INFO SOUGHT	DEVICE	PAPER NEEDED	STATUTE	AUTHORIZING OFFICIAL(s)	DURATION	STANDARD OF REVIEW
Phone Number Dialed- Real Time (outgoing)	Pen Register	Court Order	18 USC 3122, 3123	Magistrate	60 days	Relevance
Phone Number Dialed- Real Time (incoming)	Trap & Trace/ Caller ID	Court Order	18 USC 3122, 3123	Magistrate	60 days	Relevance
Incoming And Outgoing Phone Numbers Dialed And Subscriber Info- In Storage	Toll Records	Subpoena (grand jury or trial) Admin Subpoena Court Order	18 USC 2703(c)	Grand Jury/ Agency/ Magistrate		Specific And Articulable Facts (Relevant and material to an ongoing investigation) (Only if court order needed)
Cell Locating Information (tracking cell phones)	Pen Register/ Smart System	Court Order	18 U.S.C. 2703(d)	Magistrate	60 Days	Specific And Articulable Facts
Oral Communications	Bug	Title III	18 USC 2518	Dist Ct Judge and DOJ - DAAG/ OEO	30 Days (from 1st interception, or 10 days from signing)	Probable Cause+
Faxed Documents (real time)	Fax Machine (electronic communications)	Title III	18 U.S.C. 2518	Dist Ct Judge and DOJ- DAAG/OEO	30 Days	Probable Cause+
Computer Files/ Stored Or Down-Loaded/ Downloaded Emails	Computer Stand-Alone	Search Warrant	Rule 41 FRCP	Magistrate		Probable Cause
Computer Messages Sent Via E-Mail (Real Time Interception- Content)	Computer Network Intercept Device	Title III (if real-time interception)	18 USC 2518	Dist Ct Judge/ and DOJ- DAAG/OEO	30 days	Probable Cause+
Unopened Email (in storage- 180 days or less)	Internet Service Provider	Search Warrant	18 U.S.C. 2703(a)	Magistrate		Probable Cause
Unopened Email (in storage more than 180 days)	Internet Service Provider	Subpoena Court Order Warrant	18 U.S.C. 2703(a),(b)	Magistrate (if court order or warrant)		Specific And Articulable Facts (order) or Probable Cause (warrant)
Opened Email (still on service provider's system)	Internet Service Provider	Subpoena Court Order Warrant	18 U.S.C. 2703(b)	Magistrate (if court order or warrant)		Specific And Articulable Facts (order) or Probable Cause (warrant)
Email Subscriber Information/Transactional Information	Internet Service Provider	Court Order	18 U.S.C. 2703(c)	Magistrate		Specific And Articulable Facts
Wire Communications Over Fraudulent Phone	Cloned Cellular Phone (wire communications)[FN3]	Title III	18 USC 2518	Dist Ct Judge and DOJ- DAAG/OEO	30 days	Probable Cause+
Use Of Multiple Cellular Or Pay Phones, Calling Cards- changing so often that the phones cannot be identified	Roving	Title III	18 USC 2518(11)(b)	Dct Judge and AAG- Contact OEO	30 days	Probable Cause (must include facts reflecting that facilities changed to thwart interception)
Video (installed by agents in residence/ business)	Video- CCTV (Closed Circuit Television)	Rule 41 Search Warrant + Title III Req'ts	Rule 41 FRCP	Dct Judge and OEO (DOJ policy)	No More Than 30 Days	Probable Cause with Title III req'ts (Duration, Minimization, Necessity, etc.)
Video- camera already on premises	Security Camera- (already in place- need interception equipment to monitor	Title III (electronic communi-cation)	18 USC 2518	Dist Ct Judge and DOJ- DAAG/OEO	30 Days	Probable Cause+
Video (outside premises- public area)	Pole Camera	No Warrant Needed (unless viewing protected area)[FN4]				
Names And Numbers From Electronic Address Book	Elec. Data note book Palm pilot	Search Warrant	Rule 41 FRCP	Magistrate		Probable Cause
tracking device - (location of target subjects or targeted item)	Transponder, Bumper Beeper, GPS (global positioning system)	Search Warrant[FN5]	18 U.S.C. 3117(a) and Rule 41 FRCP	Magistrate		Probable Cause
Identify Cell Phone By Electronic Serial Number (ESN) Or Phone Number (MIN)	Cell Site Simulator, Digital Analyzer (reads Electronic Serial Number and Phone number)	Court Order (if only ESN/phone number requested and search requires phone company's cooperation[FN6]	18 U.S.C. 2703(d)	Magistrate		Specific And Articulable Facts
Info From Seized Pager	Pager-Seized	Search Warrant (unless incident to arrest- then no paper needed)[FN7]	Rule 41 FRCP	Magistrate		Probable Cause
Realtime Intercept- Messages Sent To Pager (clone)	Pager-Cloned (electronic communication)	Title III	18 USC 2518	Dist Ct Judge; Don't Need DAAG/OEO APPROVAL	30 Days	Probable Cause+

Obtaining Electronic Evidence

The previous chart and the notes below are available in the USABook Online (July 2003) published by the Department of Justice and was compiled by Michael R. Sklaire, Assistant United States Attorney, District of Connecticut.

1. **Information Sought:** Set forth below are general categories of requested information, ranging from the numbers dialed from a subject's phone to the subscriber's name to the actual intercepted conversations. As defined in 18 U.S.C. 2510, a "wire communication" is any communication involving a phone (cordless, residential, business, and including cloned). An "oral communication" is any conversation intercepted through the use of a bug or listening device placed in the room. An "electronic communication" is anything intercepted over a pager, computer, or facsimile machine. **Under federal law, if one party to a wire, oral or electronic communication consents to the recording or monitoring of that communication, then no order, warrant, or Title III is required.** The categories set forth in this chart apply to situations when **no** party consents to the interception of the communication.

2. **Device:** This category provides common terms for interception or access devices. Some agencies may refer to a pen register as a "DNR (Dialed Number Recorder)." A Caller ID device is the same thing as a "trap and trace."[FN1] A "cell site simulator" or "digital analyzer" is a device that captures the electronic serial number and phone number of a cellular phone. A "cloned cellular phone" is a device that is programmed to copy and capture the billing information of another phone so that any calls made by or to the cloned cellular phone are billed to the legitimate subscriber.

3. **Paper Needed:** A general rule is that if your agents want to intercept a conversation or message "real-time," while the communication is occurring, then a Title III warrant is needed. If they desire communications in storage, such as stored pager or computer messages, then a search warrant is needed. If the desired information is toll records or transactional data (subscriber names and addresses), then a subpoena is required. A Title III affidavit must contain much more information than just a showing of probable cause. Also, the probable cause section of a Title III is much more extensive than in an affidavit for a search warrant. Contact OEO for samples. For stored communications and data, be sure to check the case law and contact the Computer Crimes Section at the Department of Justice.

4. **Statute:** Sections 2510-2520 of Title 18 should be referred to when doing real-time interceptions of wire, oral, and electronic communications. Sections 3121-3123 should be referred to when conducting pen registers and trap and trace devices (real-time interception of dialed digits). Sections 2701-2710 should be referred to when dealing with "stored wire or electronic communications," otherwise known as computer files off a network, toll records from the phone company, historical pager communications, etc. Section 2703 sets forth whether you need a search warrant, court order, or subpoena for the stored information. **Please note that the recent Anti-Terrorism legislation (Patriot Act) amended section 2703 to include voice mail in the definition of stored communications, such that a Title III order is not required to obtain voice mail messages in storage.** Finally, Rule 41 of the Federal Rules of Criminal Procedure governs any search warrant.

5. **Authorizing Official(s):** Only district court judges may authorize Title III interceptions (real-time communications). Magistrates may authorize search warrants, pen registers, and court orders for stored communications. In addition, for a Title III, before you get district court authorization, the statute requires that the Assistant Attorney General of the Criminal Division, or one of the Deputy Assistant Attorneys General (DAAG) authorize the interception. That is accomplished by contacting the Electronic Surveillance Branch of the Office of Enforcement Operations (OEO). All Title III paperwork **must** be sent to OEO for approval, with the exception of clone pagers, which can be approved in the respective U.S. Attorney's Offices. In addition, the use of a Closed Circuit Television (CCTV) needs to be approved by OEO before getting a warrant signed.

6. **Duration:** The general rule is that you have thirty days to conduct a Title III and sixty days to conduct a pen register, before you must go back to court (and OEO in the case of Title III) for new authorization. However, if the objectives of the investigation have been met prior to the end of the thirty-day period, then

interception must be terminated. For a Title III, the thirty day interception period begins either when the interception is first conducted pursuant to the court order, or ten days after the judge signs the order, whichever comes first.

7. **Standard of Review:** For pen registers, trap and trace devices, and Caller ID devices, you must show the magistrate simply that the information is "relevant and material to an ongoing criminal investigation." For court-authorized disclosure of phone records, subscriber information, and other "transactional data," as defined in 18 U.S.C. 2703(c), you must show "specific and articulable facts" that reflect why this material is relevant and material. For a Title III search warrant, your affidavit must reflect more than probable cause for a search warrant, "probable cause plus." The probable cause standard for a Title III is higher than for a normal search warrant. In essence, you must show the court that the particular phone (fax, computer, pager ...) is **clearly** being used for illegal purposes. Mere inferences that the phone is being used based on pen registers and toll records will not usually be sufficient. Common ways to achieve "probable cause plus" are through the use of consensual calls made to the target facility, combined with pen register or toll record analysis reflecting that the facility has been and is being used for illegal purposes.

   A Title III order differs from a normal search warrant also in the statutory requirements of necessity and alternative investigative techniques contained in 18 U.S.C. 2518. The government must show the court why normal investigative procedures have not succeeded in obtaining the required evidence concerning criminal activity. Further, in a Title III affidavit, minimization provisions must be set forth.
   In addition, for a "roving" wiretap, where the targets change phones every few days, the court must make a specific finding that the phones are being dropped so often to thwart interception by law enforcement. 18 U.S.C. 2518(11)(b). Note that there is also a provision for "roving" oral interception, whereby it is not possible (or practical) to identify the location of the interception prior to the communication occurring. 18 U.S.C. 2518(11)(a).
   For a closed-circuit television (CCTV), one that is installed surreptitiously by the agents, the standard of review is probable cause, the same as a search warrant. However, many circuits have adopted the standard set forth in the Ninth Circuit in *United States v. Koyomejian*,[FN2] whereby the CCTV search warrant must resemble a Title III warrant in terms of including such Title III requirements as minimization, alternative investigative techniques, and duration. Often, a request for CCTV is filed at the same time as a request for Title III interception of oral communications (bug). Contact OEO for further details.

FN 1. *United States v. Fregoso*, 60 F.3d 1314 (8th Cir. 1995)

FN 2. 970 F.2d 536 (5th Cir. 1992).

FN 3. A Title III is needed even if the phone is fraudulent or stolen , because the "communication" is protected under Title III, regardless of the facility used.

FN 4. Examples of protected areas include the installation of a fence, closed curtains, or closed garage door. When the subjects exhibit an EXPECTATION OF PRIVACY, then a search warrant is required.

FN 5. In those rare instances when you know that the car will remain in public view at all times, then a search warrant is not required. However, a search warrant will be required when the agents are required to either break into facility or attach device to power source of car/boat. *See United States v. Gbemisola*, 225 F.3d 753 (D.C. Cir. 2000).

FN 6. No paper is needed if the agent is using this device to find this information without the phone company's assistance.

FN 7. The case law suggests that if a pager is searched **immediately** following the legitimate arrest, then no warrant is necessary pursuant to an exigent circumstances argument. However, any delay removes the exigency and a search warrant would be required..

FN 8. Patriot Act amended 18 U.S.C. § 2703 to include wire communications in storage: same rules as e-mail.