search warrant to obtain evidence to support the charges in that case, you must submit the application for the search warrant to the triall judge for the indicted case. The trial judge can then decide to review the application himself or herself to delegate that task to the designated Magistrate Judge for the indicted case or to the duty Magistrate Judge.

b5

Type of Request	Statutory Authority	Type of Legal Process/Standard	Return and Notice Required?	Comments
Stored text messages held by service provider	Fed. R. Crim P.41	- probable cause to believe an offense(s) has been/is being committed - probable cause to believe that the text messages will constitute evidence concerning the offenses under investigation ****NOTE: Almost none of the major service providers retain text messages. *See* /narcotics/electronic surveillance Non T3/Stored Text Messages**	Return: Yes Notice: No	1. Where to file. Magistrate Judge 2 Use Rule 41. Use a search warrant under Rule 41 and 18 U.S.C. §2703(a) and (b)(1)(A) 3. Jurisdiction: Rule 41 warrant may be issued by any court having jurisdiction over the offense under investigation. 18 U.S.C. §2703(b)(1)(A). 4 No notice to subscriber required. 18 U.S.C. § 2703(b)(1)(A) provides no notice to the subscriber or customer is required when you obtain a search warrant. 5 Observe search warrant protocol: 6 Preservation Letter: If you intend to obtain the evidence via a search warrant, direct a letter to the service provider pursuant to 18 U.S.C. §2703(f)(1) and (2) requiring them to preserve stored text massages pending the issuance of a court order. The stored text messages must then be retained for a period of 90 days. The retention period shall be extended for an additional period of 90 days upon a renewed request by the government. 7. Return: Yes. Fed.R.41(f)(1)(D)
Stored Voicemails held by service provider	Fed. R. Crim P.41	- probable cause to believe an offense(s) has been/is being committed - probable cause to believe that the voicemails will constitute evidence concerning the offenses under investigation	Return: Yes Notice: No	1. Where to file. Magistrate Judge 2. Use Rule 41. Use a search warrant under Rule 41 and 18 U.S.C. §2703(a) and (b)(1)(A) 3. Jurisdiction: Rule 41 warrant may be issued by any court having jurisdiction over the offense under investigation. 18 U.S.C. §2703(b)(1)(A). 4. No notice to subscriber required. 18 U.S.C. § 2703(b)(1)(A) provides no notice to the subscriber or customer is required when you obtain a search warrant. 5. Observe mandatory search warrant protocol: 6. Preservation Letter: Service providers retain voicemails on their networks only for very limited periods of time. If you intend to obtain the evidence via a search warrant, direct a letter to the service provider pursuant to 18 U.S.C. §2703(f)(1) and (2) requiring them to preserve stored voicemails pending the issuance of a court order. The stored voicemails must then be retained for a period of 90 days. The retention period shall be extended for an additional period of 90 days upon a renewed request by the government. 7. Return: Yes. Fed.R.41(f)(1)(D)

Type of Request	Statutory Authority	Type of Legal Process/Standard	Return and Notice Required?	Comments
Stored Emails Held by an Internet Service Provider	Fed. R. Crim. P. 41	- probable cause to believe an offense(s) has been/is being committed - probable cause to believe that evidence of the offense(s) under investigation will be found on the computer systems of the ISP, within the email accounts particularly identified	Return: Yes Notice: No	1. Where to file. Magistrate Judge 2. Use Rule 41. Certain provisions of 18 U.S.C. § 2703(b) authorize the government to obtain the content of certain stored emails (older that 180 days) from an internet service provider without a warrant on a showing of less than probable cause.. The Sixth Circuit in *Warshak* held that the non-warrant methods of obtaining stored emails to be unconstitutional. 3. Jurisdiction: Rule 41 warrant may be issued by any court having jurisdiction over the offense under investigation. 18 U.S.C. §2703(b)(1)(A). 4. Observe mandatory search warrant protocol: 5. No notice to subscriber required. While Rule 41 generally requires notice, 18 U.S.C. § 2703(b)(1)(A) provides no notice to the subscriber or customer is required when you obtain a search warrant. 6. 7. Preservation Letter: Service providers retain emails on their networks only for very limited periods of time. If you intend to obtain the evidence via a search warrant, direct a letter to the service provider pursuant to 18 U.S.C. §2703(f)(1) and (2) requiring them to preserve stored emails pending the issuance of a court order. The stored emails must then be retained for a period of 90 days. The retention period shall be extended for an additional period of 90 days upon a renewed request by the government. 8. Return: Yes. Fed.R.41(f)(1)(D) 9. Facebook/Twitter: see pages 30-31 below

Type of Request	Statutory Authority	Type of Legal Process/Standard	Return and Notice Required?	Comments
Real-time Interception of Wire, Oral,(i.e. "Bugs" of rooms, cars, etc.) Electronic Communications (*e.g.* email, computer transmissions, text messages, faxes, digital pagers)	18 U.S.C. § 2510-18	- probable cause plus necessity: (*see* 18 U.S.C. § 2518) - Office of Enforcement Operations ("OEO") review and approval - Assistant AG or Deputy Assistant AG approval: for wire and oral intercepts only 18 U.S.C. §§2516(1), 2510(9)	Return: No Service of Inventory: Yes:	1 Where to file. Personal appearance before chief judge or acting chief judge required for both AUSA and agent, both of whom must swear to application (AUSA) and affidavit (agent) in judge's presence. 2 Jurisdiction: For phones T3 may be signed by a judge sitting in (a) the district where the communication will be "intercepted" (*i.e.* listened to for the first time in the wire room); or (b) the district where the tapped telephone is located. Furthermore, in *U.S. v. Ramirez*, 112 F.3d 849(7th Cir. 1997), the court held pursuant to 18 U.S.C. §2518(3), the district court can authorize a wiretap after a cellular telephone regardless of the location of the cell phone or the listening post. For interceptions of oral communications, T3 order must be signed by a judge sitting in the district where the oral conversations are first listened to by the agents. 3 Duration: 30 days measure from the date on which agents begin conduct the interception (i.e. date the switch is flipped) or 10 days after the order is signed, whichever comes earliest. Extension orders are good for 30 days measured from the date the extension order is signed. 4 Minimization: Yes - for wire and oral intercepts (real time); after-the-fact minimization is permitted if (i) foreign language interpreter is not reasonably available during the interception period; and (ii) for interception of electronic communications. 5 Sealing. The recordings containing the intercepted communications must be sealed before the Chief Judge immediately upon the expiration of the authorized interception period. Prior to sealing, confirm with agent that all intercepted communications, including push-to-talk communications, are contained on the disc to be sealed. 6 Inventory: Service of the inventory (i.e. the fact that person was intercepted on a wire - but not the contents of the intercepted calls) pursuant to 18 USC § 2518(8)(d) is ordinarily required within 90 days from the expiration of the T3 orders or extensions thereof. However, this statute provides that upon an *ex parte* showing of good cause the service of the inventory may be postponed. See ¶ 12 7 Packaging pen register/ trap-and trace and cellular location requests with T3s: All independent requirements for pen register, trap and trace, cell site, lat/long or digital analyzer authority must be met even if packaged with a T3. 8 Return. If the T3 order also included authority for prospective cell-site, lat-long/GPS/or digital analyzer data, at time of sealing T3, agent and AUSA should appear to file returns (if any) for (i) cell site and (Iii) more precise lat-long/GPS/enhanced 911/digital analyzer data with chief judge. This should be done at the same time the T3 recordings are sealed. You must do those returns even if extending wiretap authorization. The return should be a separate document - not part of the sealing application or sealing order. 9 Delayed Notification. Sealing of T3 pleadings and delay in service of T3 inventory does not excuse compliance with independent delay procedures for all other relief sought, including for cellular telephone location information. 10. Sealing of T3 applications and orders: Required under 18 U.S.C. §2518(8)(b)

Type of Request	Statutory Authority	Type of Legal Process/Standard	Return and Notice Required?	Comments
BOP (including MCC) inmate recordings	BOP Program statement 1351.05	Administrative, GJ, or trial subpoena	N/A	1. To obtain the actual recorded contents of telephone conversations, law enforcement agents must use an administrative, grand jury, or trial subpoena). Law enforcement agencies may also request such information in an "emergency situation." Finally, contents of prisoner phone calls to their attorneys may not be obtained. 2. Please note that when you request recordings of prisoner phone calls from the MCC, you should always request that the MCC **not** include copies of any phone calls with attorneys. Some prisoners use the regular phones—as opposed to phones the MCC sets aside for attorney calls—to call their attorneys. They do this despite the fact that they are notified that all such calls are recorded. If we do not ask the MCC to exclude attorney calls, they will include them int eh recordings they provide. 3. Direct the subpoena to the attention of Metropolitan Correctional Center,. Non-exempt.
BOP Prisoner E-mail Accounts	BOP Program statement P5265.13	Voluntary request	N/A	1. BOP's prisoner e-mail program (called the TRULINCS System) allows disclosure of transactional data and message content for law enforcement purposes. . Subpoenas for these are not required, as compared to recorded telephone conversations. Upon receipt of a properly submitted written request from a law enforcement agency, BOP staff are authorized to release both transactional data (e.g., date, tie, electronic message address, electronic message recipient and sender, and length of the message) and copies of the electronic messages. 2. 3. Non-exempt 4. MCC does **not** filter out the attorney emails before sending them over to us. Thus you will need to set set up screen or filter team at our office before you review the emails. Non-exempt

Type of Request	Statutory Authority	Type of Legal Process/Standard	Return and Notice Required?	Comments
Data residing within seized cell phones (e.g. contacts list, telephone numbers of incoming and outgoing calls, photographs, video images		- Consent - Search incident to arrest - Rule 41	For search warrants: Returns: Yes Notice: Yes	1. If the cell phone is seized incident to arrest, the contents of the phone can be searched without a warrant under the search incident to arrest doctrine. Search incident to arrest authority covers the search of all matter contained i the cell phone's memory - call logs, address book, stored text messages, stored emails, stored pictures, and stored video. It does **NOT** however cover matter which in order to access the phone must be launched to the Internet (i.e., email messages not stored on the actual phone but rather only accessible through the service provider). Absent search incident to arrest authority or consent, , a search warrant (see pages 15-16 above) is required to search the contents of a cell phone. 2. Observe search warrant protocol 3. If you are applying for a warrant to search for evidence relating to an already-indicted case. The application should be presented first to the assigned district court judge and we should explain that the application relates to the indicted case. It is up to the district court judge to decide whether he or she will handle the matter or have the Magistrate Judge handle it. If the evidence likely to be obtained from the warrant could also implicate uncharged persons that would also be a factor. 4. Voice mail is stored on the service provider's network so a search warrant to the service provider would be required to obtain that evidence. 5. Some Magistrate Judges require a particularized probable cause to search the different features of the cell phone (contact list/in and out telephone numbers/photos, video images) 6. Remember that under *U.S. v. Burrgard,* we must obtain search warrants as quickly as feasible for cell phones. computers and other containers seized during the investigation to avoid suppression.

Type of Request	Statutory Authority	Type of Legal Process/Standard	Return and Notice Required?	Comments
			N/A	
Facebook			N/A	• You can use an administrative, GJ, or trial subpoena or a 18 U.S.C. § 2703(d) order (with non-disclosure language) to obtain subscriber records and IP addresses. • A search warrant is needed to obtain stored communications. See 18 U.S.C. 2703(b) - see page 18 above

Type of Request	Statutory Authority	Type of Legal Process/Standard	Return and Notice Required?	Comments
Twitter				Non-Person • You can use an 18 U.S.C. § 2703(d) order (with non-disclosure language) to obtain subscriber records and IP addresses. • The contents of public tweets can be captured off the web • A search warrant would be needed to obtain private tweets stored on the provider's network. See 18 U.S.C. 2703(b) - see page 18 above

Non-Recip

From: [redacted](USAILN)
Sent: Monday, March 23, 2009 1:48 PM
Subject: Email Search Warrants

A standard search protocol has been agreed to by all the magistrates which we will use for all email search warrants.
The search protocol is to be included as an addendum to the attachment A of the warrant.
Attachment A sets out the process by which an ISP provides law enforcement with the entire contents of an email account and further sets out the specific items from that account to be seized by law enforcement.
The search protocol provides a non-exclusive list of searching techniques that agents may use. The protocol also provides an admonition that the searching agents are to confine their search to those items that they have been authorized to search for under the warrant.
Copies of a sample affidavit, a sample Attachment A, and a sample Addendum to Attachment A are provided with this email. Copies will also be posted to CRIMBANK and will be made available through HOTDOCs in the near future.
All email search warrants, as with all warrants, should be reviewed by deputies, but no further review or approvals will be necessary.
Please make sure that your agents are aware of the protocol when you discuss the execution process of the warrant with them.
If you have any questions, feel free to give me a call. [redacted]

ATTACHMENT A TO SEARCH WARRANT

I. Search Procedure

a. The search warrant will be presented to [illegible] personnel, which will be directed to isolate those accounts and files described in Section II below;

b. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein;

c. Company employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant; and

d. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review all information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. Files and Accounts to be Copied by [illegible] Employees

a. All electronic mail, including attachments thereto, stored and presently contained in, or on behalf of, the following electronic mail addresses and/or individual accounts:

[EMAIL ADDRESS] from the opening of the account to the present

b. All existing printouts from original storage of all the electronic mail described above in Section II(a);

c. All transactional information of all activity of the electronic mail addresses and/or individual accounts described in Section II(a), including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations;

d. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above in Section II(a), including applications, subscribers' full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, and detailed billing records; and

e. All records indicating the services available to subscribers of the electronic mail addresses and/or individual accounts described above in Section II(a).

III. Information to be Seized by Law Enforcement Personnel

a. **DESCRIBE THE PARTICULAR EVIDENCE THAT YOU HAVE PROBABLE CAUSE TO SEIZE**– Specify the particular content that you are searching for, i.e. communications involving the formation of a particular contract, financing of that contract, etc., just like you would for a regular search warrant. Do not just request all emails or all emails that pertain to violations of particular criminal code provisions.

b. All of the records and information described in Section II(c), (d), and (e).

From: [redacted] (USANYE)
Sent: Wednesday, June 27, 2012 5:57 PM
To: USANYE-All_Criminal_AUSAs
Subject: Search warrant templates
Attachments: smart phone sw template 11.25.2011.wpd; computer and smartphone warrant template.pdf; computer sw template 2.2012.wpd; email sw affidavit template 1.19.2012.wpd; email warrant template.pdf;

[redacted]

Make sure to use the D drive forms as your templates when drafting warrants. Do not use old (or even relatively recent) go-bys from your own files or from colleagues. There has been significant litigation in this district about what these warrants should say, and we update the forms frequently. If you use a go-by from a colleague or from your own files, it may not reflect the newest approved language and could create unnecessary litigation risks.

CDT

New Procedures

Filter Teams

- Filter Agent - not associated with investigative team - will review digital evidence
- Filter Agent will share only evidence listed in SW (i.e., "responsive" evidence) with investigative team
- If Filter Agent observes other evidence of criminal conduct not listed in SW, that information will be brought to Filter AUSA – also not associated with investigative team – to determine if follow-on SW can be obtained

Risk to Digital Evidence of Deletion/Corruption/Booby-Traps

- Description of risks to integrity of digital evidence must be directed to the actual risk in that particular case
- SWA language re: concealment, encryption, deletion, etc. must recite facts indicating whether such are reasonable possibilities
- Agent's estimation of risk
- "Unknown" risk might be common

Prior Efforts to Seize Info

- Prior efforts to seize same/related info in "other judicial fora" must be disclosed in SWA
- Prior SWs, GJSs, and other subpoenas
- Not 2703(d) orders ... yet
- Must disclose results as well

Automated Hash Tools

- Used to quickly search drives for known Child Pornography images, Hacking tools/scripts, etc.
- SW must state intent to use such tools
- SWA must contain PC to support seizure of items (i.e., CP images) at which hashing tools are directed

Return/Destruction of "Non-Responsive" Data

- If no responsive data on digital device, must be returned or image destroyed
- If mixed responsive and non-responsive data, responsive data communicated by Filter Agent to investigative team, and digital device/image sealed and secured by:
  - Filter Team (if instrumentality)
  - Placing under seal with Court

Returns/Certifications

- Two separate returns will be filed
- First: by investigating agents, listing items seized from search location
- Second: by filter agents, recounting the results of the search of digital data and including lists of digital devices and forensic copies retained by the filter team as well as lists of the digital data found to fall within the scope of the warrant and, as a result, disclosed to the investigating agents
- The second return will be in the form of a sworn declaration by the filter agent