U.S. DEPARTMENT OF HOMELAND SECURITY

FEDERAL LAW ENFORCEMENT TRAINING CENTER

# OFFICE OF MISSION SUPPORT

# LEGAL DIVISION


Homeland Security

# LESSON PLAN

## ELECTORNIC LAW AND EVIDENCE

**1380** **MAR/11**

**WARNING**

**This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid 'need-to-know' without prior authorization of an authorized Department of Homeland Security Official.**

**FOR OFFICIAL USE ONLY**

Originally developed by:

(b)(6)
Branch Chief
Legal Division

and

(b)(6)
Senior Instructor
Legal Division

Revised November 2006 by:
(b)(6) Senior Instructor, LGD

Revised January 2008 by:
(b)(6) Senior Instructor, LGD

Revised JUN 2009 by:
(b)(6) Senior Instructor, LGD

Revised JUL 2010 by:
(b)(6) Senior Instructor, LGD
(reviewed for correct formatting, eliminated typographical errors, added text and citations to current caselaw)

Revised MAR 2011:
(b)(6) Senior Instructor, LGD
(added DOI_LMITP to syllabus)

## TABLE OF CONTENTS

# SYLLABUS

**COURSE TITLE:** **ELECTRONIC LAW AND EVIDENCE**

**COURSE NUMBER:** **1380**

**COURSE DATE:** **MAR/11**

**LENGTH OF PRESENTATION: SEE BELOW**

| OPTION | LECTURE | LAB | P.E. | TOTAL | PROGRAM |
|---|---|---|---|---|---|
| A | 2:00 | | | 2:00 | MDIP* |
| B | 6:00 | | | 6:00 | NCIS_CTTP |
| C | 2:00 | | | 2:00 | CESP – CETP* |
| D | 6:00 | 2:00 | | 8:00 | CITP, DOI_LMITP |
| E | 4:00 | | | 4:00 | CLETP, DCIS_SARTP ** |
| F | 2:00 | | | 2:00 | FDA-SATP * ** |
| G | 2:00 | | | 2:00 | RUVP* |
| H | 1:00 | | | 1:00 | ICARC* |
| I | 2:00 | | | 2:00 | IPCP* |
| J | 2:00 | | | 2:00 | RECVR |
| K | 2:00 | | | 2:00 | IITP |
| L | 2:00 | | | 2:00 | FRDE |
| M | 2:00 | | | 2:00 | IAITP |
| N | 2:00 | | | 2:00 | DOJOIG_IS |

* Not testable on a LGD exam.

* *The students in these courses are experienced agents. Accordingly, each class should be tailored to the experience level of the students. Additionally, special emphasis should be placed on the changes to electronic surveillance brought about by passage of the U.S.A. Patriot Act.

| **OPTION A: MDIP** |
|---|
| **DESCRIPTION**: This course will examine special considerations law enforcement officers should be aware of when preparing search warrants to search and seize cell phones and methods of executing search warrants. |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a potential investigation , the student will identify special considerations in preparing search warrants to search and seize cell phones using both a warrant and exceptions to the warrant requirement. |

| OPTION B: NCIS_CTTP |
| --- |
| **DESCRIPTION**: This course examines special considerations law enforcement officers should be aware of when preparing search warrants to search and seize computers and methods of executing search warrants. Also discussed are the Constitutional and statutory requirements regarding the interception of wire, oral, and electronic communications; the use of tracking devices; the use of pen registers and trap and trace devices; the use of video-only surveillance in protected areas; and access to stored electronic communications held by network service providers.. |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a potential investigation, the student will identify the requirements to use electronic devices to gather evidence, and the considerations to search and seize evidence stored electronically, both on personal premises and network service providers, in accordance with Federal law and Constitutional standards. |

| OPTION C: CESP/CETP |
| --- |
| **DESCRIPTION**: This course examines the Constitutional and statutory requirements regarding the interception of wire, oral, and electronic communications; the use of tracking devices; the use of pen registers and trap and trace devices; and the use of video-only surveillance in protected areas. |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a potential investigation, the student will identify the federal requirements governing the use of electronic devices that intercept wire, oral, and electronic communications; track the movement of suspects; trace telephone calls and electronic communications,and the requirements governing the use of video-only surveillance in locations where individuals have a reasonable expectation of privacy in accordance with the Best Evidence rule and the rule of authentication. |

| OPTION D: CITP, DOI_LMITP |
| --- |
| **DESCRIPTION**: This course examines special considerations law enforcement officers should be aware of when preparing search warrants to search and seize computers and methods of executing search warrants. Also discussed are the Constitutional and statutory requirements regarding the interception of wire, oral, and electronic communications; the use of tracking devices; the use of pen registers and trap and trace devices; the use of video-only surveillance in protected areas; and access to stored electronic communications held by network service providers. |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a potential investigation, the student will identify the requirements to use electronic devices to gather evidence, and the considerations to search and seize evidence stored electronically, both on personal premises and network service providers, in accordance with Federal law and Constitutional standards. |

| OPTION E: CLETP, DCIS_SARTP |
| --- |
| **DESCRIPTION**: This course examines special considerations law enforcement officers should be aware of when preparing search warrants to search and seize computers and methods of executing search warrants. Also discussed are the Constitutional and statutory requirements regarding the interception of wire, oral, and electronic communications; the use of tracking devices; the use of pen registers and trap and trace devices, and the effects of the USA Patriot Act on electronic surveillance. |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a potential investigation, the student will identify the federal requirements governing the use of electronic devices that intercept wire, oral, and electronic communications; track the movement of suspects; and the ability to obtain stored electronic communications in accordance with Federal law and Constitutional standards. |
| **OPTION F: FDA-SATP** |
| **DESCRIPTION**: This course examines the Constitutional and statutory requirements regarding the interception of wire, oral, and electronic communications; the use of tracking devices; access to stored electronic communications, and the effects of the USA Patriot Act on electronic surveillance. |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a potential investigation, the student will identify the federal requirements governing the use of electronic devices that intercept wire, oral, and electronic communications; track the movement of suspects; and the ability to obtain stored electronic communications in accordance with Federal law and Constitutional standards. |

| OPTION G: RUVP |
| --- |
| **DESCRIPTION**: The RUVP is intended for Law Enforcement Agencies that utilize remote video systems designed for long term video monitoring of criminal activity in remote areas. Though the program was designed for Land Management, there is considerable interest among other agencies charged with the collection of video evidence.<br><br>A remote video system is comprised of a recorder, cameras, and various sensors. The systems are typically weatherproof, portable, and designed to be deployed in remote locations and extreme environments where limited resources exist, such as AC power, cell service, internet, and other requirements needed for surveillance equipment installation. RUVSs are designed to be temporary and dynamic, often requiring one system to monitor several locations. The systems maximize efficiency by relieving the need for an Agent or Officer to physically monitor a site.<br><br>An example of a condition suited for a RUV system employment would be a marijuana field found on US Land Management property. The system is deployed to record activity in pathways and clearances for a period of several days. A network of sensors is attached to a processor allowing the system to remain dormant until activated, saving both battery life and recording space. When a sensor is activated the system starts recording and sends a signal to an alert message to the Officer notifying the system has been triggered. Another example would be repetitive thefts from an unoccupied structure like a storage facility. If the recurring theft does not follow a pattern, a RUVS could be deployed to monitor the facility and activate when the intruder triggers a sensor.<br><br>The course will be designed around the principles of the deployment of remote video systems. Blocks of instruction will cover camouflaging, electronic surveillance legal issues, alarm sensors, principles of video, basic electronics and battery power calculations, the theories of radio frequency transmission, RUVS deployment strategy, and the specific operation of the FLETC RUVS. The focus of the program will be on strategies and issues surrounding RUVS deployment and the assessment of video evidence collected. |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a potential investigation, the student will identify the federal requirements governing the use of electronic devices that intercept wire, oral, and electronic communications; install and use video only cameras, and Best Evidence Rule considerations. |

| OPTION H: ICARC |
| --- |
| **DESCRIPTION**: This training program involves the investigation of both Domestic and International aspects of the trafficking of archeological resources. The course is designed in the continuing case format where students will receive training in domestic and international trafficking laws, electronic communication law, writing affidavits for cultural resources, as well as electronic surveillance, investigative planning, undercover operations, interviewing and financial aspects. |

| |
|---|
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a potential investigation, the student will identify the federal requirements governing the use of electronic devices that intercept wire, oral, and electronic communications and track the movement of suspects. |

| **OPTION I: IPCP** |
|---|
| **DESCRIPTION**: This hands-on training program provides the students with the knowledge and practical experience of planning, programming, and installing an Internet Protocol (IP) camera and then using the Internet to transmit video images to a remote location for recording as evidence.<br>FLETC has built a campus wide network specifically for the IPCP program. This network simulates various types of field installation broadband connectivity such as Cable, DSL and EVDO Rev A Cellular. Each student will be assigned a complete inventory of equipment to create both wired and wireless IP camera installations. Various field exercises are designed to allow students to gain experience on programming, installing and recording of IP cameras. |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a potential investigation, the student will identify the federal requirements governing the use of electronic devices that intercept wire, oral, and electronic communications; track the movement of suspects; use video only surveillance, and application of the Best Evidence Rule. |

| **OPTION J: RECVR** |
|---|
| **DESCRIPTION**: This hands-on training program *is designed to provide the responding officer and/or the investigator with the best practices for recognizing, collecting, and properly transporting sensitive digital video evidence from crime scenes in such a manner that preserves the evidentiary integrity of the video.* |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given an incident involving a CCTV system, the responder will identify the federal evidentiary requirements governing the acquisition, authentication, and admission in a judicial proceeding of stored media evidence. |

| **OPTION K: IITP** |
|---|
| **DESCRIPTION**: This program is designed to provide the student with a basic understanding of what the internet is and how it functions and to conduct investigations of crimes in which computers are used, including child pornography and child abuse, identity theft, money laundering, financial and fraud. Students will also be taught techniques for using social networking and internet gaming sites to investigate criminal activity and to conduct tracking of emails and undercover operations on the internet. |

| |
|---|
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given an investigation of a crime involving the use of the Internet, the student will demonstrate the ability to use of a computer and the Internet legally to access, acquire, and preserve evidence of criminal activity. |

| **OPTION L: FRDE** |
|---|
| **DESCRIPTION**: This program is designed to provide the student with a basic understanding of the legally proper methods by which electronic and/or digital evidence may be acquired for use in a criminal prosecution. |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a scenario involving electronic and/or digital evidence, the student will be able to identify potential items of evidence and properly collect and preserve the evidence according to guidelines established by the Department of Justice Guidelines on Computer Search and Seizure and Federal case law. |

| **OPTION M: IAITP** |
|---|
| **DESCRIPTION**: This program is designed to provide the student with a basic understanding of the legally proper methods by which electronic and/or digital evidence may be acquired for use in a criminal prosecution. |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a scenario involving electronic and/or digital evidence, the student will be able to identify potential items of evidence and properly collect and preserve the evidence according to guidelines established by the Department of Justice Guidelines on Computer Search and Seizure and Federal case law. |

| **OPTION N: DOJOIG_IS** |
|---|
| **DESCRIPTION**: This course examines special considerations of which criminal investigators should be aware when conducting a search and seizure of computers and methods of executing search warrants. Also discussed are the Constitutional and statutory requirements regarding the the use of tracking devices; the use of pen registers and trap and trace devices; the use of video-only surveillance in protected areas; and access to stored electronic communications held by network service providers. |
| **TERMINAL PERFORMANCE OBJECTIVE (TPO)**: Given a potential investigation, the student will identify the requirements to use electronic devices to gather evidence, and the considerations to search and seize evidence stored electronically, both on personal premises and network service providers, in accordance with Federal law and Constitutional standards. |

## ENABLING PERFORMANCE OBJECTIVES

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | Applicable EPO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | X | X | X | X | X | X | X | X | | X | | X | | 1. Identify the federal requirements governing the use of electronic devices that intercept wire, oral, and electronic communications. **MEPO 1380-1.** |
| | X | X | X | X | X | | X | X | | | | | X | 2. Identify the federal requirements governing the use of electronic devices that track the movements of suspects. **MEPO 1380-2.** |
| | X | | X | X | | | | | | X | | | | 3. Identify the federal requirements governing the use of electronic devices that trace telephone calls and electronic communications. **MEPO 1380-3.** |
| | X | X | X | X | | X | | X | | | | X | | 4. Identify the federal requirements governing the use of video-only surveillance in locations where an individual has a reasonable expectation of privacy. **MEPO 1380-4.** |
| | X | | X | X | X | | | | | | | X | X | 5. Identify the federal requirements governing access to stored electronic communications. **MEPO 1380-5.** |
| | X | X | | X | | X | | X | X | X | | | | 6. Identify the application of the Best Evidence rule and the rule of authentication to recordings. **MEPO 1380-6.** |
| X | X | | X | X | | | | | | | X | | X | 7. Describe when computers may be searched and/or seized without a search warrant. **MEPO 1380-7.** |
| X | X | | X | X | | | | | | | X | | | 8. Describe special considerations in preparing a search warrant to search and/or seize computers. **MEPO 1380-8.** |

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | Applicable EPO |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **X** | | **X** | **X** | | | | | | | **X** | **X** | **X** | 9. Describe special considerations in executing a search warrant to search and/or seize computers. **MEPO 1380-9.** |
| | **X** | | **X** | **X** | | | | | **X** | | | | | 10. Describe special issues involving authentication of information contained on computers. **MEPO 1380-10.**[1] |
| | | | | | | | | | | | | | | 11. Describe special considerations should privileged information or Privacy Protection Act materials be encountered during a search of computers. **MEPO 1380-11. (Inactive EPO)** |

**STUDENT SPECIAL REQUIREMENTS**: NONE

**METHOD OF EVALUATION:** Written, multiple-choice examinations in all courses except those indicated as non-testable.

[1] This is identical to MEPO 1121-10 (in Courtroom Evidence.)

**METHODOLOGIES:**

1. Lecture
2. Discussion

**TRAINING AIDS:**

1. Instructor:
    a. PowerPoint slides
    b. Dry erase board and markers

2. Student: NONE

**SPECIAL INSTRUCTOR REQUIREMENTS:**

NONE

## OUTLINE OF INSTRUCTION

### I. INTRODUCTION & RAPPORT AND OPENING STATEMENT

#### A. INTRODUCTION.

#### B. RAPPORT AND OPENING STATEMENT

1. Select from the following paragraphs depending on the issues being taught.

   a. **Increased use of electronic surveillance.** The use by law enforcement of various forms of electronic surveillance has taken on a new sense of importance based upon the increased use by criminal offenders of the Internet. Unfortunately, the application of traditional Fourth Amendment concepts to "cyberspace" has resulted in varying degrees of precision. Congress has recognized that real-time interception of oral, wire, or electronic communications and accessing electronic communications held in storage by a network service provider, such as America Online or Prodigy, requires a balancing between the legitimate needs of law enforcement and the privacy interest of the individual whose communications are being obtained. Because of this recognition, statutory protections for phone service and network account holders have been enacted as part of the Omnibus Crime Control and Safe Streets Act of 1968 an the Electronic Communications Privacy Act of 1986.

   b. **The Regulation of Electronic Surveillance.** Nonetheless, Congress has recognized the highly intrusive nature of this type of surveillance and has enacted stringent requirements concerning the use of electronic surveillance. The purpose of this course is to provide a framework for analyzing the requirements governing the use of the surveillance devices discussed above.

c. **Increased Usage of Computers and other Electronic Devices.** Some courts have called computers the modern equivalent of filing cabinets. Other courts distinguish them from mere filing cabinets because they are capable of storing enormous amounts of data. Whereas criminals in times past might have paper files that contain evidence of their activities, the modern criminal uses a computer to send e-mail, keep accounts, prepare correspondence, and generally keep electronically what they formally kept on paper. In other cases - especially in cases of child pornography - the computer is the method of choice not just for the criminal possession of child pornography but also for the transmission of contraband images among multiple violators. While traditional rules governing searches apply to the search of computers, to include those connected to networks, special considerations apply because many innocent items are commingled with evidence of crime. In addition, seizing a computer can often end a person's ability to conduct legitimate business activities, and in recognition of this possibility, judges will often require agents to describe their search strategy to minimize the impact of a computer search.

d. **Application of the Fourth Amendment to Cyberspace.** As noted, application of the Fourth Amendment to "cyberspace" is imprecise. The following example can be used to explain the realistic problems associated with application of the Fourth Amendment to stored electronic communications. While the Fourth Amendment protects the home, "when we use a computer network such as the Internet ... we do not have a physical 'home.' Instead, the closest most users have to a 'home' is a network account consisting of a block of computer memory allocated to them but owned by a network service provider.... If law enforcement investigators need the contents of a network account or information about how it is used, they do not need to go to the user to get that information. Instead, the government can go to the network provider and obtain the information directly from that provider. Although the Fourth Amendment generally requires the government to obtain a warrant to search a home, it does not necessarily require the government to obtain a warrant to obtain the stored contents of a network account. Instead, depending on the status of the various types of data retained by a network provider, it may be constitutionally permissible for the government to issue a subpoena to a network provider ordering the provider to divulge the contents of an account. The Electronic Communications Privacy Act (ECPA) provides the government with this ability while also offering network account holders a range of statutory privacy rights against access to stored account information held by network service providers." *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at 115-149~~75-76~~, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice (2009).

e. **INSTRUCTOR NOTE:** The legal instructor in CESP, CETP, or IPCP class will not have sufficient time in this two-hour block to cover Title III in as much detail as would happen in Electronic Law and Evidence taught to CITP classes. Therefore, the instructor should focus on when a Title III order must be obtained in order to conduct certain operational activities and the exceptions to Title III, emphasizing the need for close coordination with the U.S. Attorney's Office on such issues.

## II. PRESENTATION

### A. EPO # 1: IDENTIFY THE FEDERAL REQUIREMENTS GOVERNING THE USE OF ELECTRONIC DEVICES THAT INTERCEPT WIRE, ORAL, AND ELECTRONIC COMMUNICATIONS

1. **The Background of Title III.** The Omnibus Crime Control and Safe Streets Act of 1968 (hereinafter referenced as Title III), codified at 18 USC §2510 et seq., lays out the Federal requirements governing the use of electronic devices to conduct non-consensual intercepts of real-time transmissions of wire, oral, and electronic communications. [2] To fully understand the strict requirements of Title III, it is vital to understand both the history of this legislation and that Congress, in enacting it, recognized that real-time electronic surveillance of private communications should be restricted to extraordinary circumstances. See United States Attorney's Manual (USAM), Chapter 9-7.100.

   a. **Olmstead v. United States.** Prior to 1934, no federal statute regulating wiretapping existed. However, in 1928, a Supreme Court ruling laid the groundwork for what would ultimately become Title III. In Olmstead v. United States, 277 U.S. 438 (U.S. 1928), prohibition agents who tapped a suspect's telephone lines without his consent and without a search warrant from a location off the suspect's premises were found not to have violated the Fourth Amendment. The Court said that the Fourth Amendment protected the property rights of an individual, not privacy rights. Because the agents did not intrude onto the suspect's property when tapping his phone line, no "search" had occurred under the Fourth Amendment. In their decision, however, the Court noted that Congress could regulate wiretapping, if it desired to do so.

   b. **The Enactment of the Federal Communications Act of 1934.** Six years after the Olmstead decision, Congress did enact legislation regulating wiretapping. The Federal Communications Act of 1934 prohibited wiretapping by any person, including federal law enforcement officers.

      1) **The Language of the Statute.** "No person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purpose, effect, or meaning of such intercepted communication to anyone."

[2] *See* United States v. Radcliff, 331 F.3d 1153, 1160 (10th Cir.) cert. denied 540 U.S. (2003). ("The use of wiretaps and evidence obtained therefrom is governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968").

2) **The Impact on Eavesdropping/Bugging.** The statute, however, did not cover the interception of oral communications (e.g., "bugging" or "eavesdropping"), since this evidence was not obtained through the use of a telephone. Nonetheless, the Fourth Amendment still applied to the use of bugging or eavesdropping. Thus, if law enforcement officers physically intruded onto the suspect's property to eavesdrop, either a search warrant or consent was required.

c. **Katz v. United States.** It was not until almost 40 years later that the Supreme Court changed the basis of Fourth Amendment analysis from strictly property rights to privacy rights. In Katz v. United States, 389 U.S. 347 (U.S. 1967), the defendant used a public telephone located in a booth on a public street to transmit wagering information across state lines. To monitor these conversations, federal law enforcement officers placed a sensitive microphone on the top of the telephone booth. Because they had not intruded on the defendant's property in installing and utilizing this device, the agents had complied with the mandate of Olmstead. The Supreme Court modified its holding in Olmstead, that whenever the government intrudes upon an individual's reasonable expectation of privacy, the Fourth Amendment is implicated. As a result of this decision, a suspect's Fourth Amendment rights are implicated if he or she has a reasonable expectation of privacy in the area to be searched.

2. **The Enactment of Title III.** In response to the Supreme Court's decision in Katz, Congress passed Title III to regulate the manner in which law enforcement officers may lawfully conduct real-time interceptions of wire and oral communications. "The legislative history of Title III instructs that Congress intended this definition to parallel the 'reasonable expectation of privacy test' articulated by the Supreme Court" in Katz."[3] See also, United States v. Petti, 973 F.2d 1441 (9th Cir. 1992), cert. denied, 507 U.S. 1035 (1993) ("Congress codified the requirements of ... Katz in Title III").

[3] United States v. Longoria, 177 F.3d 1179, 1181 (10th Cir.) cert. denied, 528 U.S. 892 (1999)

3. **The Purpose of Title III.** Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986 ("Federal Wiretap Act"), has two purposes: (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized. [4]

4. **What Title III Allows.** Title III permits law enforcement officials to engage in electronic surveillance if certain privacy safeguards are observed. [5] Stated differently, under Title III, law enforcement officers may utilize evidence obtained through electronic surveillance for certain criminal violations, if the officers first obtain a court order authorized under the statute.[6]

**There are, of course, situations where electronic surveillance may be conducted without first procuring a Title III court order, such as when the suspect has no reasonable expectation of privacy in his or her oral communications, or where one party to the conversation consents to the monitoring (consensual monitoring). These situations will be addressed later in this lesson plan.**

5. **The Enactment of the Electronic Communications Privacy Act.** When Title III was passed in 1968, many of the technologies that are now commonplace, such as email, IM Chat, FAX machines, and electronic funds transfers were not considered. In an effort to update Title III and extend the privacy protections of that legislation to modern, more advanced technologies, Congress passed the Electronics Communication Privacy Act of 1986 (ECPA).

---

[4] Kee v. City of Rowlett, 247 F.3d 206, 210 (5th Cir.), cert. denied, 534 U.S. 892 (2001). *See also* United States v. Lopez, 300 F.3d 46 (1st Cir. 2002) ("By enacting Title III, Congress sought to protect the privacy of wire and oral communications while, at the same time, authorizing the use of electronic surveillance evidence obtained by law enforcement under specified conditions"); Bartnicki v. Vopper, 532 U.S. 514, 523 (U.S. 2001) (Noting "[o]ne of the stated purposes of [Title III] was to protect effectively the privacy of wire and oral communications")(internal quotation marks and citation omitted); United States v. Hammond, 286 F.3d 189, 193 (4th Cir), cert. denied, 537 U.S. 900, 537 U.S. 900 (2002) (Noting the statute reflected "congressional concern for protecting privacy"); Adams v. City of Battle Creek, 250 F.3d 980, 986 (6th Cir. 2001) ("The legislation seeks to balance privacy rights and law enforcement needs, keeping in mind the protections of the Fourth Amendment against unreasonable search and seizure").

[5] United States v. McGuire, 307 F.3d 1192, 1196 (9th Cir. 2002).

[6] *See, e.g.*, Abraham v. County of Greenville, 237 F.3d 386, 389 (4th Cir. 2001)(Noting Title III "protects an individual from all forms of wiretapping except when the statute specifically provides otherwise"); United States v. Turner, 209 F.3d 1198, 1200 (10th Cir.), cert. denied, 531 U.S. 887 (2000)("Title III governs the interception by the government and private parties of wire, electronic, and oral communications").

a. **The Addition of "Electronic" Communications.** With the ECPA, Congress added a new category of communications, "electronic communications," whose interceptions would now be regulated. Title I of the ECPA amended the federal Wiretap Act, which previously had addressed only interception of wire and oral communications, to also address interception of electronic communications. [7] Where Title III had been limited to voice communications, whether face-to-face or over a wire, the ECPA extended Title III to include non-oral or wire communications that occur over computers, digital-display pagers, and facsimile machines. USAM, Chapter 9-7.100.

b. **The Addition of Regulations Concerning Stored Communications.** Additionally, the ECPA contains provisions regarding the acquisition of stored communications in what is commonly referred to as the Stored Electronic Communications Act (18 USCS § 2701 et. seq.) [8] This portion of the ECPA will be discussed later in this lesson plan. It must also be noted that Title I of the ECPA deals with the law of electronic communications as covered in this course. As a consequence of the ECPA's passage, this area is referred to alternately by various federal departments and agencies as either Title I or Title III. For purposes of this course, the term Title III will be used to discuss the law of electronic communications.

6. **Relevant Definitions from Title III.** The following definitions will assist in understanding the application of Title III. This list is not exhaustive, but intended to cover those definitions key to an understanding of Title III as discussed in this course. The definitions of additional terms encountered throughout Title III are contained at 18 USCS § 2510.

[7] *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1046 (11th Cir.), cert. denied, 538 U.S. 1051 (2003)

[8] *See* Steiger, 318 F.3d at 1047 ("At the same time, Title II of the ECPA created the Stored Communications Act … to cover access to stored communications and records");
Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878-79 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003) (Noting that ECPA "created the [Stored Communications Act] for the express purpose of addressing access to *stored* … electronic communications and transactional records")(emphasis in original); Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 924 (D. Wis. 2002) ("In 1986, Congress added the Electronic Communications Storage Act, also known as the Stored Communications Act, to the Wiretap Act").

a. **Wire Communications - Defined.** Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce. 18 U.S.C. § 2510(1).

b. **Aural Transfer - Defined.** Means a transfer containing the human voice at any point between and including the point of origin and the point of reception. 18 U.S.C. § 2510(18).

c. **Oral Communication - Defined.** Any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication. 18 U.S.C. § 2510(2).

d. **Electronic Communication - Defined.** Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce, but does not include:

   1) Any wire or oral communication;

   2) Any communication made through a tone-only paging device;

   3) Any communication from a tracking device; or

   4) Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.18 U.S.C. § 2510(12).

e. **Intercept - Defined.** The aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. 18 U.S.C. § 2510(4).

f. **Electronic, Mechanical, or Other Device - Defined.** Any device or apparatus which can be used to intercept a wire, oral, or electronic communication, other than:

   1) **Hearing Aid Exception.** A hearing aid or similar device being used to correct subnormal hearing to not better than normal. 18 U.S.C. § 2510(5).

**Note to instructors**: The extension phone exception below is very narrow and would hardly ever apply to law enforcement picking up the phone. The exception is only useful when, in a business setting, an operator would do so. Recommend this exception NOT be taught.

2) **Extension Telephone "Exception."** Also excluded from the definition of a "device" is telephone equipment used by the subscriber in the "ordinary course of business." This exception is narrow; it applies to employers who monitor their employee's performance, and law enforcement monitoring with notice usually in the inmate setting. It does not apply to non-consensual eavesdropping. The Department of Justice takes the following position:

The exception is for telephone instruments furnished to a subscriber or user by a provider of a wire or electronic communication service and which are being used by the subscriber or user in the ordinary course of its business. The courts of appeals do not agree on the scope of the exception as it pertains to telephone extensions. The Criminal Division believes that the better view is found in *United States v. Harpel*, 493 F.2d 346, 351 (10th Cir. 1974), wherein the court held that "a telephone extension used without authorization or consent to surreptitiously record a private telephone conversation is not used in the ordinary course of business. This conclusion comports with the basic purpose of the statute, the protection of privacy . . . ." *Accord Deal v. Spears*, 980 F.2d 1153, 1157-58 (8th Cir. 1992). *But cf. Epps v. St. Mary's Hospital of Athens, Inc.*, 802 F.2d 412, 415 (11th Cir. 1986); *Briggs v. American Air Filter, Inc.*, 630 F.2d 414 (5th Cir. 1980); *Anonymous v. Anonymous*, 558 F.2d 677 (2d Cir. 1977). In addition, the Criminal Division takes the position that supervisory observing equipment used by some employers to monitor employee telephone communications falls within the "ordinary use" exception only if it is used solely for the legitimate business purpose of determining the need for training or improving the quality of service rendered by employees in the handling of telephone calls, and only after all employees are informed that their business telephone contacts are subject to observation. *See James v. Newspaper Agency Corp.*, 591 F.2d 579 (10th Cir. 1979). USAM, Title 9, Criminal Resource Manual 1047.

7. **The Requirements for a Title III Court Order are greater than those for an ordinary search warrant.** Title III prohibits electronic surveillance by the federal government except under carefully defined circumstances. The procedural steps provided in the Act require strict adherence, and utmost scrutiny must be exercised to determine whether wiretap orders conform to Title III.[9] The effect of Title III is that Congress has placed statutory requirements on warrants authorizing wiretaps that extend beyond the constitutional minimum requirements for a search warrant.[10]

   a. **Any "investigative or law enforcement officer" may initially apply for a Title III court order.** The phrase "investigative or law enforcement officers" is defined as any officer of the United States or of a state or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses. 18 U.S.C. § 2510(7).

   b. **Title III Court Orders May Only Be Obtained For Certain Crimes.** An investigative or law enforcement officer may submit an application for a Title III court order only when investigating certain crimes that are specifically enumerated in 18 U.S.C. § 2516. The type of interception being requested (e.g., wire or electronic) will play a role in this analysis.

      1) **An Application for the Interception of Wire or Oral Communications – Predicate felonies.** When an investigative or law enforcement officer is seeking to intercept wire or oral communications, that officer must have probable cause to believe that one of the predicate offenses specifically listed in 18 U.S.C. § 2516(1) is being committed. As a practical matter, virtually every felony crime is listed under that section of the chapter. Nonetheless, only those crimes enumerated in 18 U.S.C. § 2516(1) may be investigated through the interception of wire or oral communication.

      2) **An Application for the Interception of Electronic Communications – any federal felony.** When an investigative or law enforcement officer is seeking to intercept electronic communications, that officer must have probable cause to believe that ***any*** Federal felony is being committed. 18 U.S.C. § 2516(3).

---

[9] United States v. Blackmon, 273 F.3d 1204, 1207 (9th Cir. 2001)(citations and internal quotation marks omitted). United States v. Nelson-Rodriguez, 319 F.3d 12, 32 (1st Cir.) Cert. denied, 539 U.S. 928 (2003).

[10] United States v. Giordano, 416 U.S. 505, 515 (1974).

c. **Department of Justice Officials Must Authorize a Title III Order.** Before an investigative or law enforcement officer may submit his or her application to a court for a Title III order, that officer's application must be reviewed and approved by an appropriate Department of Justice official. Who must authorize the application depends, again, on what type of interception is being requested.

1) **An Application for the Interception of Wire or Oral Communications.** A high-ranking member of the Department of Justice must authorize any application to a "Federal judge of competent jurisdiction" requesting permission to intercept wire or oral communications. [11] Ordinarily, approval at DOJ will be by the Assistant Attorney General for the Criminal Division; however, the following individuals also may authorize an application to intercept wire or oral communications:

a) The Attorney General;

b) The Deputy Attorney General;

c) The Associate Attorney General;

d) Any Assistant Attorney General;

e) Any Acting Assistant Attorney General; or

f) Any Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General.

2) **An Application for the Interception of Electronic Communications.** The authorization for an electronic communication has been modified by the Department of Justice to be more restrictive than required by statute.

a) **The Statute.** By statute, any government attorney may authorize the making of an application to a Federal court to intercept electronic communication to investigate any Federal felony. [12]

b) **The Department of Justice Policy is more restrictive than the statute.**

(1) AUSAs may approve *applications* to intercept digital display pagers before the application is submitted to a judge.

[11] 18 U.S.C. § 2516(1). Section 2516(1) "[e]vinced the clear intent to make doubly sure that the statutory authority be used with restraint and only where the circumstances warrant the surreptitious interception of wire and oral communications." United States v. Giordano, 416 U.S. 505, 515 (1974).

[12] 18 U.S.C. § 2516(3)

(2) Department of Justice policy requires applications for the interception of electronic communications - other than digital display pagers - to be approved at the Department of Justice before the application is submitted to a judge.[13]

d. **The Contents of the Application.** Every application for a Title III court order must contain specific information before a court can authorize the interception. Further, the application must be in writing, under oath, and signed by the United States Attorney or an Assistant United States Attorney.[14]

1) **The Identity of the Officer Making the Application.** The application must contain the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application.[15]

2) **A Full Statement of the Facts and Circumstances of the Case.** The application must have a complete statement of the facts and circumstances relied upon by the applicant to justify his belief that an order should be issued, including:[16]

a) **Details As to the Particular Offense That Has Been, is Being, or is About to be Committed.** (It must be remembered that interceptions of wire or oral communications may only be authorized if the offense being investigated is one of the predicate offenses listed in 18 U.S.C. § 2516(1), while 18 U.S.C. § 2516(3) provides that electronic communications may be intercepted during the investigation of any federal felony.)

b) **A Description of the Nature and Location of the Facilities.** A particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted must be included in the application.

There is an exception to this rule in those situations where a "roving" intercept is being requested. A "roving" intercept is one in which the government seeks approval to intercept communications without specifying with particularity the facilities or places where the communication is to be intercepted (such as in the case of intercepting those calls made to a cellular telephone). The specific requirements that must be met for a "roving" intercept will be discussed in more detail in subparagraph 8, below.

[13] USAM, Chapter 9.7-100.

[14] 18 U.S.C. § 2518; USAM, Chapter 9, Criminal Resource Manual at 28.

[15] 18 U.S.C. § 2518(1)(a).

[16] 18 U.S.C. § 2518(1)(b).

c) A particular description of the type of communications sought to be intercepted; and

d) **The Identity of the Individuals Whose Communications Are to Be Intercepted.** The identity of the individuals, if known, committing the offense and whose communications are to be intercepted must also be included in the application.

(1) **The Supreme Court's Interpretation of This Provision.** In interpreting this provision, the Supreme Court has held the "Government is not required to identify an individual in the application unless it has probable cause to believe that:

(a) The individual is engaged in the criminal activity under investigation, and

(b) The individual's conversations will be intercepted over the target telephone."

United States v. Donovan, 429 U.S. 413 (U.S. 1977)

(2) **The Department of Justice Policy.** It is the policy of the Department of Justice to "name as potential subjects all persons whose involvement in the alleged offenses is indicated." USAM, Chapter 9, Criminal Resources Manual at 28.

(3) **Intercepts of Individuals Not Named in the Application.** If the interception obtains evidence against an individual not named in the application (e.g., someone not named because they were unknown at the time of the application), that evidence may still be used against the non-named defendant, providing that the remainder of Title III's requirements have been met. [17]

[17] *See, e.g.*, Donovan, 492 U.S. at 435 (Noting that, where Title III requirements have been met, "the failure to identify additional persons who are likely to be overheard engaging in incriminating conversations could hardly invalidate an otherwise lawful judicial authorization");United States v. Miller, 116 F.3d 641 (2d Cir. 1997), cert. denied, 524 U.S. 905 (1998).

3) **A Full Statement Regarding Other Investigative Procedures (the necessity requirement).** A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous. 18 U.S.C. § 2518(1)(c).

This section is sometimes referred to as the "necessity" requirement, and simply means that the interception must be shown to be necessary to the investigation of the case. This aspect of a Title III Order is discussed more fully in subparagraph 9, below.

4) **Statement of the Time Period for Which the Interception is to be Conducted – 30 days or shorter.** The application must contain a statement of the period of time for which the interception is to be maintained,[18] and no Title III order may "authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty (30) days.[19]

a) **The Running of the Time Period.** The thirty-day period authorized by the statute begins on the earlier of either:

(1) **The Day the Interceptions Begin.** The day on which the investigative or law enforcement officer begins to conduct an interception under the order ... OR

(2) **Ten Days after the Order is Issued.** The time period may begin running ten days after the order is issued. This ten-day period is "intended primarily for the installation of oral monitoring equipment, before the thirty-day period begins to be calculated. This provision may also be used when delays arise in installing monitoring devices used in wire or electronic interceptions."

18 U.S.C. § 2518(5) USAM, Chapter 9, Criminal Resources Manual at 29.

[18] 18 U.S.C. § 2518(1)(d).

[19] 18 U.S.C. § 2518(5).

b) **Extensions of a Title III Court Order.** Extensions of a Title III order may be granted, but only upon again meeting the requirements of the initial Title III application. Where the Title III application is for an extension of a previously approved order, the application "must include a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results."[20]

5) **A Full Statement Regarding Previous Applications Must Be Included.** The application must also contain "a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each such application."[21]

a) **Intentional Non-Compliance with This Provision.** When the applicant intentionally fails to provide the information required by 18 U.S.C. § 2518(1) (e), it can result in the suppression of any evidence obtained through the surveillance. [22]

b) **Inadvertent Non-Compliance with This Provision.** However, where the failure to comply with the statute was inadvertent or unintentional, the courts have uniformly refused to suppress the evidence obtained through the surveillance.[23]

[20] 18 U.S.C. § 2518(1)(f).

[21] 18 U.S.C. § 2518(1)(e).

[22] United States v. Bellosi, 163 U.S. App. D.C. 273 (D.C. Cir. 1974).

[23] *See, e.g.*, United States v. Zannino, 895 F.2d 1, 9 (1st Cir.), cert. denied, 494 U.S. 1082 (1990); United States v. Pinelli, 890 F.2d 1461, 1475 (10th Cir. 1989), cert. denied, 493 U.S. 960 (1990); United States v. Van Horn, 789 F.2d 1492, 1500 (11th Cir.), cert. denied, 479 U.S. 854 (1986)

c) **Actual Knowledge of the Prior Application is Required.** In order to suppress evidence based upon a violation of 18 U.S.C. § 2518(e), it must be shown that the law or investigative officer applying for the order had actual knowledge of the previous applications or orders. Constructive knowledge will not suffice.[24]

6) **The Requirement for Minimization.** The application should also contain a statement by the law or investigative officer that the surveillance will be "conducted in such a way as to minimize the interception of communications not otherwise subject to interception." [25]

The requirement for minimization is discussed more fully in subparagraph 10, below.

7) **A Request for the Assistance of Service Providers.**

a) 18 U.S.C. § 2511(2) (a) (ii) authorizes "providers of wire or electronic communication service" to "provide information, facilities, or technical assistance" to law or investigative officers. The application should contain a request for this type of service provider assistance, as well as an order not to disclose the contents of the court order or the existence of the investigation. USAM, Chapter 9, Criminal Resources Manual at 28.

b) *Case note*. In Company v. United States (In re United States), 349 F.3d 1132 (9th Cir. 2003), the provider of in-vehicle cell-phone service ("the company" was probably On-Star) was served with an approved Title III order directing that the cell phone in the subject's car be turned on as the covert listening device. The Company resisted claiming that while the Title III order did require the company to assist, that assistance was not required when the very service a provider is being paid to provide would be eclipsed by assisting law enforcement. The court agreed that The Company did not have to honor the Title III order because if the cell phone was turned on, the automatic emergency cell-phone alert services would be disabled.

[24] *See, e.g.*, Zannino, 895 F.2d at 9 (Noting Title III "requires actual, not constructive, knowledge").

[25] 18 U.S.C. § 2518(5). *See also* USAM, Chapter 9, Criminal Resources Manual at 28 (The application "should contain a statement affirming that all interceptions will be minimized....").

8) **Request for Covert Entry to Install, Maintain, and Remove Devices.**

a) The Supreme Court has held that a request for covert entry is not required in a Title III application, and that covert entry is implied when a Title III has been issued.[26]

b) **DOJ Policy: Application for Title III must contain request for covert entry to install device.** The Department of Justice requires that the Title III application contain a request for permission to surreptitiously enter to install, maintain, and remove electronic surveillance devices. USAM, Chapter 9, Criminal Resources Manual at 28. provides, "In an oral (and occasionally in a wire or electronic) interception, [the application] must contain a request that the court issue an order authorizing investigative agents to make all necessary surreptitious and/or forcible entries to install, maintain, and remove electronic interception devices in or from the targeted premises (or device). When effecting this portion of the order, the applicant should notify the court as soon as practicable after each surreptitious entry."

9) **Only a District Court or Court of Appeals Judge May Approve a Title III Application.**

[26]In Dalia v. United States, 441 U.S. 238 (U.S. 1979), the Supreme Court addressed two questions pertaining to the covert installation of electronic surveillance equipment: "First, may courts authorize electronic surveillance that requires covert entry into private premises for installation of the necessary equipment? Second, must authorization for such surveillance include a specific statement by the court that it approves of the covert entry?" Id. at 241 (footnotes omitted). The answer to the first question was "yes." The answer to the second was "no." In sum, the Court held that "[t]he Fourth Amendment does not prohibit *per se* a covert entry performed for the purpose of installing otherwise legal electronic bugging equipment." Id.. at 248 (footnote omitted)(emphasis in original). While noting that Title III does not explicitly refer to convert entry, "[t]he language, structure, and history of the statute, however, demonstrate that Congress meant to authorize courts - in certain specified circumstances - to approve electronic surveillance without limitation on the means necessary to its accomplishment, so long as they are reasonable under the circumstances." Id. at 249. As the Court noted: "Those considering the surveillance legislation understood that, by authorizing electronic interception of oral communications in addition to wire communications, they were necessarily authorizing surreptitious entries." Id. at 252.

a) The Title III application must be submitted for approval to "a judge of competent jurisdiction,"[27] which is in this instance a judge of a United States district court or a United States court of appeals.[28] Additionally, the application must be "accompanied by the Department of Justice's authorization memorandum signed by an appropriate Department of Justice official." USAM, Chapter 9, Criminal Resources Manual at 28.

b) **Magistrate Judges.** A United States Magistrate Judge does not have authority to approve a Title III application. [29]

e. **Requirements for Approving a Title III Application.** If all of the required information is contained in the Title III application, the judge may enter an order approving of the interception(s), if the judge determines on the basis of the application that:

1) **Predicate Offense.** First, the judge must find that "[t]here is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in 18 USCS § 2516; Title 18 U.S.C. § 2518(3)(a).

2) **Communications Concerning the Offense.** Second, the judge must find that "[t]here is probable cause for belief that particular communications concerning that offense will be obtained through such interception." 18 U.S.C. § 2581(3)(b).

3) **Necessity Requirement Met.** Third, the judge must find that "[n]ormal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(3)(c).

[27] 18 U.S.C. § 2518(1).

[28] 18 U.S.C. § 2510(9).

[29] *See* In re United States of America, 10 F.3d 931 (2d Cir. 1993), cert. denied, 513 U.S. 812 (1994) ("In sum, we are unwilling, in the absence of explicit statutory direction, to expansively interpret Title III's definition of a 'judge of competent jurisdiction' ... to include magistrate judges.").

4) **Target Facilities or Premises.** Finally, the judge must find, except in those situations where a "roving" intercept is requested, that "[t]here is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person." 18 U.S.C. § 2518(3)(d).

f. **Contents of the Title III Court Order.** All Title III court orders must contain certain information. Additionally, the court order may contain information in addition to what is required by statute. The following information either must be included, or may be included, in the court order:

1) **Identity.** The court order must contain "[t]he identity of the person, if known, whose communications are to be intercepted." 18 U.S.C. § 2518(4)(a).

2) **Target Facilities or Premises.** The court order must contain "[t]he nature and location of the communications facilities, as to which, or the place where, authority to intercept is granted." 18 U.S.C. § 2518(4)(b).

3) **Particular Description of Communications.** The court order must contain "[a] particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates." 18 U.S.C. § 2518(4)(c).

4) **Agency Identification and Authorization.** The court order must contain "[t]he identity of the agency authorized to intercept the communications, and of the person authorizing the application. 18 U.S.C. § 2518(4)(d).

5) **Time Period.** The court order must contain "[t]he period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained." 18 U.S.C. § 2518(4)(e).

6) **Assistance of Service Providers.** If requested, the Title III court order must direct "[t]hat a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference...." 18 U.S.C. § 2518(4)(e).

7) **Progress Reports.** A Title III court order may contain a requirement that periodic progress reports be made to the judge who issued the order, "showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require." 18 U.S.C. § 2518(6).

8) **Covert Entry for Installation, Monitoring, Removal of Electronic Device.** The Title III court order may contain language authorizing the covert or surreptitious entry into the location for installation, monitoring, or removal of any electronic surveillance equipment.

8. **The Rules on "Roving" Intercepts.** As noted earlier, a "roving" intercept is one in which the government seeks approval to intercept communications without specifying with particularity the facilities or places where the communication is to be intercepted (such as in the case of intercepting those calls made to a cellular telephone). Special requirements must be met before a law enforcement officer may utilize a "roving intercept during the course of an investigation. The following requirements must be met when requesting a "roving" intercept:

a. **Requirements Regarding the Interception of Oral Communications.** With regards to the interception of oral communications, the government must show that:

1) Specification of the location is not practical; and

2) The identity of the person committing the offense and whose communications are to be intercepted.

18 U.S.C. § 2518(11)(a). *See also* United States v. Bianco, 998 F.2d 1112, 1123 (2d Cir. 1993), cert. denied, 511 U.S. 1069 (1994). ("Section 2518(11)(a) specifically addresses some of the concerns expressed by the Supreme Court that warrants be particular; it requires a full and complete statement as to why a particular description of the location to be monitored is not practical").

b. **Requirements Regarding the Interception of Wire or Electronic Communications.** With regards to the interception of wire or electronic communications, the government must:

1) Identify the person believed to be committing the offense and whose communications are to be intercepted, and

2) Show that there is probable cause to believe that the person's actions could have the effect of thwarting interceptions from a specified facility.

18 U.S.C. § 2518(11)(b). *See also* United States v. Gaytan, 74 F.3d 545 (5th Cir.) cert. denied 519 U.S. 821 (1996) (Holding that requirement to show that suspect's actions could have the effect of thwarting surveillance was met where "government's request for the wiretap order indicated that the defendants had engaged in a pattern of changing cellular phone numbers in an effort to avoid surveillance").

c. **Department of Justice Authorization for "Roving" Interceptions.** When the government seeks to intercept any type of communication with a "roving" intercept, the Department of Justice's authorization must be made by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an Acting Assistant Attorney General. 18 U.S.C. § 2518 (11)(a) (i) and b (i).

d. **Additional Requirements.** All of the other requirements of Title III, such as duration, minimization, etc., which will be discussed in the following sections, still apply to "roving" intercepts.

9. **The "Necessity" Requirement.** As noted previously, 18 U.S.C. § 2518(1)(c) requires "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." This section is sometimes referred to as the "necessity" requirement, and simply means that the interception must be shown to be necessary to the investigation of the case. 18 U.S.C. § 2518(1)(c) was "designed to assure that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime. [30]

   a. **What Must the Government Show to Meet the "Necessity" Requirement?** "In order to prove that a wiretap is necessary, the government must show that traditional investigative techniques:

      1) Have been tried unsuccessfully,

      2) Reasonably appear to be unsuccessful if tried, or

      3) Are too dangerous to attempt." [31]

   b. **Only One of the Three Must Be Established.** These requirements are set forth in the alternative and thus the government need only establish one of the three. [32] Stated differently, the government must only prove that "traditional investigative techniques" have been tried and failed, ***or*** would reasonably be unlikely to succeed if tried, ***or*** are too dangerous to attempt.

   c. **Exhaustion of All Other Investigative Methods is not Required.** The government is not required to prove that all other investigative techniques have been tried and exhausted. In examining necessity challenges to wiretap orders, the courts have repeatedly held that law enforcement officials are not required to exhaust all other conceivable investigative procedures before resorting to wiretapping.[33] In addition, the necessity requirement can be met even though law enforcement does not utilize traditional methods, such as ordinary physical surveillance, regular search warrants, confidential informants, and infiltration of the organization by undercover agents or informants.[34]

---

[30] United States v. Kahn, 415 U.S. 143 (U.S. 1974) (dictum).

[31] United States v. Ramirez-Encarnacion, 291 F.3d 1219 (10th Cir. 2002).

[32] United States v. Fudge, 325 F.3d 910, 918 (7th Cir. 2003)(citation omitted).

[33] In United States v. Garcia-Vallalba, 585F.3d 1223 (9th Cir. 2009), the Court held that it is not necessary to the government to exhaust every conceivable alternative before obtaining a wiretap. Rather, the necessity requirement satisfied by a good faith showing that (1) ordinary investigative procedures would likely be ineffective, and (2) wiretap evidence is needed in order to develop proof beyond reasonable doubt of target's guilt, (not merely probable cause). *See also,* United States v. Edwards, 69 F.3d 419 (10th Cir. 1995), cert. denied, 517 U.S. 1243 (1996) (internal quote marks and citations omitted).

[34] United States v. Smith, 31 F.3d 1294 (4th Cir. 1994), cert. denied, 513 U.S. 1181 (1995).

d. "Necessity" Must Be Determined on a Case By Case Basis. Instead, whether the "necessity" requirement has been met must be determined on a case-by-case basis, examining the specific facts applicable in each case. The government's burden of proving 'necessity' is not high35 and this requirement ordinarily can be satisfied by a showing in the application that ordinary investigative procedures, employed in good faith, would likely be ineffective in the particular case. 36

e. **Examples of "Traditional" Investigative Techniques.**[37]

1) Standard visual and aural surveillance;

2) Questioning and interrogation of witnesses or participants (including the use of grand juries and the grant of immunity if necessary);

3) Use of search warrants; and

4) Infiltration of conspiratorial groups by undercover agents or informants."

f. **Failure of Other Investigative Methods.** An investigative or law enforcement officer may show that other investigative methods have been tried and failed. In these situations, it must be shown that the investigators gave serious consideration to the non-wiretap techniques prior to applying for wiretap authority and that the court be informed of the reasons for the investigators' belief that such non-wiretap techniques have been or will likely be inadequate.[38]

a) Case examples:

(1) Necessity requirement met where traditional investigative techniques were tried or reasonable likely to fail, including physical surveillance with ground vehicles and aircraft, grand jury subpoenas, interviews, search warrants, and undercover agents.[39]

[35] United States v. Dumes, 313 F.3d 372, 378 (7th Cir. 2002) (citation omitted).

[36] United States v. McGuire, 307 F.3d 1192, 1196 (9th Cir. 2002).

[37] United States v. Vanmeter, 278 F.3d. 1156, 1163-64 (10th Cir. 2002). (citation omitted).

[38] United States v. Lambert, 771 F.2d 83, 91 (6th Cir.), cert. denied, 474 U.S. 1034 (1985).

[39] United States v. Dumes, 313 F.3d at 379.

(2) Necessity requirement met where confidential informants were tried, access to witness protection program was tried and rejected, visual surveillance was tried inconclusively, suspect's roots in the neighborhood made it impossible for surveillance to remain inconspicuous, an adequate number of agents were assigned to the case, "fear of physical harm on the part of various persons impeded the hunt," and pen registers and telephone toll records were examined.[40]

g. **Unlikelihood of Success of Other Investigative Methods.** An investigative or law enforcement officer may show that other investigative methods reasonably appear unlikely to succeed. In United States v. Uribe, 890 F.2d 554 (1st Cir. 1989), the court commented on the "necessity" requirement: "Title III demands a practical, commonsense approach to exploration of investigatory avenues and relative intrusiveness. In essaying such an approach, the type of crime is important. By its very nature, interstate drug trafficking is hard to pin down. Surely, 'the law was not meant to force the government to run outlandish risks or to exhaust every conceivable alternative before seeking a wiretap.' Here, we think the necessary predicate was laid: supporting documents filed by the government carefully detailed a variety of investigative procedures which had been utilized, set out a solid basis for believing that drugs were being sold, and explicated the need for more sophisticated inquiry. Defendants do not cast any real doubt on the scope or sincerity of the government's earlier investigatory efforts, nor do they convincingly suggest what else, short of electronic surveillance, the FBI might fruitfully have attempted to further the probe." Uribe, 890 F.2d at 556-57 (citation omitted).

[40] United States v. Hoffman, 832 F.2d 1299, 1307 (1st Cir. 1987)

h. **Other Investigative Methods are too Dangerous.** Finally, an investigative or law enforcement officer may show that other investigative methods are too dangerous to attempt. For example, in United States v. Wilkinson, 754 F.2d 1427, 1433 (2d Cir.), cert. denied, 472 U.S. 1019 (1984), the court noted that the "necessity" requirement had been met because, among other things, "concerns about the safety of the agents had arisen." Similarly, in United States v. Robertson, 15 F.3d 862, 874 (9th Cir. 1994), rev'd on other grounds, 514 U.S. 945 (1995), the necessity requirement was met where, among other things, the agents explained "that further undercover operations in the form of fronting funds would be high-risk as it could result in rip-offs."

i. **Specific Examples of How to Meet the "Necessity" Requirement.** As noted, the government must either try traditional investigative techniques or, where not tried, explain that failure with particularity. Below are specific examples of how a law enforcement officer was able to establish that various forms of traditional investigative techniques had been tried and failed. These examples come directly from the case of United States v. Cline, 349 F.3d 1276 (10th Cir. 2003), which involved wiretapping during the investigation of a large-scale narcotics ring.

1) **Infiltration by Undercover Officers.** In this instance, the affidavits "explained how infiltration by undercover agents had been unsuccessful because most members of the organization had lived in the same area for years, had known each other for years, and were suspicious of anyone new. Further, the affidavits stated that the investigation revealed that [the leader] kept his subordinates separate so that they did not always know each other's identity or know what other members of the organization were doing." Cline at *12-*13.

2) **Review of Telephone Records, Including Pen Register Results.** Additionally, "[t]he affidavits recounted the use of pen register information in the investigation, but stated that such information was limited in its usefulness because it did not reveal the identities of the parties to the conversation nor the nature or substance of the conversation, nor differentiate between legitimate calls and those for criminal purposes." Cline. at *13-*14.

3) **Questioning of Potential Witnesses, With or Without Grants of Immunity.** Further, "[t]he affidavits further detailed that while some cooperating individuals had been interviewed, further questioning of individuals was unlikely to prove fruitful. A number of individuals involved in the drug organization had histories of violence. Several murders were believed by those close to the organization to be related to the organization's drug activity. Several individuals had indicated that, while they had provided some confidential information, they would refuse to testify because of fear for their safety." Cline at *14.

4) **Use of Informants.** While law enforcement had made use of confidential informants, "the organization revealed itself to be 'compartmentalized' and 'close-natured.' The affidavits revealed the use of three cooperating individuals who had some degree of success in infiltrating the targeted criminal organization but whose future usefulness was virtually nil. …unlikely. Given that the targets were a The affidavits adequately established that, due to the close-knit community, as well as the suspicious nature of those involved in the drug organization and the difficulty of introducing anyone new into it, the government sufficiently demonstrated that the further use of informants the traditional investigative technique of informants had been tried but was unlikely to meet with further success. Cline. at *14-*15.

5) **Physical Surveillance.** While physical surveillance had been used in the investigation, the affidavit "detailed the difficulties encountered in conducting surveillance in the rural area: the officers and their vehicles stood out among the locals; [the suspects] used sophisticated counter-surveillance techniques; members of the drug organization were familiar with and used back roads where surveillance was difficult or easily detected; surveillance of [one suspect's] business was hampered by the fact that some suspects in the drug organization were county employees and local business persons." Cline. at *16.

6) **Use of Search Warrants.** Finally, "[t]he affidavits detailed the limited success obtained thus far by the use of search warrants. While they had resulted in the seizure of drugs and methamphetamine laboratories and proceeds, they had failed to uncover the scope of the operations, or identify the sources of the precursor chemicals, the methods of distribution, and other members of the conspiracy." Cline

j. **The Minimization Requirement.** As noted previously, Title 18 U.S.C. § 2518(5) requires that wire, oral, or electronic communications intercepts be "conducted in such a way as to minimize the interception of communications not otherwise subject to interception." In sum, "[m]inimization requires that the government adopt reasonable measures to reduce to a practical minimum the interception of conversations unrelated to the criminal activity under investigation while permitting the government to pursue legitimate investigation." McGuire, 307 F.3d at 1199. *See also* United States v. Mansoori, 304 F.3d 635, 646 (7th Cir. 2002), cert. denied sub nom. Cox v. United States, 538 U.S. 967 (2003)("What the minimization requirement means, essentially, is that once the monitoring agent has had a reasonable opportunity to assess the nature of an intercepted communication, he or she must stop monitoring that communication if it does not appear relevant to the government's investigation").

1) **The Standard for Determining Minimization.** In determining whether the requirement for minimization was met, the "critical inquiry is whether the minimization effort was managed reasonably in light of the totality of the circumstances." United States v. Charles, 213 F.3d 10 (1st Cir.), cert. denied, 531 U.S. 915 (2000)[*citing* Scott v. United States, 436 U.S. 128 (1978)]. *See also* Mansoori, 304 F.3d at 647 ("A court assessing the sufficiency of the government's efforts in this regard must ultimately decide whether the steps that agents have taken to minimize the interception of communications unrelated to the investigation were objectively reasonable given the circumstances confronting the agents"). In this regard, "the government is held to a standard of honest effort; perfection is usually not attainable, and is certainly not legally required." United States v. London, 66 F.3d 1227, 1236 (1st Cir. 1995), cert. denied, 517 U.S. 1155 (1996)(citation omitted).

2) **Factors to Consider in Determining Whether the Minimization Requirement Was Met.** Although determining whether the minimization requirement was met is necessarily dependent on the specific facts in any given case, courts have focused on a variety of factors, including:

a) **The nature and complexity of the suspected crimes.** *See, e.g.*, Scott, 436 U.S. at 140 (Noting that, "when the investigation is focusing on what is thought to be a widespread conspiracy more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise …"); Charles, 213 F.3d at 22 (Noting that "the nature and complexity of the suspected crimes" is a "crucial factor in measuring the reasonableness of the government's conduct"); United States v. Ozar, 50 F.3d 1440, 1447 (8th Cir.), cert. denied, 516 U.S. 871 (1995)(Noting "the complexity of the acts under investigation" is relevant in determining reasonableness of minimization efforts); United States v. Brown, 303 F.3d 582, 604 (5th Cir. 2002), cert. *denied,* 537 U.S. 1173 (2003)(Noting three-part test to determine the reasonableness of minimization includes examination of "the nature and scope of the criminal enterprise under investigation"); United States v. Fregoso, 60 F.3d 1314, 1322 (8th Cir. 1995)("However, we have been more tolerant of extensive surveillance involving the use of wiretaps in large scale narcotics conspiracy cases involving frequent drug related conversations").

b) **The number of target individuals.** *See* Ozar, 50 F.3d at 1447 ("Relevant considerations" in assessing reasonableness of minimization efforts include "the number of target individuals").

c) **The ambiguity of the intercepted conversations.** *See* Ozar, 50 F.3d at 1447 ("Relevant considerations" in assessing reasonableness of minimization efforts include "the ambiguity of the intercepted conversations"); Brown, 303 F.3d at 604 (Noting "the Government's reasonable inferences of the character of a conversation from the parties to it" should be considered in determining reasonableness of minimization efforts).

d) **Whether the calls involved coded or foreign languages.** Title 18 U.S.C. § 2518(5) provides, in pertinent part, that "[i]n the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception." *See also* Mansoori, 304 F.3d at 647 (Noting the adequacy of government's minimization efforts depends on the facts of the case, including the "use of code"); London, 66 F.3d at 1236 (Noting that, "when an interpreter is not reasonably available, Title III explicitly allows full-scale recording and post hoc minimization of conversations carried out in foreign languages").

e) **The length of the calls.** Some courts have found that calls of less than 2 minutes to not require minimization. *See* United States v. Malekzadeh, 855 F.2d 1492 (11th Cir. 1988); United States v. Apodaca, 820 F.2d 348 (10th Cir. 1987).

f) **The thoroughness of the government precautions to bring about minimization.** *See, e.g.*, McGuire, 307 F.3d at 1201 ("Another factor weighing in favor of the reasonableness of the FBI's minimization procedure is the effort the agency made to protect the defendants' privacy").

g) **The degree of judicial supervision over the surveillance practices.** *See* Charles, 213 F.3d at 22 (Noting "the degree of judicial supervision over the surveillance practices" as "crucial factor in measuring the reasonableness of the government's conduct"); Ozar, 50 F.3d at 1447 (Noting "the extent of the issuing judge's involvement in the surveillance" is a "relevant consideration" in determining the reasonableness of minimization efforts); Brown, 303 F.3d at 604 (Noting "the extent of judicial supervision" goes into analysis of minimization efforts).

h) **After-the-fact minimization.** The government need not show, as a prerequisite to after-the-fact minimization, that contemporaneous minimization was an utter impossibility. Rather, it need only demonstrate in good faith that contemporaneous minimization was not reasonably available and that the after-the-fact minimization utilized protected the suspect's privacy interests to the same extent as contemporaneous minimization would have. *See* *Scott v. United States*, 436 U.S. 128, 139-42, 56 L. Ed. 2d 168, 98 S. Ct. 1717 (1978); *Uribe*, 890 F.2d at 557; *United States v. Gambino*, 734 F. Supp. 1084, 1106 (S.D.N.Y. 1990). When the interception is of electronic communications over a digital-display pager or a fax machine, such communications are recorded and then examined by a monitoring agent and/or a supervising attorney to determine their relevance to the investigation. Disclosure is then limited to those communications by the subjects or their confederates that are criminal in nature. *See United States v. Tutino*, 883 F.2d 1125 (2d Cir. 1989), *cert. denied*, 493 U.S. 1081 (1990). See USAM, Title 9, Criminal Resource Manual 29.

3) **Violations of the Minimization Requirement.** Where the government fails to adequately minimize the electronic surveillance, any evidence obtained from those impermissible intercepts will be suppressed. However, "errors in minimizing one particular interception within the context of a lengthy and complex investigation ... do not automatically warrant the suppression of all the evidence obtained through electronic surveillance." United States v. Baltas, 236 F.3d 27 (1st Cir. 2001). Instead, suppression of all electronic surveillance is proper only where the defendant demonstrates that the entire surveillance was tainted by the impermissible intercepts. United States v. Hoffman, 832 F.2d 1299 (1st Cir. 1987).

10. **Suppression as a Remedy for a Title III Violation.** Where a Title III violation has occurred, suppression of any evidence obtained may result from the violation.

a. **Title 18 U.S.C. § 2515.** This section provides that "whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter."

b. **Title 18 U.S.C. § 2518(10)(a)(i).** This section provides that "any aggrieved party in or before any court … may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on that grounds that – the communication was unlawfully intercepted."

c. **Not All Violations of Title III Will Result in Suppression.** "[I]t is well-settled that not every failure to comply fully with any requirement provided in Title III necessitates suppression." United States v. Escobar-de Jesus, 187 F.3d 148, 171 (1st Cir. 1999), cert. denied, 528 U.S. 1176 (2000).

1) **When is Suppression Required?** Instead, "suppression is required only for a 'failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device.'" United States v. Donovan, 429 U.S. 413, 433-34 (1977)(citation omitted). There are, of course, exceptions to this general rule.

2) **There is an "Impeachment" Exception to the Suppression Remedy.** Numerous circuit courts of appeal have recognized an "impeachment" exception to the suppression remedy. *See, e.g.,* United States v. Baftiri, 263 F.3d 856 (8th Cir. 2001); Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993); United States v. Echavarria-Olarte, 904 F.2d 1392 (9th Cir. 1990); Jacks v. Duckworth, 651 F.2d 480 (7th Cir. 1981), cert. denied, 454 U.S. 1147 (1982); and United States v. Caron, 474 F.2d 506 (5th Cir. 1973). In Baftiri, the Eight Circuit Court of Appeals cited each of the above cases with approval, noting that "these holdings were in accord with the Supreme Court's Fourth Amendment jurisprudence, under which evidence obtained by an unreasonable search and seizure, in violation of that Amendment, can be used to impeach a defendant who chooses to take the witness stand in his own defense. Evidence seized in violation of the Fourth Amendment or the federal wiretapping statute cannot be used by the government in its case-in-chief. But, if the defendant chooses to testify, and swears to a sequence of events inconsistent with his own previously recorded statements, the Constitution does not require the government to leave the lie (or what it contends to be a lie) unchallenged." (citation omitted). The court went on to emphasize that "[i]t makes no sense for evidence obtained in violation of a mere statute to be more severely restricted than evidence obtained in violation of the Constitution. At the time the statute was enacted, evidence obtained in violation of the Fourth Amendment could be used for impeachment purposes. It is reasonable to assume that Congress had this background in mind when the statute was passed, and that, in the absence of an express statement, it did not intend to draw the line of exclusion in a different place."

11. **Various Types of Surveillance Are Exempted From Title III.** Not all interceptions of wire, oral, or electronic communications require a Title III court order. Some of these exclusions will be discussed in more detail later in this lesson plan. However, two of the most important exemptions to the general rule requiring a Title III court order involve situations where (1) an individual has no reasonable expectation of privacy in his or her oral communications, and (2) one of the parties to the conversation has given consent to intercept his or her communications (consensual monitoring). Each of these exceptions will be addressed in turn.

a. **A Title III Court Order is Not Required Where There is No Reasonable Expectation of Privacy in an Oral Conversation.** In Katz v. United States, 389 U.S. 347 (1967), the Supreme Court established the standard for determining whether a reasonable expectation of privacy (REP) exists. The test for REP is two-pronged: First, the individual must have exhibited an actual (subjective) expectation of privacy; and, second, that expectation must be one that society is prepared to recognize as reasonable. If either prong of the test is not met, then no REP exists.

1) **18 U.S.C. § 2510(2).** The statute defines an "oral communication" as one "uttered by a person exhibiting an expectation of privacy that such communication is not subject to interception under circumstances justifying such expectation...."

2) **This Definition Parallels the Privacy Test of Katz.** "The legislative history of Title III instructs that Congress intended this definition to parallel the 'reasonable expectation of privacy test' articulated by the Supreme Court in Katz. … Accordingly, for Title III to apply, the court must conclude: (1) the defendant had an actual, subjective expectation of privacy - i.e., that his communications were not subject to interception; and (2) the defendant's expectation is one society would objectively consider reasonable." United States v. Longoria, 177 F.3d 1179, 1181-82 (10th Cir.), cert. denied, 528 U.S. 892 (1999).

3) **No Similar Exception Exists for Wire Communications.** Of note, "[n]o similar exception is contained in the definition of wire communications and, therefore, the non-consensual interception of wire communications violates Title 18 U.S.C. § 2511, regardless of the communicating parties' expectation of privacy, unless the interceptor complies with the court authorization procedures of Title III...." USAM, Chapter 9-7.301 (Consensual Monitoring - General Use).

4) **There is No Reasonable Expectation of Privacy in Conversations Exposed to the Public.** "[C]onversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable." Katz, 389 U.S. at 361 (Harlan, J., concurring). "[W]hat a person knowingly exposes is not constitutionally protected from observation." Id. at 389 U.S. at 363 (Harlan, J., concurring). "Neither are activities or objects which are exposed, regardless of subjective intent, in a manner inconsistent with reasonable expectations of privacy. Thus, it is not a 'search' to observe that which occurs openly in public. Nor is it a search when a law enforcement officer makes visual observations from a vantage point he rightfully occupies. This applies also to perceptions derived from hearing or smelling." United States v. Burns, 624 F.2d 95 (10th Cir.), cert. denied, 449 U.S. 954 (1980)(citations omitted). Finally, "[t]he risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society." Hoffa v. United States, 385 U.S. 293 (1966)[*quoting* Lopez v. United States, 373 U.S. 427 (1963) (Brennan, J., dissenting)].

5) **There is No Reasonable Expectation of Privacy for Conversations in the Back of a Police Car.** The federal courts have consistently refused to find an expectation of privacy for conversations held in the back of a police car.[41]

[41] See United States v. Turner, 209 F.3d 1198, 1200-01 (10th Cir.), *cert. denied*, 531 U.S. 887 (2000)("We conclude that under Title III or the Fourth Amendment, society is not prepared to recognize an expectation that communications in a patrol car, under facts presented here, are not subject to interception")(internal footnote omitted); United States v. McKinnon, 985 F.2d 525, 528 (11th Cir.), *cert. denied*, 510 U.S. 843 (1993)("We hold that McKinnon did not have a reasonable or justifiable expectation of privacy for conversations he held while seated in the back seat area of a police car"); United States v. Clark, 22 F.3d 799, 802 (8th Cir. 1994)("We conclude that a person does not have a reasonable or legitimate expectation of privacy in statements made to a companion while seated in a police car").

b. **Consensual Monitoring by one or more parties to the communication.** Title 18 U.S.C. § 2511(2)(c) provides that "[i]t shall not be unlawful ... for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception." This section permits "government agents, acting with the consent of a party to a communication, to engage in warrantless interceptions of telephone communications, as well as oral and electronic communications." USAM, Chapter 9-7.301. This also reflects case law. [42]

1) **Department of Justice Policy.** On January 20, 1998, the Attorney General promulgated guidelines for the investigative use of consensual monitoring by law enforcement agencies within the Executive Branch. These guidelines are enumerated in the United States Attorney's Manual, Chapter 9-7.302.

a) **Oral Authorization for Most Consensual Monitoring.** On May 30, 2002, the Department of Justice issued a memorandum revising the obligations of a law enforcement officer to seek the authorization of an Assistant United States Attorney prior to conducting a consensual monitoring. Previously, the Justice policy required "concurrence or authorization for consensual monitoring by the United States Attorney, an Assistant United States Attorney, or the previously designated Department of Justice attorney for a particular investigation (in short, a 'trial attorney')." DOJ Memorandum of May 30, 2002. Now, ~~"prior to receiving approval for consensual monitoring from~~ the head of the department or agency (or his or her designee)~~" to which the law enforcement officer belongs,~~ that plans to conduct consensual monitory must first obtain from a designated Department of Justice attorney ~~must provide~~ "advice" that the monitoring is lawful. Further, the memorandum notes that no Assistant United States Attorney contacts, consent, advice or approval is required to consensually monitor telephone or radio communications.

[42] *See* United States v. White, 401 U.S. 745 (1972); United States v. Tangeman, 30 F.3d 950 (8th Cir.), *cert. denied*, 513 U.S. 1009 (1994)("Neither a defendant's Fourth Amendment rights nor section 2511(2)(c) are violated when a defendant's conversation with a government informant is recorded with the consent of the informant").

b) **Special and Sensitive Cases - Written Approval of Department of Justice Required.** In certain sensitive and/or high visibility cases, the Department of Justice requires written approval before an oral communication can be monitored without the consent of all parties to the communication. This approval must come from the Director or Associate Directors of the Office of Enforcement Operations, Criminal Division, Department of Justice. The sensitive situations requiring written approval are when:

(1) The monitoring relates to an investigation of a Congressman, a Federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;

(2) The monitoring relates to an investigation of a Governor, Lieutenant Governor, or Attorney General of any State or Territory, or a judge or justice of the highest court of any State or Territory, and the offense investigated is bribery, conflict of interest, or extortion relating to the performance of his or her official duties;

(3) Any party to the communication is a member of the diplomatic corps of a foreign country;

(4) Any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;

(5) The consenting or non-consenting party is in the custody of the Bureau of Prisons or the United States Marshals Service; or

(6) The Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the United States Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

2) **Special Limitations on the Use of Consensual Monitoring.** "When a communicating party consents to the monitoring of his or her oral communications, the monitoring device may be concealed on his or her person, in personal effects, or in a fixed location. When engaging in consensual monitoring, the law enforcement agency involved must ensure that the consenting party will be present at all times when the device is operating." USAM, Chapter 9.7-302 (Part IV).

a) **Placing the Device on the Person.** The monitoring device may be placed on the person of the consenting party but the consent given by the party must be voluntarily given. If it is, the party (be it an undercover agent of a confidential informant) may record any conversations he has with the suspect. *See* Hoffa v. United States, 385 U.S. 293 (1966)(An expectation of privacy does not attach to a "wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

b) **Placing the device on an unwitting person.** In Shell v. United States, 448 F.3d 951 (7th Cir. 2006), agents obtained a Title III order to intercept the conversation of a prisoner and named visitors. Prison officials placed the listening device in the visitor's badge without the visitor's knowledge. The court found the placement of the device lawful.

c) **Placing the Device in a Fixed Location.** The monitoring device is not required to be on the person of the consenting party. Instead, in many instances, it is necessary to fix the device in a specified location (e.g., a hotel room where the confidential informant and the suspect are to meet). When the device is placed in a fixed location, two aspects of the installation and monitoring must be considered.

(1) **Obtaining a Warrant to Install the Device.** First, it may be necessary to obtain a search warrant for the installation of the device, depending on the circumstances. For example, where a confidential informant rents a hotel room and consents to having the device placed in the room, no warrant would be required for the installation.

(2) **Monitoring May Only Be Done When the Consenting Party is Present.** Second, the device may not be monitored when the consenting party to the conversation is absent, even temporarily. *See* United States v. Yonn, 702 F.2d 1341 (11th Cir.), cert. denied, 464 U.S. 917 (1983) (Upholding use of recording device fixed in motel room where recordings were made only when confidential informant was in the room). *See also* United States v. Nerber, 222 F.3d 597, 604-605 (9th Cir. 2000)(While case dealt with use of video surveillance when consenting informant was not present in a motel room, court noted that "although no federal statute regulates the government's use of video surveillance, the existence of a law which prohibits the warrantless use of audio surveillance on a citizen alone in another person's hotel room is strong evidence that society is not prepared to accept the warrantless use of an even more intrusive investigative tool in the same situation").

12. **Forms of Electronic Communications Excluded From Title III.** As was previously noted, the ECPA extended Title III protection to "electronic communications." However, the following types of communications were specifically excluded from this protection. Thus, a Title III court order is not required for interception of these types of electronic communications:

a. **Tone-Only Pagers.** The term "electronic communication" does not include "any communication made through a tone-only paging device." 18 U.S.C. § 2510(12)(B). *See also* Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995) (noting scope of definition of "electronic communications" "was … narrowed by excluding several types of communication that fell within the general description, including … 'any communication made through a tone-only paging device'").

b. **Beepers, Transponders, and Tracking Devices.** The term "electronic communication" does not include "any communication from a tracking device (as defined in section 3117 of this title)." 18 U.S.C. § 2510(12)(C). The rules governing installation and use of beepers and transponders will be discussed more fully below.

c. **AM/FM Radio Station Broadcast**, Title 18 U.S.C. § 2511(2)(g)(ii)(I);

d. **Citizen Band Radios**, Title 18 U.S.C. § 2511(2)(g)(ii)(III);

e. **Walkie-Talkies**, Title 18 U.S.C. § 2511(2)(g)(ii)(III);

f. **Ham Radios**, Title 18 U.S.C. § 2511(2)(g)(ii)(III).

g. **Video-Only Surveillance in Public.** This type of surveillance is not regulated by Title III, but is regulated by the Fourth Amendment. *See* United States v. Koyomejian, 970 F.2d 536 (9th Cir.), cert. denied, 506 U.S. 1005 (1992)("Although domestic silent video surveillance is not regulated by statute, it is of course subject to the Fourth Amendment").

Nonetheless, as will be discussed more fully in EPO #4, below, some federal circuits have held in case law that some of the requirements of Title III do apply when video-only surveillance is being used in a place where a reasonable expectation of privacy exists.

## B. EPO # 2: IDENTIFY THE FEDERAL REQUIREMENTS GOVERNING THE USE OF ELECTRONIC DEVICES THAT TRACK THE MOVEMENTS OF SUSPECTS

1. **Background.** "The use of transmitting devices and/or infra-red tracking devices in the detection of crime is a valuable and well-accepted law enforcement tool." [43] Under federal law, electronic tracking devices are defined as "electronic or mechanical device[s] which permit the tracking of the movement of a person or object." Title 18 U.S.C. § 3117(b).

2. **Beepers**. A commonly used tracking device is a "beeper" or "transponder." When the term beeper or transponder is used, it usually refers to a transmitter than sends a signal that can be read by radio-frequency direction finders. In general law enforcement applications, this technology can only tell the user the general direction that the beeper or transponder is located and some rough idea whether the beeper is moving closer or farther away. Under ideal conditions, beepers have a range of roughly a mile. [44] Beepers can also be configured in controlled delivery applications to send a special tone when a specially wired package has been opened.

3. **GPS (Global Positioning Satellite)**. Far more capable are GPS devices. By receiving signals from satellites, GPS receivers calculate their own location on earth.

   a. The simplest form of GPS installation consists of a GPS receiver, antenna, power supply, and logging device that record where the vehicle has moved. Depending on the equipment, the data on the logging device can be remotely obtained electronically or may require physically retrieving the device to access the data. The devices could be in single or multiple units.

   b. Live tracking applications will require the above items plus a transmitter and separate antenna to transmit the GPS location information.[45]

---

[43] In re Application of the United States ("White Truck"), 155 F.R.D. 401, 402 (D. Mass. 1994).

[44] See also this definition: "Colloquially known as a 'beeper' ... the transponder is a small, battery-operated electronic device which emits periodic signals which can be picked up on radio frequency, and which establish the approximate location of the object to which the transponder is attached by providing a line of position, to the left or right, between the transmitter and the intercepting equipment." *Attachment or Use of Transponder (Beeper) to Monitor Location of Airplane or Automobile as Constituting "Search" Within Fourth Amendment*, 57 A.L.R. Fed. 646 (2000). *See also* United States v. Knotts, 460 U.S. 276 (1983)(defining a "beeper" as "a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver").

[45] For an overview of how GPS works and many other technical details, to include GPS tracking technology, go to: http://en.wikipedia.org/wiki/GPS (last visited June 5, 2010). For an excellent survey of GPS uses and applicability to law enforcement, *see* John S. Ganz, *Comment: It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Tracking Devices*, 95 J. CRIM. L. & CRIMINOLOGY 1325 (Summer 2005). *See also, Government Surveillance in Context, for E-mails, Location, and Video: Personal Privacy in the Face of Government Use of GPS, 3 ISJLP 473 (2008)*.

4. **Electronic Tracking Devices Are Regulated By the Fourth Amendment, Not Title III.** Title III does not regulate the installation or monitoring of a beeper or transponder.[46] Instead, the installation and monitoring of a beeper or transponder is governed by basic Fourth Amendment principles.[47]

**Except where noted, the remainder of this EPO will address the use of GPS used to track vehicles as that is the most common application today. The principles of the Fourth Amendment as to GPS vehicle tracking apply to all forms of tracking devices.**

5. **Fourth Amendment Compliance is a Two-Part Test.** In assessing whether using a tracking device meets the requirements of the Fourth Amendment, it is easiest to analyze the issue by breaking it down into two separate questions:

   a. Did the **installation** of the tracking device comply with the Fourth Amendment?

   b. Did the **monitoring** (tracking) of the tracking device comply with the Fourth Amendment?

6. **Overview: Analyzing the Installation of the Tracking Device and Monitoring Considerations.**

   a. **Installation of the device**. If no governmental intrusion into a protected area occurs in the installation, then no "search" has occurred and the Fourth Amendment is not implicated. However, if the device is installed in a location where a reasonable expectation of privacy exists, the intrusion necessary for the installation would qualify as a "search" under the Fourth Amendment. As such, the installation must be accomplished either with a search warrant or with an exception to the warrant requirement (e.g., consent).

**For the remainder of this EPO, it will be assumed that neither consent nor another exception to the warrant requirement exists. The focus of the presentation will be the covert installation and monitoring of tracking devices.**

   b. **Monitoring the device**. If the tracking device will be used to follow a person into an REP area, then a warrant is required.

7. **Requirement for a warrant – simplified:**

   a. **Rule 1:** If the vehicle is located in such a location that an intrusion into an REP area is required to access the vehicle, then a warrant will be required to install the tracking device.

   b. ***Rule 2***: If installing the device in or on the vehicle requires an intrusion ***into*** the vehicle, then a warrant will be required to install the tracking device.

---

[46] 18 U.S.C. § 2510(12)(C)("Electronic communication ... does not include any communication from a tracking device (as defined in section 3117 of this title").

[47] *See United States v. Knotts*, 460 U.S. 276 (1983) and *United States v. Karo*, 468 U.S. 705 (1984).

c. ***Rule 3:*** Separate from the question of installation of the device, if tracking will occur in places where a person has a reasonable expectation of privacy, a warrant is required to conduct the tracking.

8. **Rule 1 – Location of vehicle at time of installation.**

a. **Installation Requiring Intrusion into an Area Where a Reasonable Expectation of Privacy Exists.** If installation requires physically trespassing onto the curtilage of a residence or into an attached garage, the Fourth Amendment requires a search warrant or an exception to the warrant requirement.[48]

b. **Those areas where law enforcement officers have the right to be (public places) are not REP places.** So, vehicles parked on public streets, in apartment parking lots,[49] and in gated communities[50] are not located in REP places. A vehicle parked in a garage or covered carport of a residence, however, is probably within the curtilage of a home, placing the vehicle in an REP area.

[48] *See e.g.*, In re Application of the United States ("White Truck"), 155 F.R.D. at 402 n.6 (Noting Fourth Amendment not implicated unless "installation of such devices … [required] … entry into homes or other places otherwise entitled to Fourth Amendment protection"); United States v. Hufford, 539 F.2d 32 (9th Cir.), cert. denied, 429 U.S. 1002 (1976)("Had the agents not resorted to a warrant, entrance into the garage and the opening of the truck's hood would have been an invasion of an area in which Hufford had a reasonable expectation of privacy"). *But see* United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010)(Absent apparent efforts to exclude passerby from residential driveway, homeowner has no REP in it even if portion of driveway located within the cartilage; thus, warrantless installation of tracking device on suspect's car did not violate 4th Amendment.)

.

[49] *United States v. Cruz-Pagan*, 537 F.2d 554 (1st Cir. 1976) and *Cornelius v. State*, No. A03-704, 2004 Minn. App. LEXIS 149 (Minn. Ct. App. February 10, 2004).

[50] *United States v. Harris*, No. 99-5435, 2001 U.S. App. LEXIS 3918 (6th Cir. March 7, 2001) and *Wheeler v. State*, No. 05-94-01957-CR, 1996 Tex. App. LEXIS 2546 (Tex. App. June 26, 1996).

c. **Attaching tracking device to the exterior of the car is not a search. "**The defendant's contention that by attaching the memory tracking device the police seized his car is untenable. The device did not affect the car's driving qualities, did not draw power from the car's engine or battery, did not take up room that might otherwise have been occupied by passengers or packages, did not even alter the car's appearance, and in short did not "seize" the car in any intelligible sense of the word. But was there a search? The Supreme Court has held that the mere tracking of a vehicle on public streets by means of a similar though less sophisticated device (a beeper) is not a search. *United States v. Knotts*, 460 U.S. 276, 284-85, 103 S. Ct. 1081, 75 L. Ed. 2d 55 (1983)." *United States v. Garcia*, 474 F.3d 994 (7th Cir., 2007), certiorari denied, 2007 U.S. LEXIS 10567 (U.S., Oct. 1, 2007). See also *United States v. Gbemisola*, 225 F.3d 753 (D.C. Cir., 2000).

9. **Rule 2: Location on or in the vehicle.**

a. **Installation of an Electronic Tracking Device on EXTERIOR of a Vehicle.**

1) The Supreme Court has held that there is no reasonable expectation of privacy in the exterior of a vehicle.[51] In another case, the Court found that "[t]he exterior of a car…is thrust into the public eye, and thus to examine it does not constitute a 'search." These cases indicate that the installation of a tracking device on the outside of a vehicle would be permissible without a warrant because no "search" is occurring. Other courts in non-GPS situations have come to the same conclusion. [52]

2) In United States v. Moran, 349 F. Supp. 2d 425 (D.N.Y. 2005), a federal district court applied the same rationale directly to GPS tracking devices. [53]

3) See also. *United States v. Garcia*, 474 F.3d 994 (7th Cir., 2007), certiorari denied, 2007 U.S. LEXIS 10567 (U.S., Oct. 1, 2007). and *United States v. Gbemisola*, 225 F.3d 753 (D.C. Cir., 2000).

**Minority view – for use by instructors only:**

[51] *Cardwell v. Lewis,* 417 U.S. 583 (1974).

[52] *United States v. McIver*, 186 F.3d 1119 (9th Cir. 1999), cert. denied, 528 U.S. 1177 (2000); *United States v. Rascon-Ortiz*, 994 F.2d 749 (10th Cir. 1993); *United States v. Gonzalez-Acosta*, 989 F.2d 384 (10th Cir. 1993); *United States v. Muniz-Melchor*, 894 F.2d 1430 (5th Cir. 1990), cert. denied, 495 U.S. 923 (1990); and *United States v. Lyons*, 2005 U.S. Dist. LEXIS 6963 (D. Kan. 2005).

[53] See also, *United States v. Jones*, 2006 U.S. Dist. LEXIS 56473 (D.D.C. 2006)

**One federal district court judge has agreed with a magistrate judge's recommendation that reasonable suspicion is required before placing a GPS device on the exterior of a vehicle that is located in a public place. In the author's opinion, that recommendation is unsupported by any other case except in dicta or by innuendo. The chances are, however, that this issue may not receive any further appellate review because the magistrate later concluded, and recommended the federal district court judge find, that there was not only reasonable suspicion, but also probable cause (albeit no warrant) to install the tracking device. United States v. Garcia, No. 05-CR-155-C, 2006 U.S. Dist. LEXIS 4642 (W.D. Wis. February 3, 2006); United States v. Garcia, No. 05-CR-0155-C-01, 2006 U.S. Dist. LEXIS 6424 (W.D. Wis. February 16, 2006). United States v. Garcia, No. 05-CR-155-C, 2006 U.S. Dist. LEXIS 29596 (W.D. Wis. May 10, 2006).**

**Another court that addressed this issue has noted that, while the installation of a tracking device is not a "search," reasonable suspicion is still required before utilizing the device. See United States v. Webster, 750 F.2d 307 (5th Cir. 1984), cert. denied, 471 U.S. 1106 (1985)(while noting that "in United States v. Michael, 645 F.2d 252 (5th Cir.)(en banc), cert. denied, 454 U.S. 950 (1981), we decided that the attachment of a beeper to the outside of a vehicle parked in a public place does not constitute a search," the court still required reasonable suspicion to install the tracking device due to the minimal intrusion that takes place).**

**Finally, a third court that has reviewed the legal requirements for installation of a tracking device on the exterior of the vehicle has found the installation to be a "search," yet viewed the warrantless installation to be lawful so long as the officers installing the tracking device had probable cause. This conclusion was based on the lessened expectation of privacy associated with vehicles. *See* United States v. Moore, 562 F.2d 106 (1st Cir. 1977)[noting that their decision was in keeping with Supreme Court precedent in other vehicular contexts and citing Chambers v. Maroney, 399 U.S. 42 (1970)].**

b. **Installation of an Electronic Tracking Device on the Inside of Vehicle.** An individual can have a reasonable expectation of privacy in the interior of a vehicle. Thus, when a physical trespass into the interior of a vehicle is required to install the tracking device, courts have uniformly found this action to constitute a "search."[54]

10. **Rule 3: Monitoring of Tracking Device.** As with the installation of the tracking device, the legality of monitoring the device depends on whether the tracking device enters an area where an individual has a reasonable expectation of privacy.

[54] United States v. Butts, 710 F.2d 1139 (5th Cir. 1983), rev'd en banc, 729 F.2d 1514 (5th Cir. 1984), cert. denied, 469 U.S. 855 (1984)("We hold that the installation of an electronic tracking device in the interior of a vehicle or conveyance is a 'search' within the meaning of the fourth amendment."). United States v. Hufford, 539 F.2d 32 (9th Cir.), cert. denied, 429 U.S. 1002 (1976)("Had the agents not resorted to a warrant, entrance into the garage and the opening of the truck's hood would have been an invasion of an area in which Hufford had a reasonable expectation of privacy").

a. **Monitoring Electronic Tracking Devices in Areas with No REP – No warrant required.** In United States v. Knotts, 460 U.S. 276 (1983), the Supreme Court held that a radio frequency beeper may be monitored without a warrant while in a location where a defendant has no reasonable expectation of privacy. [55]

b. **Monitoring Electronic Tracking Devices in Areas with REP – Warrant required.** In *United States v. Karo*, 468 U.S. 705 (1984), the Court held that the Fourth Amendment is violated "where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house." Karo, 468 U.S. at 715.[56]

[55] In Knotts, government agents inserted a beeper in a container of chloroform. When one of Knotts' co-defendants purchased the container, the agents followed the vehicle in which the container had been placed, using both visual surveillance and the signal emitted from the beeper. After losing visual surveillance for a period, the agents ultimately traced the container to the defendant's cabin through use of the beeper. No evidence was produced that the beeper was used in any way to reveal information as to the movement of the container within the cabin, or in any way that would not have been visible to the naked eye from outside the cabin. In addressing the monitoring of the beeper on the open roads, the Court first noted that "the governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways." Id. at 281. Further, "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the co-defendant] traveled over the public streets, he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property." Id. at 281, 282. The Court concluded their analysis of the issue by noting that, "admittedly, because of the failure of the visual surveillance, the beeper enabled the law enforcement officials in this case to ascertain the ultimate resting place of the chloroform when they would not have been able to do so had they relied solely on their naked eyes. But scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise. A police car following [the co-defendant] at a distance through his journey could have observed him leaving the public highway and arriving at the cabin owned by the defendant, with the drum of chloroform still in the car." Id. at 285.

[56] The Court also remarked that in these types of cases, "the beeper tells the agent that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched. Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations, but also establishes that the article remains on the premises." Id. Because it is often difficult to determine where the instrument containing the beeper will ultimately come to rest, the Supreme Court commented in Karo that "warrants for the installation and monitoring of a beeper will obviously be desirable since it may be useful, even critical, to monitor the beeper to determine that it is actually located in a place not open to visual surveillance." Id. at 713 n.3.

c. **Knots and Karo applied to GPS cases - Tracking on public streets not 4th Amendment search.** Tracking a suspect's whom law enforcement has a reason to track as the suspect moves on public streets, as opposed to mass tracking of people, is not a 4th Amendment search. *United States v. Garcia*, 474 F.3d 994 (7th Cir., 2007), certiorari denied, 2007 U.S. LEXIS 10567 (U.S., Oct. 1, 2007). See also *United States v. Gbemisola*, 225 F.3d 753 (D.C. Cir., 2000).

11. **How to get a Warrant for a Tracking Device**

a. Federal Rule of Criminal Procedure 41 -sets forth the procedure to request and issue a warrant *if* a warrant is required.[57]

b. **Judge in District where vehicle located issues warrant – warrant good for tracking in all districts.** Rule 41(b)(4)). A magistrate judge in the district where the device will be installed may issue a warrant to install a tracking device. The issuing magistrate judge may authorize tracking in the district where the device will be installed, another district, or both.

c. **Contents of the warrant**. Rule 41(e)(2)(B). The warrant must contain the following:

1) Identity of the person or property to be tracked.

2) Identity of the magistrate judge to whom the return on the warrant will be made.

3) A reasonable period of time that the device may be used.

a) The time will not exceed 45 days.

b) Other extensions for not more than 45 days may be granted for good cause shown.[58]

4) A command that the device be installed:

---

[57] Rule 41 reflects the view that if the officers intend to install or use the device in a constitutionally protected area, they must obtain judicial approval to do so. If, on the other hand, the officers intend to install and use the device without implicating any Fourth Amendment rights, there is no need to obtain the warrant. *See e.g. United States v. Knotts*, where the officer's actions in installing and following tracking device did not amount to a search under the 4th Amendment. . . . . Amended Rule 41(d) includes new language on tracking devices. . . . . The Supreme Court has acknowledged that the standard for installation of a tracking device is unresolved, and has reserved ruling on the issue until it is squarely presented by the facts of a case. The amendment to Rule 41 does not resolve this issue or hold that such warrants may issue only on a showing of probable cause. Instead, it simply provides that if probable cause is shown, the magistrate must issue the warrant. And the warrant is only needed if the device is installed (for example, in the trunk of the defendant's car) or monitored (for example, while the car is in the defendant's garage) in an area in which the person being monitored has a reasonable expectation of privacy." Judicial Conference of the United States, *Report of the Advisory Committee on Criminal Rules*, May 17, 2005, *Committee Note*, Rules App. D-34. (internal citation omitted).

[58] If the results of the tracking device thus far disclose evidence of criminal activity,that fact should always be mentioned in the request for an extension.

a) Within 10 days or less from the time the warrant is issued, and

b) During the daytime, unless the magistrate for good cause shown authorizes another time.

5) A command that there shall be a return on the warrant.

d. **Return on Warrant**. Rule 41(f)(2). Within ten days after use of the device has ended, the officer executing the warrant must make the return to the magistrate judge specified in the warrant. The return must contain the exact dates and times of both installing the device and the period in which it was used.

1) The return must be served on the person who was tracked, or whose property was tracked, within ten days after use of the device has ended.[59]

2) Delays in the Return – Rule 41(f)(3). Upon request of the government, the magistrate judge may delay providing the notice required by the return.

## C. EPO # 3: IDENTIFY THE FEDERAL REQUIREMENTS GOVERNING THE USE OF ELECTRONIC DEVICES THAT TRACE TELEPHONE CALLS AND ELECTRONIC COMMUNICATIONS

### 1. Pen/Trap Statute - Background.

a. The federal statutes pertaining to pen register and trap and trace devices are found at Title 18 U.S.C. §§ 3121 – 3127. These statutes deal with real-time, non-consensual electronic surveillance of certain data relating to telecommunications. Prior to the USA PATRIOT Act, this statute only sought to obtain telephone numbers. Since the USA PATRIOT Act, this statute may also be used on Internet communications to identify to whom a target is sending emails as well as from whom the target receives them. Whether used with respect to telephones or Internet communications, the pen/trap statute does not authorize intercepting the *content* of the communications.

b. **Title III does not apply to the use of these devices**.[60]

### 2. Relevant Definitions from Title 18 U.S.C. §§ 3121 – 3127.

[59] Any delay in the required notification must be one "authorized by statute." *See* 18 U.S.C. § 3103a (2006).

[60] *See, e.g.*, United States Telecom Ass'n v. Federal Communications Commission, 227 F.3d 450, 453 (D.C. Cir. 2000)("The legal standard that law enforcement agencies … must satisfy to obtain authorization for electronic surveillance of telecommunications depends on whether they seek to intercept telephone conversations or to secure a list of the telephone numbers of incoming and outgoing calls on a surveillance subject's line").

a. **Pen Registers – Defined (Captures Outgoing information.)** A "pen register" is a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication …." Title 18 U.S.C. § 3127(3).

b. **Trap and Trace Devices – Defined (Captures Incoming Information.)** A "trap and trace" device is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." Title 18 U.S.C. § 3127(4).

3. **Pen Registers and Trap and Trace Devices Are Not Governed By the Fourth Amendment.** The use of pen registers and trap and trace devices is governed by Title 18 U.S.C. §§ 3121 - 3127.[61] Because there is no REP in the information obtained from these devices, their use does not implicate the Fourth Amendment.[62]

4. **Court Order or Consent required to install or use a pen register or trap and trace device.** As a general rule, "no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123." Title 18 U.S.C. § 3121(a). Of course, consent can be utilized to install and use these devices, where appropriate.

5. **Applying for a Court Order for a Pen Register or Trap and Trace Device.** An application in the Federal system for a court order requesting to install and use a pen register or trap and trace device must meet the following requirements (Title 18 U.S.C. § 3122.)

---

[61] Title 18 U.S.C. § 2511(2)(h)("It shall not be unlawful under this chapter - (i) to use a pen register or a trap and trace device...."). *See also* United States v. New York Tel. Co., 434 U.S. 159, 166 (1977)("Both the language of the statute and its legislative history establish beyond any doubt that pen registers are not governed by Title III"); United States v. Fregoso, 60 F.3d 1314, 1321 (8th Cir. 1995)("Title III makes it clear that devices which satisfy the statutory definition of pen registers or trap and trace devices … are exempted from its requirements").

[62] *See* Smith v. Maryland, 442 U.S. 735 (1979)("We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.' The installation and use of a pen register, consequently, was not a 'search,' and no warrant was required"); United States v. Hallmark, 911 F.2d 399 (10th Cir. 1990)("The installation and use of a pen register and trap and trace device is not a 'search' requiring a warrant pursuant to the Fourth Amendment")(*citing* Smith, supra).

a. **Who May Request?** The application for a court order requesting a pen register or trap and trace must be made by "an attorney for the Government." Title 18 U.S.C. § 3122(a)(1). An "attorney for the Government" is defined as that term is used in F.R.Cr.P. 54(c). Title 18 U.S.C. § 3127(5).

b. **The Form of the Request.** The application must be in writing, under oath or equivalent affirmation, and directed to "a court of competent jurisdiction"[63] which is defined as "any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated."[64]

c. **The Contents of the Application.** The application must include the following information:

1) **Identity.** The application must "identify the attorney for the Government ... making the application and the identity of the law enforcement agency conducting the investigation." Title 18 U.S.C. § 3122(b)(1).

2) **Certification.** The application must include "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." Title 18 U.S.C. § 3122(b)(2).

6. **Nationwide Nature of Pen/Trap Orders – Relevance is the Standard.** A court order authorizing the installation and use of a pen register or trap and trace device "***anywhere within the United States***" shall be issued "if the court finds that the attorney for the Government ... has certified to the court that the information likely to be obtained by such installation and use is **relevant to an ongoing criminal investigation**." Title 18 U.S.C. § 3123(a)(1).

7. **The Contents of the Court Order**. A court order for the installation and use of a pen register or trap and trace device must specify:[65]

a. **The Identity of Individual to Whose Telephone Line the Device Will Be Attached.** "[T]he identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied." Title 18 U.S.C. § 3123(b)(1)(A).

[63] Title 18 U.S.C. § 3122(a)(1).

[64] Title 18 U.S.C. § 3127(2)(A).

[65] Title 18 U.S.C. § 3123(b).

b. **The Identity of Target.** "[T]he identity, if known, of the person who is the subject of the criminal investigation." Title 18 U.S.C. § 3123(b)(1)(B).

c. **The Phone Number and Physical Location of the Line or Facility.** "[T]he attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order." Title 18 U.S.C. § 3123(b)(1)(C).

d. **A Statement of the Offense.** "[A] statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates." Title 18 U.S.C. § 3123(b)(1)(D).

e. **A Request for Provider Assistance.** "[U]pon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124...." Title 18 U.S.C. § 3123(b)(2).

8. **Court Orders (and extensions) for Pen Registers or Trap and Trace Devices Are Good for Sixty (60) Days.**

a. A court order for a pen register or trap and trace device cannot exceed 60 days. Title 18 U.S.C. § 3123(c)(1).

b. Extensions may be granted, but a new showing must be made that the requirements of Title 18 U.S.C. § 3122 have been met.

c. Extensions may be granted for a period not exceeding 60 days. Title 18 U.S.C. § 3123(c)(2).

9. **Nondisclosure of Existence of Pen Register or a Trap and Trace Device.** Title 18 U.S.C. § 3123(d) provides that "[a]n order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that:

a. **Sealed.** The order be sealed until otherwise ordered by the court; and …

b. **Owner or Provider may not disclose existence of pen or trap.** The person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached, or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

10. **Limitations on the Use of Pen Registers and Trap and Trace Devices.** A law enforcement officer should not use a pen register to obtain information beyond that necessary to record the numbers dialed (e.g., account or PIN number information entered over the telephone). This requirement is set out in Title 18 U.S.C. § 3121(c) that provides "[a] government agency authorized to install and use a pen register or trap and trace device under this chapter ... shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications." For example, a law enforcement officer should not use a pen register to obtain information beyond that necessary to record the numbers dialed (e.g., account or PIN number information entered over the telephone).

11. **Sanctions for Violating the Pen/Trap Statute.** The penalty for impermissibly installing or using a pen register or trap and trace device is a fine and/or imprisonment for not more than one year. Title 18 U.S.C. § 3121(d). The statute regulating the installation and use of pen registers or trap and trace devices contains no provision for suppression of the evidence obtained from those devices in violation of the statute.[66]

12. **Exceptions to the General Requirement of a Court Order for Use of a Pen Register or Trap and Trace Device.** There are three exceptions for "a provider of electronic or wire communication service" to the general rule that a court order must be obtained prior to installing and utilizing a pen register or trap and trace device.[67]

    a. **Operation, Maintenance, and Testing.** If the use of the device is necessary to ensure the operation, maintenance, and testing of a wire or electronic communications service, or for the protection of users of the service from abuse or unlawful use of the service.

---

[66] *United States v. Thompson*, 936 F.2d 1249 (11th Cir. 1991), cert. denied, 502 U.S. 1075 (1992)(holding that exclusionary rule does not apply to violations of the statute because, inter alia, installation and use of pen register or trap and trace device is not a search under Fourth Amendment; because Fourth Amendment not implicated, invocation of exclusionary rule is not warranted; statutory scheme enacted by Congress does not provide for suppression as a remedy for violations; and statutory violations by themselves are insufficient to justify exclusion of any evidence obtained).

[67] Title 18 U.S.C. § 3121(b).

b. **Protection from Abusive, Fraudulent, or Unlawful Service.** Where the device is used to protect the provider or a user from fraudulent, abusive, or unlawful use of that service.

c. **Consent of User.** Where the consent of the user of that service has been obtained (e.g., Caller ID).

## D. EPO # 4: IDENTIFY THE FEDERAL REQUIREMENTS GOVERNING THE USE OF VIDEO-ONLY SURVEILLANCE IN LOCATIONS WHERE AN INDIVIDUAL HAS A REASONABLE EXPECTATION OF PRIVACY

1. **The Fourth Amendment, and not Title III, governs video-only surveillance.** The use of video-only surveillance is not addressed in Title III (18 U.S.C. § 2510, et seq.) Although not covered by Title III, the use of video-only surveillance is governed by the Fourth Amendment. When a reasonable expectation of privacy exists under Katz[68] for the place where video-only surveillance is sought, a search warrant should be obtained to install and record using the device unless consent has been obtained. If no reasonable expectation of privacy exists, then no search warrant is required for the installation and monitoring of the device.

2. **There is No REP when a person wears a concealed camera in the presence of an Informant.** Without the defendant's knowledge, an informant wore a wire and a concealed camera which revealed the defendant (in the informant's presence) making false IDs. Because the defendant invited the informant into his home, the court held, the defendant forfeited his privacy interest in those activities that were exposed to the informant. United States v. Brathwaite, 458 F.3d 376 (5th Cir. 2006).

3. **Video Only Surveillance in middle school dressing room violates 4th Amendment.** In a 1983 action, school authorities were denied qualified immunity for installing hidden cameras in school gym dressing rooms where female students could be viewed in their underwear. The cameras were installed for school safety and security purposes, and the students did not know of the presence of the cameras. *Brannum v. Overton County Sch. Bd*., 516 F.3d 489 (6th Cir. 2008).

[68] Katz v. United States, 389 U.S. 347, 357 (1967).

4. **Many Courts Have Adopted Heightened Requirements for Video-Only Search Warrants.** While recognizing that Title III does not govern the use of video-only surveillance, six circuits require that search warrants for video-only surveillance meet certain higher, constitutional standards required under Title III. USAM, Chapter 9.7-200. Specifically, in addition to showing that probable cause exists to believe that evidence of a Federal crime will be obtained through the surveillance, the Second, Fifth, Seventh, Eighth, Ninth, and Tenth Circuits require the following information in order to obtain a search warrant for video-only surveillance:[69]

   a. **Necessity Statement.** A factual statement that alternative investigative methods have been tried and failed or reasonably appear to be unlikely to succeed if tried or would be too dangerous;

   b. **Minimization Statement.** A statement of the steps to be taken to assure that the surveillance will be minimized to effectuate only the purposes for which the order is issued;

   c. **Description of the Premises.** A particularized description of the premises to be surveilled;

   d. **Statement of Duration.** A statement of the duration of the order, which shall not be longer than necessary to achieve the objective of the authorization, nor, in any event, longer than 30 days, measured from the date of the order (without any 10-day grace period to begin interception, but with 30-day extension periods possible); and

   e. **Identity of Persons to be Surveilled.** The names of the persons to be surveilled, if known.

2. **DOJ Authorization is Required for Video-Only Surveillance in REP areas.** The Department of Justice (DOJ) requires that the investigative agency seeking to use court-ordered video-surveillance obtain prior approval from the appropriate DOJ official. Pursuant to Department of Justice Order No. 985-82, dated August 6, 1982, certain officials of the Criminal Division of the DOJ have been delegated to review requests to use video surveillance for law enforcement purposes when there is a constitutionally protected expectation of privacy requiring judicial authorization. Specifically, this authority was delegated to:

   a. *The Assistant Attorney General;*

   b. *Any Deputy Assistant Attorney General; and*

[69] For caselaw that supports this section of the Lesson Plain, see *United States v. Falls*, 34 F.3d 674 (8th Cir. 1994); *United States v. Koyomejian*, 970 F.2d 536 (9th Cir.), cert. denied, 506 U.S. 1005 (1992); *United States v. Mesa-Rincon*, 911 F.2d 1433 (10th Cir. 1990); United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987); *United States v. Biasucci*, 786 F.2d 504 (2d Cir. 1986), cert. denied, 479 U.S. 827 (1986); and *United States v. Torres*, 751 F.2d 875 (7th Cir. 1984), cert. denied, 470 U.S. 1087 (1985).

c. *The Director and Associate Directors of the Office of Enforcement Operations.*

*See* USAM, Chapter 9.7-200.

**Note to instructors: The below materials are BONUS and not part of the EPO. For some programs and students, this statute might be discussed because issues raised about lawful government surveillance raises questions about video voyeurism.**

3. **Video Voyeurism, 18 U.S.C. § 1801 (effective Dec 2004.)** This statute does NOT govern how law enforcement is able to conduct video surveillance, as section (c) of the statute provides, "This section does not prohibit any lawful law enforcement, correctional, or intelligence activity."

   a. Elements of the offense:

      1) Within the Special Maritime and Territorial Jurisdiction of the US,

      2) Capture of an image of a private area of an individual,

      3) Under circumstances where the person has a reasonable expectation of privacy, and

      4) Without the person's consent.

   b. Definitions:

      1) Capture means "to videotape, photograph, film, record by any means, or broadcast."

      2) Broadcast "means to electronically transmit a visual image with the intent that it be viewed by a person or persons." This would include posting it on the internet or sending it to another as an email attachment.

      3) "'A private area of the individual' means the naked or undergarment clad genitals, pubic area, buttocks, or female breast[70] of that individual."

      4) "The term 'under circumstances in which that individual has a reasonable expectation of privacy' means—

         a) circumstances in which a reasonable person would believe that he or she could disrobe in privacy, without being concerned that an image of a private area of the individual was being captured; or

[70] Defined as "any portion of the female breast below the top of the areola."

b) circumstances in which a reasonable person would believe that a private area of the individual would not be visible to the public, regardless of whether that person is in a public or private place."

c. Punishable as a Class A misdemeanor.

## E. EPO # 5: IDENTIFY THE FEDERAL REQUIREMENTS GOVERNING ACCESS TO STORED ELECTRONIC COMMUNICATIONS

1. Background.

a. The Electronic Communications Privacy Act (ECPA)[71] was enacted in 1986 as an amendment to Title III of the Omnibus Crime Control and Safe Streets Act of 1968. ~~It~~ ECPA contained two distinct parts. The first, termed the Wiretap Act, was essentially a continuation of the provisions in the old statute requiring a Title III court order for real-time, non-consensual interception of electronic communications. The second part of the act, termed the Stored Communications Access Act, outlined the requirements for obtaining wire or electronic communications when they are being stored by a network service provider (e.g., America Online). Electronic mail (e-mail) stored on a network server is the primary example of this type of stored communication.

b. **Nationwide application of warrants for stored electronic communications.** The USA PATRIOT Act expanded the scope of federal warrants for stored electronic communications. Rather than being limited to issuing such warrants only within their districts, a judicial official with "jurisdiction over the offense under investigation" may issue a warrant that can be enforced nationwide. Under this change, if a suspect in the Eastern District of Virginia had stored electronic communications on a server in California and Texas, a Federal judge in the Eastern District of VA could issue a search warrant for the stored emails in California, and Texas. Depending on the nature of the crime, Federal judges in other Districts where there is venue could also issue the same warrant.

c. Some general rules make a basic understanding of this portion of the statute possible.

1) **What information does law enforcement want?** It is important to first determine what type of information is being sought (e.g., Is the law enforcement officer seeking "basic subscriber information" or the actual "contents" of an e-mail?).

[71] Title 18 U.S.C. §§ 2701 – 2711.

2) **Then determine what type of document or process** may be utilized to compel disclosure of the information sought (Search warrant, subpoena, or court order.)

2. **Classifying the Information Sought.** There are three general types of information that a law enforcement officer may wish to obtain from a network service provider. Each of those types is defined below.

a. **Basic Subscriber Information.** "Basic subscriber information" includes the following:

1) Name;

2) Address;

3) Local and long distance telephone connection records, or records of session times and durations;

4) Length of service (including start date) and types of services utilized;

5) Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

6) Means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service…." Title 18 U.S.C. § 2703(c)(2).

b. **Transactional Records or Other Information (a catch all category).** A law enforcement officer may wish to obtain "transactional records or other information" about the subscriber. Title 18 U.S.C. § 2703(c)(1)(A) defines this type of information as "**a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications**....)." "This is a catch-all category that includes all records that are not contents, including basic subscriber information." *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at 83. Examples of "transactional records or other information" include:

1) Web sites visited;

2) Cell-site data for cellular telephone calls; and

3) E-mail addresses of other individuals with whom the account holder has corresponded (e.g., names of senders and recipients of user's e-mail).

**Instructor note: Obtaining an order for transactional information to capture email addresses will yield the historical record of *past* emails. To obtain an on-going record of the addresses of current emails as sent or received, agents should utilize a pen/trap order.**

c. **Contents.** The "contents" of a network account includes the actual files stored in the account. 18 U.S.C. § 2510(8) provides that "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." Content would include the body of the email and the subject line.

3. **The Three Basic Methods for Compelling Disclosure of the Information Listed Above.** A law enforcement officer may use three basic methods to compel disclosure of the information listed in paragraph 2(a)-(c), above. (It should be remembered that all of the information sought could be obtained through consent of the customer or subscriber.)

   a. Search Warrants;

   b. Title 18 U.S.C. § 2703(d) Court Orders; and

   c. Subpoenas.

4. **What Information Can Be Obtained Using Each Legal Method.** The legal method that must be utilized in any given case depends on the type of information the law enforcement officer is seeking. A law enforcement officer may always seek the consent of the customer or subscriber; however, there are occasions where consent is not sought for some reason. ***Listed below are the minimum legal methods that can be used to compel production by the network service provider of the specific information sought. It should be remembered that "[o]ne feature of the compelled disclosure provisions of the ECPA is that greater process generally includes access to information that can be obtained with lesser process.*** Thus ... a search warrant can compel the production of everything that a § 2703(d) order [or subpoena] can compel...." *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at 85.

a. **Obtaining Basic Subscriber Information - Subpoena.** This type of information may be obtained using a subpoena. Pursuant to Title 18 U.S.C. § 2703(c)(2), a law enforcement officer may compel a network service provider to provide basic subscriber information "when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena." (*See* Attachment 1 for "Sample Subpoena Language.")

1) **What Types of Subpoenas May Be Used to Obtain Basic Subscriber Information?** The following types of Federal subpoenas are authorized for obtaining basic subscriber information:

a) Federal Grand Jury subpoenas;

b) Federal trial subpoenas;

c) Administrative subpoenas authorized by a Federal statute (e.g., subpoenas authorized by § 6 (a)(4) of the Inspector General Act).

2) **Prior Notice is not Required.** When using a subpoena to obtain basic subscriber information, the government is not required to provide notice to the subscriber or customer. Title 18 U.S.C. § 2703(c)(3).

b. **Obtaining Transactional Records or Other Information.** To obtain transactional records or other information, a law enforcement officer may use a court order issued pursuant to Title 18 U.S.C. § 2703(d).

1) **Who May Issue the Order?** A court order under Title 18 U.S.C. § 2703(d) may be issued by "a court of competent jurisdiction." In the Federal system, this would include:

a) A Circuit Court of Appeals judge;

b) A District Court judge; and

c) A Magistrate judge.

2) **“Specific and Articulable” and “Relevant and Material” Facts Must Be Shown to Obtain a § 2703(d) Court Order.** To obtain a § 2703(d) court order, the law enforcement officer must “offer **specific and articulable facts** showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are ‘relevant and material’ to an ongoing criminal investigation.” (*See* Attachments 1 and 2 for “Sample Title 18 U.S.C. § 2703(d) Application for Court Order” and “Sample Title 18 U.S.C. § 2703(d) Court Order.”)

3) **Prior Notice is not Required.** Again, there is no requirement that the government provide prior notice to the customer or subscriber before compelling the disclosure of transactional records or other information.

c. **Obtaining the Contents of Wire or Electronic Communications.** A network service provider may be compelled to provide the actual contents of wire or electronic communications held in storage in different ways, depending on (1) whether the e-mail has been retrieved (opened) and (2) the length of time the communication has been held in storage.

1) **Obtaining Unopened Communications in Storage for 180 Days or Less – Search Warrant.** To obtain the contents of an unopened wire or electronic communication in storage (e.g., an e-mail) for 180 days or less, the government must obtain a **search warrant.** Title 18 U.S.C. § 2703(a).

a) **No Prior Notice is Required.** When a search warrant is used to compel the production of information, no prior notice to the customer or subscriber is required.

b) **Delayed Notice by Network Service Provider.** Further, pursuant to Title 18 U.S.C. § 2705(b), the government may apply for a court order commanding the network service provider “not to notify any other person of the existence of the warrant....”

(1) **The Requirements for Getting Notice Delayed.** A delayed notice request shall be entered if the court determines that "there is reason to believe that notification of the existence of the warrant ... will result in:

(a) Endangering the life or physical safety of an individual;

(b) Flight from prosecution;

(c) Destruction of or tampering with evidence;

(d) Intimidation of potential witnesses; or

(e) Otherwise seriously jeopardizing an investigation or unduly delaying a trial."

Title 18 U.S.C. § 2705(b).

(2) **How Long May Notice Be Delayed?** There is no specific period established for how long a network service provider may be precluded from providing notice to the customer or subscriber after service of a search warrant. Instead, Title 18 U.S.C. § 2705(b) provides that such an order may be issued "for such period as the court deems appropriate."

2) **Obtaining Retrieved (Opened) Communications and Those in Storage for More Than 180 Days – Minimum "paper" is a subpoena.** To obtain the contents of a wire or electronic communication that has (1) been retrieved (opened) or (2) been in storage for more than 180 days, a law enforcement officer has three options, each with strengths and weaknesses. Title 18 U.S.C. § 2703(b).

a) **Search Warrant.** A search warrant issued pursuant to F.R.Cr.P. § 41 by a court with jurisdiction over the offense will allow a law enforcement officer to compel the production of the contents of wire or electronic communications that have been retrieved or have been kept in storage for more than 180 days (whether retrieved or not). When a search warrant is utilized, the notice requirements outlined in paragraphs 1(a) and (b), above, apply.

b) **Title 18 U.S.C. § 2703(d) Court Order.** To obtain the contents of a wire or electronic communication that has been retrieved or held in storage more than 180 days (whether retrieved or not), a law enforcement officer may use a court order issued pursuant to Title 18 U.S.C. § 2703(d), provided that certain notice requirements are met or excused.

(1) **Notice is Required.** Title 18 U.S.C. § 2703(b)(1)(B)(ii) requires that the government provide prior notice to the customer or subscriber before using a court order to obtain the contents of a wire or electronic communication in storage more than 180 days. However, notice may be delayed in appropriate circumstances.

(2) **Delaying the Required Notice.** Pursuant to Title 18 U.S.C. § 2705(a)(1)(A), the government may request that the prior notice requirement be delayed. "In such cases, agents generally will obtain this order by including an appropriate request in the agents' § 2703(d) application and proposed order...." *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at 89.

(a) **The Requirements for Obtaining Delayed Notice.** The request for delayed notice will be granted, "if the court determines that there is reason to believe that notification of the existence

of the court order may have an adverse result...", such as:

i. Endangering the life or physical safety of an individual;

ii. Flight from prosecution;

iii. Destruction of or tampering with evidence;

iv. Intimidation of potential witnesses; or

v. Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(b) **Notice may be delayed for 90 days.** Notice to the customer or subscriber may be delayed for "a period not to exceed ninety days." Title 18 U.S.C. § 2705 (a)(1)(A).

(c) **Extensions of the Delay of Notice.** A law enforcement officer may also request extensions to the delay of notice to the customer or subscriber. Title 18 U.S.C. § 2705(4). However, each time that an extension is requested, the law enforcement officer must still justify the delay using one of the factors outlined above (e.g., flight from prosecution, etc.).

(d) **Expiration of the Delayed Notice Period.** "Upon expiration of the delayed notice period, the statute requires the government to send a copy of the request or process along with a letter explaining the delayed notice to the customer or subscriber." *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at 86; Title 18 U.S.C. § 2705(a)(5).

(3) **Delayed Notice by Network Service Provider.** As with a search warrant, the government may, in certain circumstances, pursuant to Title 18 U.S.C. § 2705(b), apply for a court order precluding the network service provider from notifying the customer or subscriber of the existence of the court order "for such period as the court deems appropriate."

c) **Subpoena.** Finally, the government may obtain wire or electronic communications that have been retrieved or held in storage for more than 180 days (whether retrieved or not) through the use of an administrative subpoena authorized by a Federal statute (e.g., an IG subpoena), a Federal grand jury subpoena, or a Federal trial subpoena. Title 18 U.S.C. § 2703(b)(1)(B)(i). (*See* Attachment 4 for "Sample Subpoena Language"). Again, however, prior notice is required, unless the delayed notice provisions of the statute have been met.

(1) **Prior Notice is Required.** Title 18 U.S.C. § 2703(b)(1)(B) requires that the government provide prior notice to the customer or subscriber before using a subpoena to obtain the contents of a wire or electronic communication in storage more than 180 days. However, notice may be delayed in appropriate circumstances.

(2) **Delaying the Required Notice.** When using a subpoena, Title 18 U.S.C. § 2705(a)(1)(B) allows notice to be delayed for a period not to exceed ninety days "upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result..."

(a) **Supervisory Official.** This is defined as "the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office." Title 18 U.S.C. § 2705(6).

(b) **Adverse Result.** An "adverse result" includes:

i. Endangering the life or physical safety of an individual;

ii. Flight from prosecution;

iii. Destruction of or tampering with evidence;

iv. Intimidation of potential witnesses; or

v. Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) **Extensions of the Delay of Notice.** Upon request, the court may delay notice for successive ninety-day periods, as long as the requirements of a supervisory official and an adverse result are present.

(4) **Expiration of the Delayed Notice Provisions.** Once the delayed notice provisions have expired, notice must be made to the customer or subscriber as required by Title 18 U.S.C. § 2705(a)(5).

(5) **Delayed Notice by the Network Service Provider.** Again, in certain circumstances, Title 18 U.S.C. § 2705(b) precludes the network service provider, for a period determined by the court to be appropriate, from notifying the customer or subscriber of the existence of the subpoena.

5. **2703(f) Preservation Orders - Ensuring the Preservation of Evidence.**

a. Federal law does not require that internet service providers keep records of stored electronic communications for any particular period of time. Consequently, during the time that agents are obtaining a subpoena, search warrant or court order, the internet service provider could delete the records or data as part of their ordinary course of business.

b. The first step law enforcement officers should take when attempting to obtain data or records pursuant to the Stored Electronic Communications Act is to obtain a "2703(f) preservation order" under 18 U.S.C. § 2703(f)(1). When such an order is issued, a network service provider must, upon request of a law enforcement officer, "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or further process." These records must be retained for "for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity." Title 18 U.S.C. § 2703(f)(2). (*See* Attachment 3 for "Sample Language for Preservation Request Letter under Title 18 U.S.C. § 2703(f)").

c. Law enforcement officers, without judicial intervention or assistance, may issue 2703(f) orders. The order only directs that the evidence not be destroyed, but does not give access to the records themselves.

d. These orders are NOT prospective – they preserve only what exists at the time the letter is issued and not what will come into existence after the letter is issued.

## F. EPO # 6: IDENTIFY THE APPLICATION OF THE BEST EVIDENCE RULE AND THE RULE OF AUTHENTICATION TO RECORDINGS.

**Note to instructors – This EPO is taught in only a very few programs.**

Resources:1. Volume 2 of "Wiretapping and Eavesdropping," second edition.

2. 1-4 Courtroom Criminal Evidence 1-4 § 408, Matthew Bender & Company (2005).

3. 5-RULE 901 Federal Rules of Evidence Manual § 901.03, Matthew Bender & Company (2005).

4. Admissibility of Sound Recordings As Evidence In Federal Criminal Trial, 10 L. Ed. 2d 1169 (2006).

5. Omission Or Inaudibility Of Portions Of Sound Recording As Affecting Its Admissibility In Evidence, 57 A.L.R.3d 746 (2006).

6. Imwinkelried, Edward J., Evidentiary Foundations 5th Edition (2002) pp. 111-117 (hereinafter Imwinkelried).

Note: The Federal Rules of Evidence will ordinarily be abbreviated just "FRE".

For a more detailed discussion of the points discussed below, the instructor should consult the above references.

### 1. Introduction

a. **"Recordings" versus "audio recordings**." Prior versions of this EPO addressed "tape recordings." This has been changed to "audio recordings" because in recent years, digital recording to flash memory, CD, or other media has replaced tape. In addition, as video devices become smaller and their value in court greater, law enforcement frequently captures audio and video simultaneously.

b. **Applicability to video recordings**. The same principles that apply to audio recordings will also apply to video except where noted in the lesson plan.

c. **"Capture."** "Capture" is frequently used to describe the taking of a digital photo or making a digital recording whether audio or video or both.

d. **Links and case cites.** The links used in this lesson plan take users directly to Lexis.

2. **Scope of this EPO – excludes questions concerning the lawfulness of obtaining the recording.** This EPO assumes that the recording was lawfully obtained by whatever means: Title III wiretap order, warrant, other court order, consent of one or more parties to the conversation, public (no REP) conversations, or otherwise in compliance with the US Constitution. Earlier EPOs in this lesson plan address how to comply with Constitutional and other requirements to lawfully obtain the recording.

3. **CAUTION – Real Time Monitoring - Video recordings.**

   a. This EPO was designed for situations when there is a witness to the recording available to testify for the government. That witness could be an agent, an informant, friendly witness, or someone who is monitoring the conservation real-time as it is recorded. When audio and video is captured at the same time, this EPO fully applies to video as well as audio.

   b. It is common in video-only applications that there is neither real-time monitoring nor a witness such as a public surveillance video of a murder. This EPO would NOT address the authentication requirements in such a situation because there is no authenticating witness.

4. **Value of recordings to a criminal case**.

   a. Sound recordings are valuable in a criminal trial, and when properly authenticated, can be admitted as:

      1) Independent evidence of a crime or other event.
      2) Evidence of a defendant's confession or admission.
      3) Corroboration of a witness' testimony.
      4) Present memory refreshed.
      5) Impeachment of a witness' testimony.

   b. **"Most reliable evidence."** The Supreme Court long ago recognized the admissibility and evidentiary value of recordings in a criminal case. In Lopez v. United States, 373 U.S. 427 (U.S. 1963), the Court observed, "the [recording] device was used only to obtain the most reliable evidence possible of a conversation in which the Government's own agent was a participant and which that agent was fully entitled to disclose." The same case rejected the defendant's argument that he had a constitutional right to rely on possible flaws in the agent's memory, or to challenge the agent's credibility without being beset by corroborating evidence that was not susceptible of impeachment.

5. **Necessity to authenticate evidence in court**. Only evidence that is authentic (that is, evidence for which a foundation has been laid) is admissible. To that end, it is important for officers to understand fundamental evidentiary foundational requirements (authentication) so evidence is collected, handled and preserved in a way to enhance its chances of being admitted.

6. **The Process – Role of the Agent, AUSA, Judge and Jury.**

   a. **The role of the agent – make good recordings and preserve them.** The agent has several duties to assist in getting recordings admitted at trial:

      1) Follow procedures in using the equipment.

      2) Make technically audible, intelligible and complete recordings.

      3) Preserve the recordings so they are not lost or altered and can be authenticated in court.

      4) Keep records about the events leading up to the recording, making the recording, and preserving the recording.

      5) Be prepared to testify about the above to lay a foundation to authenticate the recordings.

   b. **The role of the AUSA – with the agent's testimony, lay a foundation.** The AUSA is responsible for presenting the case and carrying the burden to authenticate the recordings and get them admitted at trial. When agents perform their duties well, the AUSA's job is easier.

   c. **Role of the trial judge - decide admissibility of evidence.** The trial judge decides whether the recording will be admitted so the jury may consider it. Thus, it is the duty of the trial judge to determine whether the recordings (and where applicable, transcripts) will go to the jury. This is ordinarily done by having the judge listen to the recordings unless the parties stipulate (agree) to their admissibility. 10 L. Ed. 2d 1169, § 6b. When attempting to have recordings or transcripts admitted, the trial judge is the person to be convinced that a foundation has been laid.

   d. **The duty of the jury – weigh the evidence**. The jury will decide, however, whether to believe what is presented to them and the weight to be given to that evidence. So even when the trial judge admits evidence, it is no guarantee that the jury will place any weight on it. By working to ensure the quality and authenticity of the evidence acquired in each criminal case, the Agent will enhance the likelihood that the jury will positively view and weigh the evidence offered by the government.

7. **Checklist approach versus FRE 901(a) authentication.** Prior to the Federal Rules of Evidence, the federal courts tended to use a "checklist" approach in determining authenticity. This approach resulted in cases that contained usually 7 factors, 6 of which will be discussed *infra*. (Factor 7 concerns the lawfulness of making the recording which is beyond the scope of this EPO.)

   a. **From the Pre-FRE approach to "modern" cases**. Since the adoption of the Federal Rules of Evidence, the "checklist cases" have been largely disbanded in favor of the simpler Federal Rule of Evidence authentication approach in FRE 901(a). From this approach, it appears well-settled that:

      1) Authentication using the standard of authentication in FRE 901(a) is the law, and whether a party can lay a foundation meeting the standard is for the judge to decide.[72]

      2) Slavishly meeting the checklist factors is unnecessary to authenticate a recording provided FRE 901(a) is satisfied.

      3) Satisfying FRE 901(a) also tends to satisfy the checklist factors.

      4) The checklist factors still remain useful because to satisfy the factors also tends to satisfy FRE 901(a).[73]

   b. **Preview of Discussion**. This lesson plan will first describe the authentication process of Federal Rule of Evidence 901(a), and the major elements that the government must prove to authenticate a recording. The checklist factors will then be discussed along with commentary on how they might be satisfied. Finally, this lesson plan will explore specific authentication issues and the use of transcripts.

---

[72] Courts now hold that there is no single rigid standard for determining whether a tape recording may be admitted into evidence. See United States v. Lance, 853 F.2d 1177, 1181 (5th Cir. 1988) (federal courts do not require "conclusive proof of authenticity" before admitting tapes); United States v. Haldeman, 559 F.2d 31 (D.C. Cir. 1976) (evidence of admissibility of tapes "need not conform to any particular model"). Tapes may be authenticated by testimony describing the process or system that created the tape. See United States v. Sivils, 960 F.2d 587 (6th Cir. 1992), cert. denied, 113 S. Ct. 130 (1992); United States v. Haldeman, 559 F.2d 31 at 107-09 (D.C. Cir. 1976), or by testimony from parties to the conversation affirming that the tape contained an accurate record of what was said. See United States v. Lance, 853 F.2d 1177 (5th Cir. 1988); United States v. Sandoval, 709 F.2d 1553 (D.C. Cir. 1983), and United States v. Dale, 991 F.2d 819 (D.C. Cir. 1993) cert. denied 510 U.S. 1030 (1996). See also United States v. Singh, 922 F.2d 1169 (5th Cir. 1991) cert. denied 500 U.S. 938 (holding conclusive proof of authenticity is not a prerequisite to the admissibility of disputed evidence. Rule 901 of the Federal Rules of Evidence provides that authentication is "satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.").

[73] Some cases still mention the factors, but in the context that satisfying them tend to also satisfy FRE 901(a). United States v. Webster, 84 F.3d 1056 (8th Cir. 1996); United States v. Webster, 84 F.3d 1056 (8th Cir. 1996), and United States v. Sanchez-Gonzalez, 294 F.3d 563, 567 (3d Cir. 2002).

8. **FRE 901(a) authentication – basics. (Is there evidence to show the item is what its proponent claims?)** The rule on authentication is codified at Federal Rule of Evidence 901, which provides: "The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Note that this rule does not establish a checklist of what things must be done before the judge is satisfied the evidence "is what its proponent claims" it to be. The Federal Rules of Evidence were specifically intended not to provide for a checklist approach, but to let each judge in each case make a fact-specific decision.

9. **The bottom line authentication – Identity of the speakers and the accuracy of the recording.**

   a. FRE 901(a) authentication is satisfied when:[74]

      1) The recording accurately reproduces the conversation (audible and intelligible.)

      2) A witness testifies they heard a conversation (a party to the conversation or an operator),

      3) The parties to the conversation can be identified.

   b. Case illustrations of the general principle.

      1) Todisco v. United States, 298 F.2d 208 (9th Cir. 1961), cert. denied 368 US 989, (holding agent's identifying voices, place where the recording was made, the date and the persons present, and that the recording was accurate in as the agent had listened to it shortly after the conversations took place sufficient to authenticate the recording).

      2) United States v. Hamilton, 334 F.3d 170 (2d Cir. 2003) (recordings were adequately authenticated by a witness who heard the conversations and made the recordings, and by various parties to the conversations).

      3) *United States v. White*, 116 F.3d 903 (D.C. Cir. 1997) ("Where one witness testified at length about the process of creating the tapes and identified the originals, and where another witness confirmed the accuracy of the portions of the tapes with which he was familiar, the Government met its burden" [of authentication].).

[74] Imwinkelried.

4) *United States v. Buchanan*, 70 F.3d 818 (5th Cir. 1995) (admitting recordings where all voices were identified, there was no intimation the tape had been altered, and the testifying officer explained how the recording was made and testified to its accuracy).

c. **The person authenticating the recording does not have to speak the language used in the recording.** United States v. Rengifo, 789 F.2d 975 (1st Cir. 1986) (officer's ability to authenticate recordings did not depend on knowledge of Spanish, but upon knowledge of methods used and degree to which agents complied with methods prescribed).

10. **Are the recordings audible and intelligible?**

a. Whether a recording is *audible* is a question whether it can be heard. A recoding is *intelligible* if it can be understood. Because these two factors are so closely related, they will not be separately analyzed.

b. A recording that can be plainly heard and understood stands a favorable chance of being admitted into evidence, assuming the recording is authenticated. At the other extreme, a recording that cannot be heard and/or understood is usually, if not always, useless as evidence in the case. A more difficult situation arises, however, when the recording is only partially audible (i.e., portions of the recording can be clearly heard and understood, while other portions fail to meet one or both of these prerequisites). These types of recordings raise additional issues that a trial judge must confront before ruling on the admissibility of the recording.

11. **Recordings That Are Partially Inaudible – A question of trustworthiness of the recording as a whole.**

a. **Partially audible or unintelligible recordings, like partially audible or intelligible conversations, are admissible**. *United States v. Doyon*, 194 F.3d 207 (1st Cir. 1999) (reasoning "[a]n accurate tape recording of part of a conversation is not inherently less admissible than the testimony of a witness who heard only part of a conversation and recounts the part that he heard").

b. **The general rule is that "A recording that is only partly unintelligible is admissible unless the unintelligible portions are so substantial as to render the recording as a whole untrustworthy."** United States v. Solis Jordan, 223 F.3d 676 (7th Cir. 2000). *See also* Wiretapping and Eavesdropping at 24-7, 8 ("Partial inaudibility is no bar to admissibility, unless the unintelligible portions are so substantial as to render the recording as a whole untrustworthy or would require the jury to speculate unduly.") (citations omitted); United States v. West, 948 F.2d 1042 (6th Cir. 1991), cert. denied, 502 U.S. 1109 (1992) ("Taped recordings are admissible unless the incomprehensible portions of the tapes are so substantial as to render the recordings as a whole untrustworthy")(citation omitted); and United States v. McIntyre, 836 F.2d 467 (10th Cir. 1987) (same). [75]

c. **Incomplete recordings can still be admissible when there is evidence the conversations are substantially complete**. United States v. Traficant, 558 F. Supp. 996 (D. Ohio 1983).

d. **Gaps in recording follows the same general rule as partially inaudible or unintelligible recordings.** Gaps in the recording are analyzed the same as those which are partially inaudible or unintelligible. United States v. Risken, 788 F.2d 1361 (8th Cir. 1986), cert. denied, 479 US 923 (trial court properly admitted tape recording made by informant of conversation with accused regarding contract to kill union leader, even though recording had been made without assistance of FBI and had at least eight gaps and several unidentified speakers, where informant testified tape was an accurate record of conversation, and expert testified that gaps were apparently caused by rewinding and playing back tape after recording and that unidentified voices were merely background noise) and United States v. Buzzard, 540 F.2d 1383 (10th Cir. 1976), cert. denied, 429 US 1072 (holding that recording was sufficiently authenticated to allow admission despite testimony proving theoretical possibility of erasure, even though tape lasted three minutes less than time indicated on tape, where party to conversation testified that recording was complete).

---

[75] See also United States v. Dukes, 139 F.3d 469 (5th Cir. 1998), cert. denied, 525 U.S. 894; United States v. White, 219 F.3d 442 (5th Cir. 2000);United States v. Booker, 334 F.3d 406 (5th Cir. 2003); United States v. Johnson, 767 F.2d 1259 (8th Cir. 1985); and *United States v. Ray*, 250 F.3d 596 (8th Cir. 2001) (court finding no error in the admission of a tape and transcript of the defendant's conversation with a drug buyer although there were a number of places on the tape in which the conversation was unintelligible).

12. **Enhanced recordings are generally admissible**. United States v. Madda, 345 F.2d 400 (7th Cir. 1965) (evidence established proper foundation for admission of both original tape recording which was initially inaudible, and re-recording made audible by cutting down background noises.)

a. **Generally - Enhancements to improve the quality of the recording are admissible**. "It is sometimes possible to improve the audibility of a recorded conversation by making a re-recording which filters out background noise or which is capable of greater amplification. Once the duplicate has been authenticated, it can then be played to the court and jury in lieu of the original." Fountain v. United States, 384 F.2d 624 (5th Cir. 1967), cert. denied, 390 U.S. 1005 (1968) ("The existence of a significant degree of background noise which might well have interfered with the jury's ability to understand the substance of the conversations, plus the availability of a reliable method of removing the interference by making a copy and running it through the noise suppression device sufficiently justify the admission and use of the copy.").

b. **In order to authenticate a re-recording, the following steps must be accomplished**:

1) **The original recording should NEVER be altered or changed**. Even though a laboratory may request the original be sent to them, the enhancement will be made to a copy of the recording.

2) **Offer the Original Recording Into Evidence.** The original, unaltered recording should be offered into evidence before the enhanced recording.

3) **Testimony by the Technical Expert.** A technical expert who made the re-recording should explain how he did so. His testimony should include a statement that he made no additions or deletions and did not alter the original in any way except to improve its audibility or clarity.

c. **Recordings that are enhanced may be authenticated provided no words are added to or deleted from the recording.**

1) An enhanced recording is admissible provided it meets other standards of authentication and no words are added or deleted from the recording. The enhancement process will not do this, but instead filter out noise, raise volume levels, and make what cannot be heard either more audible or intelligible.

2) Case illustrations of the general principle.

a) Iacobucci v. Boulter, 193 F.3d 14 (1st Cir. 1999) (tapes admissible where party offering the recording testified he did not alter the tape in any way, and the defendant offered no evidence in contradiction).

b) United States v. Thompson, 130 F.3d 676 (5th Cir. 1997) (no error in admitting a recording where an FBI signal processing analyst testified that the recording was made by electronically filtering out noises, such as from a public address system, on the original recording and explaining that he did not add or delete any words in making the enhanced recording).

c) United States v. Calderon-Rodriguez, 244 F.3d 977 (8th Cir. 2001) (no error in the admission of digitally enhanced recordings of intercepted conversations, where the government established that the recording device and the enhancement device were both operative at the appropriate times; that the operator of devices was competent to operate them; that the recording was authentic; and that no changes were made other than a change in volume as a result of the digital enhancement).

d) United States v. Carbone, 798 F.2d 21 (1st Cir. 1986), cert. denied, 493 U.S. 1078 (1990) (recordings were admissible although one tape had large gaps due to inaudibility caused by overlay of background noises and tape was filtered and then enhanced into new tape which was clear and understandable).

d. **The Judge decides whether to admit an enhanced recording.** If the court concludes that the re-recording is an accurate reproduction of the original, the re-recording is then admitted into evidence and played at trial. Wiretapping and Eavesdropping at 24-11, 12 [*citing* United States v. Craig, 573 F.2d 455 (7th Cir. 1977), cert. denied, 439 U.S. 820 (1978) and United States v. Gordon, 688 F.2d 42 (8th Cir. 1982)].

13. **Identification of the speakers**. A witness must testify they can identify who is on the recording. This will require a person with personal knowledge of that fact (such as a party to the recorded conversation) or another person who can identify the voices. The operator of the recording equipment who was not a party to the conversation could provide this testimony if that operator could identify the voices.

    a. **An expert is not required to identify a voice**. See FRE 901 (b)(5) that provides: "(b) By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule: .... (5) Voice identification. Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker. "

    b. **Ways to identify the speaker – minimal familiarity with the voice**. Identifying the speakers can be accomplished in a variety of ways, including direct identification testimony; direct comparison testimony; voice exemplar comparison; circumstantial evidence; and spectrographic analysis. United States v. Mansoori, 304 F.3d 635, 665 (7th Cir. 2002) ("an individual's 'minimal familiarity' will suffice to permit him to identify a speaker's voice. (W)e cannot say as a matter of law that the brief opportunity [a witness] had to hear the defendants in court was insufficient to permit his voice identification"), *cert. denied sub nom.* Cox v. United States, 538 U. S. 967 (2003).

    c. **The identification must be by someone familiar with the voice**. United States v. Degaglia, 913 F.2d 372 (7th Cir. 1990) (identity of defendant's voice was properly authenticated by testimony of government agent who identified defendant's voice that he had had verbal contact with defendant on several occasions for periods of up to one and one half hours and that defendant had very distinctive voice).

    d. **The familiarity with the voice can be obtained after the recording was made**. United States v. Watson, 594 F.2d 1330 (10th Cir. 1979), cert. denied, 444 U.S. 840.

14. **Chain of custody issues**.

a. **Once the government establishes the authenticity and accuracy of the recording, a chain of custody is not required.** The general purpose of a chain of custody is to defeat or protect against claims that the evidence has been altered or substituted. When a proper foundation can be laid that the recording is accurate, then there is no *legal* requirement for a chain of custody. Still, it is a good practice that agency chain of custody procedures be followed in handling the original recording in the event a chain of custody is needed depending on the dynamics of the trial.

b. Cases illustrating that a chain of custody is not legally required once the recording is authenticated.

1) United States v. Jadusingh, 12 F.3d 1162 (1st Cir. 1994) (once the government establishes the authenticity and accuracy of the recording, a chain of custody is not required).

2) United States v. Thomas, 294 F.3d 899 (7th Cir. 2002) ("It is well-settled that a party offering a tape recording into evidence must prove that the tape is a true, accurate, and authentic recording of the conversation between the parties involved. That standard can be established in two ways: (1) a chain of custody showing that the tapes are in the same condition as when recorded; or (2) other testimony to demonstrate the accuracy and trustworthiness of the evidence).

3) United States v. Brown, 136 F.3d 1176 (7th Cir. 1998) (affirming authenticity of tapes even though the government had not established a chain of custody, and further noting that the purpose of the chain of custody requirement is served where "a proper foundation demonstrating the accuracy and trustworthiness of the evidence is laid").

15. **The Checklist Cases - the McKeever Standard.** Remember that proving each of the "checklist" factors is not required, but being able to do so will go a long way in laying a foundation for the recordings. The seminal case on authenticating tape recordings is United States v. McKeever, 169 F. Supp. 426 (D.N.Y. 1958), rev'd on other grounds, 271 F.2d 669 (2d Cir. 1959). The McKeever factors are comprised of the following six factors pertinent to this EPO.

a. **The Device Must Be Shown To Be Operational.** The recording device must be shown capable of recording the conversation. In satisfying this factor of the test, it must generally be shown that the device was capable of making the recording, and that the actual device used was in working condition at the time the recording was made. This would suggest the device is tested and determined functional before the recording was made. United States v. Capanelli, 257 F. Supp. 2d 678 (S.D.N.Y. 2003).

b. **The Operator Must Be Shown To Be Competent.** Was the operator of the device competent to operate it? Those who operate the device should be prepared to describe their training and experience in using the device (i.e., what type of training and experience has the operator had with the device).

c. **The Recording Must Be Shown To Be a Correct Rendition.** The recording must be shown authentic and correct. This can generally be proven through the testimony of a participant in the conversation or an individual who monitored the conversation.

d. **No Changes Were Made To the Recording.**

1) **Offering party must be prepared to meet a challenge the recordings were altered.** The party offering the recording must be prepared to show that no changes, additions or deletions have been made to the recording. Again, either a party to the conversation or an individual who monitored it can testify to this portion of the foundation.

2) **Burden of going forward on party challenging the recording.** Most courts hold that before the one offering the recording is required to prove there have been no alterations, the defense must first offer some evidence of erasure or alteration. United States v. Muzychka, cert. denied, 467 US 1206.[76] , 725 F.2d 1061 (3d Cir. 1984)

e. **The Recording Has Been Preserved.**

[76] See also United States v. Blakey, 607 F.2d 779 (7th Cir. 1979) (where government established both chain of custody and correspondence between tape's version of events and recollections of eye witnesses to events; trial court properly ruled that defendant, in making conclusory allegation based upon mere suspicion that tape had been edited, had failed to rebut government's showing.) See also United States v. Morrison, 153 F.3d 34 (2d Cir. 1998) (tape recordings of accused's purportedly threatening telephone conversations were admissible--where (1) accused alleged that tapes were altered, (2) accused's expert testified that there were anomalies, edits, and pauses on three of tapes, and (3) government's expert testified that nothing on tapes indicated tampering--as contents of taped conversations were coherent and flowed logically, making it improbable that any material was deleted or added.)

1) The proponent of the recording must be able to establish that the recording has been preserved in a manner shown to the Court. There are several ways this can be done:

a) If a witness says the recording accurately reflects the conversation, this "requirement" is met.

b) If there are allegations that the recording has been erased or altered, a chain of custody document was utilized for the recording from the time it was recorded to the time it is offered at trial.

2) In the usual case, a court will not require a chain of custody unless there is some evidence offered by the opponent to the recording that the recording has been tampered with.

f. **The Speakers Must Be Identified.** The speakers on the recording must be identified, and this factor is required even in the "modern" foundation.

16. **Remember, satisfying the checklist factors also helps show FRE 901(a) authentication.**

17. **The Admissibility of Transcripts – Only as an aid, not as evidence (unless the recordings are in a language other than English.)** To assist a jury in their review of a recording, a transcript of that recording is often provided. The majority rule is that the transcripts only aid the jury in following the recording, and unless the recording itself is in a language other than English, a transcript is not a substitute for the tape. The reason for this rule is largely embodied in the Best Evidence Rule discussed *infra*.

a. **How Transcripts Can Assist a Jury.** "The need or desire for [jury access to] transcripts arises generally from two circumstances. First, portions of a recording may be relatively inaudible. Second, without the aid of a transcript, it may be difficult to identify the speakers." Wiretapping and Eavesdropping at 24-19 [*quoting* United States v. Onori, 535 F.2d 938 (5th Cir.-OLD 1976) (emphasis in original)].

b. **The Judge Determines Whether the Transcript is Presented to the Jury.** As with the admissibility of tape recordings, the trial judge is solely responsible for determining whether a transcript may be provided to the jury.[77]

[77] See United States v. Capers, 61 F.3d 1100 (4th Cir. 1995), cert. denied, 517 U.S. 1211 (1996)("Whether to allow the use of transcripts to aid in the presentation of tape recorded evidence is within the district court's sound discretion") (citation omitted); United States v. West, 948 F.2d 1042 (6th Cir. 1991), cert. denied, 502 U.S. 1109 (1992)("The decision to admit tape transcripts is ... within the sound discretion of the court").

c. **Testimony Concerning the Preparation of the Transcripts.** In any event, when transcripts are used, "the person transcribing the tapes should testify concerning the accuracy of the transcripts and the method used in transcribing the tapes."
United States v. Hughes, 895 F.2d 1135 (6th Cir. 1990). Alternatively, an individual who actually participated in the recorded conversation, or an individual who monitored the conversation, may testify as to the accuracy of the statements contained in the transcript. United States v. Clark, 986 F.2d 65 (4th Cir. 1993).

18. **The "Best Evidence" Rule.**

a. **Purpose – prevent inaccuracies**. The purpose of the "Best Evidence" rule is "to prevent inaccuracy and fraud when attempting to prove the contents of a writing") United States v. Ross, 33 F.3d 1507 (11th Cir. 1994), cert. denied, 515 U.S. 1132 (1995). The "rule" itself actually consists of a number of different rules, some of which are discussed below. As shown below, recordings are also within scope of the Best Evidence Rule.

b. **Better remembered as the "Original Writing (Recording) Rule."** The name "Best Evidence Rule" is quite misleading as it implies there is a requirement that only the best evidence of a fact is admissible. The Best Evidence Rule is best remembered as the "Original Writing (Recording) Rule."

c. **The Rules.** Among the different rules that comprise what is commonly referred to as the "Best Evidence" rule are FRE 1001, FRE 1002, FRE 1003 and FRE 1004. These rules can be summarized as follows:

1) To prove the contents of the recording, one must have the original.

2) A proper duplicate can be substituted for an original.

3) Only if the original and any duplicates (which can be substituted for an original) are unavailable, the contents of the recording can be proved by other means.

d. **The language of the Rules.**

1) **The Best Evidence Rule - Federal Rule of Evidence 1002.** The "Best Evidence" rule is outlined in FRE 1002. This rule provides that, "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress."

2) **What is an Original - Federal Rule of Evidence 1001(3).** An "original of a recording is the recording itself or any counterpart intending to have the same effect by a person executing it.

3) **Duplicates are admissible - Federal Rule of Evidence 1003.** FRE 1003 governs the admissibility of "duplicates," and provides that "[a] duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."

4) **What is a duplicate - Federal Rule of Evidence 1003(4).** FRE 1003(4) states, "***A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix***, or by means of photography, including enlargements and miniatures, *or* ***by mechanical or electronic re-recording*****,** or by chemical reproduction, ***or by other equivalent techniques which accurately reproduces the original***." (emphasis added.)

5) **When the original is unavailable. Federal Rule of Evidence 1004.** FRE 1004 governs the admissibility of other evidence to prove the contents of writings, recordings, or photographs.

e. **Remember: Duplicates of recordings are admissible to the same extent as an original** unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original. Notwithstanding this modern rule, agents should *ALWAYS* retain the original.

f. **Recordings and FRE 1002**. A prosecuting attorney has a great many ways that he or she may introduce at trial the recorded statements made by a defendant.

1) **The actual recording satisfies the Best Evidence Rule**. The prosecuting attorney may, following proper authentication, introduce the actual recordings (tape, CD, flash memory etc.) of the conversation to prove the defendant's statements. This clearly satisfies the Best Evidence Rule because the original recording is involved. FRE 1002

2) **A properly made duplicate may be used**. FRE 1003.

3) **The Best Evidence Rule does not prohibit a witness to a conversation to testify to the conversation's contents**.

   a) The prosecutor could also offer the testimony of a witness who overheard the conversation or even participated in it to prove what the defendant said. Commonly, this strategy will draw an objection from a defense attorney that the testimony of the witness violates the "Best Evidence" rule, as the recording is the true "best evidence" of what was said during the conversation. Uniformly, this type of objection has been rejected. As noted by one of these courts: "FRE 1002 is not relevant to this situation.... The intention here is not to prove the content of a recording, but rather to corroborate a conversation which the government claims to have occurred." United States v. Martin, 920 F.2d 393 (6th Cir. 1990). In other words, it is not the content of the *recording* that is being offered, but the content of the *conversation*. [78]

   b) Thus, the "Best Evidence" rule is not violated by the witness' testimony, in that the government is not attempting to prove the ***contents of the tape recording***, but rather the ***contents of the conversation*** that the witness personally overheard.

[78] FRE 1002 is "a rule applicable only when one seeks to prove the contents of documents or recordings.... Thus, if the ultimate inquiry had been to discover what sounds were embodied on the tapes in question, the tapes themselves would have been the 'best evidence.' However, the content of the tapes was not in itself a factual issue relevant to the case. The inquiry concerned the content of the conversations. The tape recordings, if intelligible, would have been admissible as evidence of those conversations. But testimony by the participants was equally admissible and was sufficient to establish what was said. United States v. Gonzales-Benitez, 537 F.2d 1051 (9th Cir. 1976), cert. denied, 429 U.S. 923 (1976)(footnote omitted).

c) If the witness were to try to offer testimony about what was actually contained on the tape, the "Best Evidence" rule may be violated, because the "best evidence" of the recording's contents is the actual recording. *See* United States v. Workinger, 90 F.3d 1409 (9th Cir. 1996).
("We, of course, are well aware of the fact that a tape recording cannot be said to be the best evidence of a conversation when a party seeks to call a participant in or observer of the conversation to testify to it. In that instance, the best evidence rule has no application at all.")(citation omitted).

g. **Transcripts In Lieu of Recordings – Subject to Best Evidence Objection.**

1) **Transcripts in lieu of the tapes are generally not admissible in the face of a Best Evidence objection**. When the government offers into evidence transcripts of a recording, but not the actual tapes, the "Best Evidence" rule may prevent introduction of the transcripts without also introducing the actual tapes. This is because the "best evidence" of the contents of the tapes is the tapes themselves, not a secondary source like the transcripts. However, "[i]f both sides stipulate that a transcript of a tape is accurate ... the [best evidence] rule provides no barriers to using the transcript in lieu of the recording, since the reason underlying the rule, i.e., assuring accuracy, has been satisfied." Wiretapping and Eavesdropping at 25-57.

2) **Lost tape but transcript exists – transcript possibly admissible.** A related scenario occurs when a tape was transcribed, then subsequently was lost or destroyed. In such situations, FRE 1004 may provide a means of getting the transcript admitted into evidence, despite the fact that it is a secondary source of the evidence.[79]

---

[79] Illustrative on this point is United States v. Ross, 33 F.3d 1507 (11th Cir. 1994), cert. denied, 515 U.S. 1132 (1995), in which recorded conversations were transcribed by the Spanish National Police. Unfortunately, following the transcription, the recordings were "destroyed in the ordinary course of business." Over objection, the district court permitted the government to offer the transcriptions of the conversations without producing the actual tape recordings. In affirming the district court's decision, the Ninth Circuit justified their decision based on FRE 1004. The court first noted that FRE 1004(1) \\FTC\DFS root\DFS root\Lesson Plans\LGD\Lesson Plans Master Folder - READ ONLY\FRE 1004.htm stated that, "where the original of a recording has been lost or destroyed, the original is not required and other evidence of its content is admissible, unless the proponent lost or destroyed the original in bad faith." Once the terms of FRE 1004 are satisfied, the party seeking to prove the contents of the recording – here the government – may do so by any kind of secondary evidence. The terms of FRE 1004 were met in this case. First, the transcripts constituted "other evidence" of the lost recordings. Second, the prosecution was not responsible for the loss or destruction of the tapes, which the Spanish National Police had destroyed in the ordinary course of business. Finally, the transcripts were admissible because the constituted evidence of the contents of the lost or destroyed recordings. *See also* Wright v. Farmers Co-op of Arkansas & Oklahoma, 681 F.2d 549 (8th Cir. 1982) and United States v. Maxwell, 383 F.2d 437 (2d Cir. 1967), cert. denied, 389 U.S. 1043 (1968) and cert. denied 389 U.S. 1047 (1968).

3) **Recordings not in English and transcribed translation exists – transcript admissible.** When the recording is not in English and is transcribed into English, the transcript is admissible in lieu of the original recording provided that:

a) The recording can be authenticated,

b) The recording is audible and intelligible, and

c) The translation was performed by a person qualified to do so.

4) **Cases illustrating the above.**

a) United States v. Garcia, 20 F.3d 670 (6th Cir. 1994) (transcript of translated conversations in Spanish where a professional translator testified to its accuracy and the defendant did not point to any inaccuracies or offer an alternative translation).

b) United States v. Briscoe, 896 F.2d 1476 (7th Cir. 1990) (tape-recorded telephone conversations conducted in Yoruba sufficiently authenticated with respect to both the identity of the speakers and the accuracy of the translations).

c) United States v. Grajales-Montoya, 117 F.3d 356 (8th Cir. 1997) (allowing transcripts of translations of tape-recorded conversations that had been conducted in Spanish without introducing the tapes).

19. **Disclosure of Technical Data.** In electronic surveillance cases, defense attorneys will often request (usually during the discovery phase) technical data concerning the equipment used to intercept and/or record a defendant's conversations. "In many of these cases, courts have faced the issue of whether a 'police surveillance privilege' exists that prohibits the disclosure of such information because disclosure would frustrate future surveillance, would educate criminals about how to avoid surveillance or would endanger the individuals who allowed or conducted it." *Police Surveillance Privilege*, 67 A.L.R.5th 149 (2001).

a. **Most Courts Have Recognized a Qualified Privilege.** The majority of courts that have addressed this issue "have recognized a qualified privilege prohibiting disclosure of the location, equipment, and techniques used during police surveillance." Typical of the rationale used by courts who have confronted this issue is United States v. Van Horn, 789 F.2d 1492 (11th Cir. 1986), cert. denied, 479 U.S. 854 (1986). In Van Horn, the court recognized a "qualified government privilege not to disclose sensitive investigative techniques." In their ruling, the court analogized this privilege to the "informer's privilege" recognized by the Supreme Court in Roviaro v. United States, 353 U.S. 53 (U.S. 1957). In sum, the court held that "... the privilege applies equally to the nature and location of electronic surveillance equipment. Disclosing the precise locations where surveillance devices are hidden or their precise specifications will educate criminals regarding how to protect themselves against police surveillance. Electronic surveillance is an important tool of law enforcement, and its effectiveness should not be unnecessarily compromised. Disclosure of such information will also educate persons on how to employ such techniques themselves, in violation of Title III."

b. **The Privilege May Be Overcome By a Showing of Need by the Defendant.** The courts have been very clear, however, that this privilege is a qualified one that "will give way if the defendant can show need for the information." This "necessity determination requires a case by case balancing process....". *See also* United States v. Harley, 221 U.S. App. D.C. 69 (D.C. Cir. 1982) and United States v. Cintolo, 818 F.2d 980 (1st Cir. 1987), cert. denied, 484 U.S. 913 (1987) (*citing* Van Horn with approval, and analogizing this issue with that presented in Harley, where court held that "a defendant seeking to learn the location of a police surveillance post should ordinarily show that he needs the evidence to conduct his defense and that there are no adequate alternative means of getting at the same point").

## G. EPO # 7: DESCRIBE WHEN COMPUTERS MAY BE SEARCHED AND/OR SEIZED WITHOUT A SEARCH WARRANT

**Important: Instructors must be careful to distinguish between searches and seizures in the electronic world. If officers have probable cause that media or a computer contains evidence of a crime, they may seize it for a reasonable period of time in order to obtain a warrant to search the computer or media (unless there is an exception, such as consent, that can be used.) That officers have the 4th Amendment authority to seize a computer or other media does not always mean that the item may be searched.**

1. **The Fourth Amendment.** As with any search or seizure issue, the starting point when dealing with computer searches is the Fourth Amendment. While search warrants issued upon a showing of probable cause are preferred by the courts, "it is well-settled under the Fourth and Fourteenth Amendments that a search conducted without a warrant issued upon probable cause is *per se* unreasonable ... subject only to a few specifically established and well-delineated exceptions." Katz v. United States, 389 U.S. 347, 357 (1967). To summarize, the search of a computer without a warrant is acceptable in one of three potential situations.

   a. **Private Searches Are Not Governed By the Fourth Amendment.** First, if the search is a private one, the Fourth Amendment is not violated.

   b. **If There is No Reasonable Expectation of Privacy, Then No "Search" Has Occurred.** Second, if the government's conduct does not intrude on an area where an individual has a "reasonable expectation of privacy" (REP), then technically no "search" has occurred and the Fourth Amendment is not implicated. Illinois v. Andreas, 463 U.S. 765, 771 (1983).

   c. **A Warrantless Search Must Be Made Pursuant to a Recognized Exception.** Third, a warrantless search will satisfy the requirements of the Fourth Amendment if the search falls within one of the "specifically established and well-delineated exceptions" to the warrant requirement. Each of these situations will be addressed below.

2. **Private Searches Are Not Governed By the Fourth Amendment.**

a. The Fourth Amendment "proscribes only governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any government official.'"[80] When a private search is conducted, the results of that private search may be made available for use by law enforcement. What law enforcement officials may not do, however, is "exceed[ ] the scope of the private search."[81] "This standard requires agents to limit their investigation to the precise scope of the private search when searching without a warrant after a private search has occurred.

b. Case examples:

1) **Search by Internet Service Provider (ISP) employees.** United States v. Kennedy, 81 F. Supp. 2d 1103, 1112 (D. Kan. 2000), the court held searches of defendant's computer by unidentified Internet user and employee of defendant's Internet provider were private searches that did not violate the Fourth Amendment.

2) **Computer repair persons**. In United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998), the court held that computer repairman's search of the hard drive of the defendant's computer was private search and did not implicate the Fourth Amendment). The same result was reached in United States v. Peterson, 294 F. Supp. 2d 797 (D.S.C. 2003), affirmed 145 Fed. Appx. 820 (4th Cir. 2005) even though a state statute required that computer repairpersons report any child pornography located on computers they repair, though the repairpersons were not required to search for same. Also, in United States v. Barth, 26 F. Supp. 2d 929, 935-37 (W.D. Texas 1998), the court held that computer repairman's initial search of defendant's computer hard drive during was a private search, but that subsequent search by law enforcement officer's exceeded the scope of the private search in violation of the Fourth Amendment).

[80] United States v. Jacobsen, 466 U.S. 109, 113 (1984)[*quoting* Walter v. United States, 447 U.S. 649, 662 (1980)].

[81] Id. at 115.

3) **No "government" search even though performed by government employee.** Search of fellow employee's personal notebook computer by fellow government employees to look for private information (instant messenger list of the notebook's owner) revealed presence of child pornography. HELD: private search because employee not looking into the computer to assist law enforcement. United States v. Inman, 558 F.3d 742 (8th Cir. Mo. 2009).

3. **Reasonable Expectation of Privacy (REP).** Katz established the standard for determining whether a reasonable expectation of privacy (REP) exists. The test for REP is two-pronged: First, the individual must have exhibited an actual (subjective) expectation of privacy; and, second, that expectation must be one that society is prepared to recognize as reasonable. If either prong of the test is not met, then no REP exists.

   a. **Computers and Expectations of Privacy.** With regard to computers, the most basic Fourth Amendment question in computer cases asks whether an individual enjoys a reasonable expectation of privacy in electronic information stored within computers ... under the individual's control. For example, do individuals have a reasonable expectation of privacy in the contents of their laptop computers, floppy disks, or pagers? If the answer is "yes," then the government ordinarily must obtain a warrant before it accesses the information stored inside.

b. **Computers as Closed Containers.** In analyzing the issue of REP in computers, courts have repeatedly analogized computers to closed containers, such as a file cabinet. To determine whether an individual has a reasonable expectation of privacy in information stored in a computer, it helps to treat the computer like a closed container, such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in a computer without a warrant if it would be prohibited from opening a closed container and examining its contents in the same situations. *See, e.g.*, United States v. Roberts, 86 F. Supp. 2d 678, 688 (S.D. Tex. 2000)(noting that "several courts have analogized the Fourth Amendment protection appropriately afforded an individual's computer files and computer hard drive to the protection given an individual's closed containers and closed personal effects"); United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991)(holding that hand-held computer "memo" book "is indistinguishable from any other closed container, and is entitled to the same Fourth Amendment protection"); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998)(court found that "Fourth Amendment protection of closed computer files and hard drives is similar to the protection it affords a person's closed containers and closed personal effects"); and United States v. Blas, 1990 U.S. Dist. LEXIS 19961 at *56 (E.D. Wis. 1990)(court held that "an individual has the same expectation of privacy in a pager, computer, or other electronic data storage and retrieval device as in a closed container ...").

4. **A Person May Lose REP In a Computer.** Although individuals generally retain a reasonable expectation of privacy in computers under their control, special circumstances may eliminate that expectation. Some of these "special circumstances" are outlined below.

a. **Exposed to the Public.** In Katz, supra, the Supreme Court made clear that "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. Thus, when an individual makes information on a computer openly available, he or she will lose any expectation of privacy in that information. For example, in United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991), a law enforcement officer looked over the defendant's shoulder to see the password used by the defendant to access a hand-held computer memo book. According to the court, the defendant had "no reasonable expectation of privacy in the display that appeared on the screen."

b. **Stolen Computers.** Generally, an individual will not have a reasonable expectation of privacy in the contents of computers they have stolen. Case illustrations:

1) **Stolen computer**. Illustrative on this point is United States v. Lyons, 992 F.2d 1029 (10th Cir. 1993), where the defendant had stolen computers and "hard disks" that were later recovered during the execution of a search warrant. The contents of the stolen disks were searched, without a warrant, and several stolen programs were discovered. The defendant claimed the warrantless search of the disks violated the Fourth Amendment, but the court disagreed. According to the court, "a search only violates a defendant's Fourth Amendment rights if a defendant demonstrates that he or she had an actual, subjective expectation of privacy in the property searched, and if the defendant establishes that society would recognize that subjective expectation as objectively reasonable. Because expectations of privacy derive in part for the right to exclude others from the property in question, lawful possession is an important consideration in determining whether a defendant had a legitimate expectation of privacy in the area searched, i.e., the hard disks." Id. at 1031 (citations omitted). Since the defendant in this case could present no evidence of any right or interest in the items seized, he "failed to meet the threshold requirement of demonstrating an expectation of privacy in the property searched." Id.

2) **Computer obtained by credit card fraud.** In United States v. Caymen, 404 F.3d 1196 (9th Cir. 2005), the defendant bought a computer by way of credit card fraud. The computer was traced to his house and seized. After it was seized, it was searched. The defendant claimed that the search of the computer (as distinguished from its seizure as fruits of a crime) was in violation of the 4th Amendment. The court held the defendant had no REP in the computer saying, "The *Fourth Amendment* does not protect a defendant from a warrantless search of property that he stole, because regardless of whether he expects to maintain privacy in the contents of the stolen property, such an expectation is not one that 'society is prepared to accept as reasonable.'"

3) **Third-Party Possession.**

a) Individuals who retain a reasonable expectation of privacy in stored electronic information under their control may lose Fourth Amendment protections when they relinquish that control to third parties. The Supreme Court has repeatedly held that individuals who divulge information to third-parties, even with the subjective expectation that the information remain private, cannot retain control over that information once it has been passed to the third-party. *See, e.g*., Hoffa v. United States, 385 U.S. 293, 302 (1966)("The risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak")(citation omitted); Smith v. Maryland, 442 U.S. 735, 743-44 (1979); and Couch v. United States, 409 U.S. 322, 335 (1973). Because computer data is "information," this line of cases suggests that individuals who send data over communications networks may lose Fourth Amendment protection in the data once it reaches the intended recipient. For example, in United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997), the defendant transmitted child pornography to an undercover law enforcement officer via an e-mail sent over the Internet. In rejecting the defendant's claim that his Fourth Amendment rights had been violated, the court noted that "an e-mail message, like a letter, cannot be afforded a reasonable expectation of privacy once that message is received." Id. at 1184.

b) **Computer Turned in for Repair.** When a person turns in a computer to a private repair person for repair, any resulting search of the computer by the private person in his private capacity is not a 4th Amendment search. (See Paragraph G 2 b 2) of this lesson plan.) In addition, the computers' owner has also given up his REP to the repair person.

c) **Subscribing to P2P networks.** P2P stands for "peer to peer" networking. This is where a person joins a group of other internet users with a common interest (such as sharing music through www.kazaa.com). Joining the P2P network permits other members of the network to access the personal computers of others members. Users can set "permissions" that limit the access other P2P members have. Once a person joins a P2P network, they lose REP in those files they have agreed to share with other members. Some P2P networks have been set up to share child pornography which law enforcement can access without a warrant by joining the network. *United States v. Shaffer*, 472 F.3d 1219 (10th Cir. 2007).

d) **Connecting a personal computer to a LAN.** When a person connects his personal computer to a LAN (local area network) that informs users that the computer is now a node on the LAN accessible to all, law enforcement on the LAN can remotely and electronically search those computers connected to the LAN. *United States v. King*, 509 F.3d 1338 (11th Cir. 2007).

5. **Exceptions to the Warrant Requirement for Computers.** Warrantless searches that fall within an established exception to the warrant requirement are Constitutional and do not violate the Fourth Amendment. Below are some of the common exceptions to the warrant requirement and how those exceptions apply to searches of computers.

a. **Consent (Generally).** "It is well-settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent."[82] In order for a consent to search to be valid, two requirements must be met: First, the consent must be given voluntarily; second, the individual giving consent must have either actual or apparent authority over the place or thing to be searched.

[82] Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973)(citation omitted).

1) **The Consent Must Be Given Voluntarily.** In order for a consent search to be valid, the consent to search must be voluntarily given. The Fourth and Fourteenth Amendments require that a consent not be coerced, by explicit or implicit means, by implied threat or covert force, and in making this determination, courts will look at the "totality of the circumstances" surrounding the giving of the consent, because "it is only by analyzing all the circumstances of an individual consent that it can be ascertained whether in fact it was voluntary or coerced."[83] Among the factors to be considered in determining whether consent was voluntarily given are the age, education, intelligence, physical and mental condition of the person giving consent; whether the person was under arrest; and whether the person has been advised of his right to refuse consent. The government carries the burden of proving that consent was voluntary. *See* United States v. Price, 599 F.2d 494, 503-04 (2d Cir. 1979).

2) **The Person Giving Consent Must Have Either Actual or Apparent Authority.** In addition to being voluntarily given, the consent to search must be given by an individual with either actual or apparent authority over the place or thing to be searched. "Actual" authority may be obtained "from the individual whose property is searched. Illinois v. Rodriguez, 497 U.S. 177, 181 (1990)(citation omitted). Additionally, consent to search may be given by a third-party "who possesses common authority over or other sufficient relationship to the … effects sought to be inspected." United States v. Matlock, 415 U.S. 164, 171 (1974). As noted by the Supreme Court in Matlock:

"*Common authority is, of course, not to be implied from the mere property interest a third-party has in the property. The authority which justifies the third-party consent does not rest upon the law of property, with its attendant historical and legal refinements…, but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched." Id. at 171 n.7.*

[83] Id.

b. **Consent and Computers.** In computer crime cases, two consent issues arise particularly often.

- First, when does a search exceed the scope of consent? For example, when a target consents to the search of a machine, to what extent does the consent authorize the retrieval of information stored in the machine?

- Second, who is the proper party to consent to a search? Do roommates, friends, and parents have the authority to consent to a search of another person's computer files?

1) **Scope of a Consent Search.** "The scope of a search is generally defined by its expressed object." Florida v. Jimeno, 500 U.S. 248, 251 (1991)[*citing* United States v. Ross, 456 U.S. 798 (1982)]. "The standard for measuring the scope of a suspect's consent under the Fourth Amendment is that of 'objective' reasonableness – what would the typical reasonable person have understood by the exchange between the officer and the suspect?" Id. (citations omitted).

2) **The Scope of a Consent Search May Be Limited.** An individual may limit the scope of any consent. Id. at 252 ("A suspect may of course delimit as he chooses the scope of the search to which he consents"). *See also* Walter v. United States, 447 U.S. 649, 656 (1980)(plurality opinion)("When an official search is properly authorized – whether by consent or by issuance of a valid warrant – the scope of the search is limited by the terms of its authorization"). In such a case, the scope of a consent search cannot exceed, either in duration of physical scope, the limits of the consent given. Should a law enforcement officer fail to comply with the limitations placed on the consent, "the search is impermissible." United States v. Strickland, 902 F.2d 937, 941 (11th Cir. 1990). *See also* Vaughn v. Baldwin, 950 F.2d 331, 333 (6th Cir. 1991).

3) **Consent to Search May Be Revoked.** An individual may also revoke his or her consent. When consent is revoked, a law enforcement officer is required to cease searching, unless another exception to the Fourth Amendment's warrant requirement is present. *See, e.g.*, United States v. Fuentes, 105 F.3d 487, 489 (9th Cir. 1997)(Suspect effectively revoked consent by shouting "No, wait" before officer could pull cocaine out of pocket).

4) **When consent is revoked after a hard drive is imaged but before that imaged is fully searched.** The defendant consented to having his computer hard drive imaged by the FBI and they did so. The FBI returned the computer to the defendant and began to search it. Later the defendant withdrew his consent. The court held that once the defendant permitted his hard drive to be copied (imaged), he lost any REP in it. *United States v. Megahed*, 2009 U.S. Dist LEXIS 24441 (M.D. Fla., 2009).

5) **Obtaining Consent to Search in Computer Cases.** Computer cases often raise the question of whether consent to search a location or item implicitly includes consent to access the memory of electronic storage devices encountered during the search. In such cases, courts look to whether the particular circumstances of the agents' request for consent implicitly or explicitly limited the scope of the search to a particular type, scope, or duration. Because this approach ultimately relies on fact-driven notions of common sense, results reached in published opinions have hinged upon subtle (if not entirely inscrutable) distinctions. Prosecutors can strengthen their argument that the scope of consent included consent to search electronic storage devices by relying on analogous cases involving closed containers. Agents should be especially careful about relying on consent as the basis for a search of a computer when they obtain consent for one reason, but then wish to conduct a search for another reason. *See* United States v. Turner, 169 F.3d 84 (1st Cir. 1999) and United States v. Carey, 172 F.3d 1268 (10th Cir. 1999). Because the decisions evaluating the scope of consent to search computers have reached sometimes unpredictable results, investigators should indicate the scope of the search explicitly when obtaining a suspect's consent to search a computer.

c. **Third Party Consent.** It is common for several people to use or own the same computer equipment. If any of those people gives permission to search for data, agents may generally rely on that consent, so long as the person has authority over the computer. In such cases, all users have assumed the risk that a co-user might discover everything in the computer, and might also permit law enforcement to search this "common area" as well. Under the Matlock approach (discussed above), a private third party may consent to a search of property under the third party's joint access or control. Agents may view what the third party may see without violating any reasonable expectation of privacy, so long as they limit the search to the zone of the consenting third party's common authority. *See* United States v. Jacobsen, 466 U.S. 109 (1984).

1) **Inquiry into an Individual's Right of Access.** This rule often requires agents to inquire into the rights of access of third party's before conducting a consent search, and to draw lines between those areas that fall within the third party's common authority and those areas outside of the third party's control. *See* United States v. Block, 590 F.2d 535, 539-42 (4th Cir. 1978).

2) **Issues Involving Password-Protected or Encrypted Files.**

a) Courts have not squarely addressed whether a suspect's decision to password-protect or encrypt files stored in a jointly-used computer denies co-users the right to consent to a search of the files under Matlock. However, it appears likely that encryption and password-protection would in most cases indicate the absence of common authority to consent to a search among co-users who do not know the password or possess the encryption key.

b) **A suspect can be compelled to produce an encryption key if there is a valid warrant to search the computer.** In re Grand Jury Subpoena (Boucher), 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009). The defendant was inspected at the border by CBP, and child pornography was found on his laptop. Unfortunately, the CBP inspector turned off the laptop, thereby re-encrypting the files seen at the border. Because the government could not break the encryption (PGP), the government sought, by grand jury subpoena, to have the defendant produce his encryption password. The defendant refused to comply, citing the 5th Amendment act of production privilege. The magistrate agreed and granted a motion to quash the grand jury subpoena. The decision was appealed to the district court, which overturned it. The district court ruled that under these facts, the discovery of the contents of the computer was a "forgone conclusion." The contents of the computer were created by the defendant voluntarily, and were not testimonial. Where the existence and location of documents are known to the government, and the evidence is properly in the government's possession, the act of producing a password to allow the government to view these images is not testimonial. Furthermore, the government did not need the password to authenticate the images.

3) **One cannot consent to searching boyfriends password protected files.** *See, e.g.,* United States v. Smith, 27 F. Supp. 2d 1111, 1115-16 (C.D. Ill. 1998) (concluding that a woman could consent to a search of her boyfriend's computer located in their house, and noting that the boyfriend had not password-protected his files). Conversely, if the co-user has been given the password or encryption key by the suspect, then she probably has the requisite common authority to consent to a search of the files under Matlock. *See generally* United States v. Murphy, 506 F.2d 529, 530 (9th Cir. 1974)(per curiam).

4) **Apparent Authority.** As a practical matter, agents may have little way of knowing the precise bounds of a third party's common authority when the agents obtain third party consent to conduct a search. When queried, consenting third parties may falsely claim that they have common authority over property. This type of situation is governed by the Supreme Court's holding in Illinois v. Rodriguez, discussed above.

5) **Specific Third Party Consent Examples**

a) **Spouses and Domestic Partners.**

(1) Absent an affirmative showing that the consenting spouse has no access to the property searched, the courts generally hold that either spouse may consent to search all of the couple's property. *See, e.g.,* United States v. Smith, 27 F. Supp. 2d 1111, 1114-16 (C.D. Ill. 1998).

(2) **Wife's consent to search husband's computer.** Agents had information that a subject had evidence of fraud on a computer at his home. They went to the subject's home to obtain consent to search the computer. The subject wasn't home, but the subject's wife was. The computer was in a public area of the home and was up and running. The Internet access account was in the wife's name and the computer was leased by the wife. Though agents did not have direct information she used the computer, what the agents knew was sufficient to establish the agent's reasonable belief the wife had apparent authority to consent to the search. United States v. Buckner, 473 F.3d 551 (4th Cir. 2007), cert. denied, 550 U.S. 913.

b) **Parents.** In some computer crime cases, the perpetrators are relatively young and reside with their parents. When the perpetrator is a minor, parental consent to search the perpetrator's property and living space will almost always be valid. When the sons and daughters who reside with their parents are legal adults, however, the issue is more complicated. Under Matlock, it is clear that parents may consent to a search of common areas in the family home regardless of the perpetrator's age. *See, e.g.,* United States v. Lavin, 1992 U.S. Dist. LEXIS 18163 at *15-17 (S.D.N.Y. 1992)(recognizing right of parents to consent to search of basement room where son kept his computer and files). When agents would like to search an adult child's room or other private areas, however, agents cannot assume that the adult's parents have authority to consent. Although courts have offered divergent approaches, they have paid particular attention to three factors:

(1) The suspect's age;

(2) Whether the suspect pays rent; and

(3) Whether the suspect has taken affirmative steps to deny his or her parents access to the suspect's room or private area.

(4) When suspects are older, pay rent, and/or deny access to parents, courts have generally held that parents may not consent. *See, e.g.,* United States v. Durham, 1998 U.S. Dist. LEXIS 15482 at *4-*12 (D. Kan. 1998)(mother had neither apparent nor actual authority to consent to search of 24-year-old son's room, because son had changed the locks to the room without telling his mother, and son also paid rent for the room). In contrast, parents usually may consent if their adult children do not pay rent, are fairly young, and have taken no steps to deny their parents access to the space to be searched. *See* United States v. Block, 590 F.2d 535, 538 (4th Cir. 1978) (mother could consent to police search of 23-year-old son's room when son did not pay rent).

c) **Adult "child" and Parental Consent**. Agents developed information that the adult suspect, who lived with his 91 year old father, had child pornography on his computer at home. When agents went to the home to seek consent, the subject wasn't home. The subject's computer was in the subject's room, the father said he felt free to go into the room when the door was open, the door to the subject's room was open, and the father consented to the search even though agents did not have other information the father used or had access to the computer other than it was accessible to the father and in the home. The subject did not pay rent, the father paid for the Internet access, and the father had access to the subject's room. The court held that the father's consent was valid. United States v. Andrus, 483 F.3d 711 (10th Cir. 2007).

d. **Consent by One Cohabitant is Invalidated when Another Present Cohabitant Objects.**

1) In Georgia v. Randolph, 126 S. Ct. 1515 (U.S. 2006), a woman gave consent to the police to search the marital home. The husband who was present objected. Police searched the house based on the wife's consent. The Supreme Court held the search was invalid because a co-habitant who was *present* objected to the search.

**Note to instructors. The law is still evolving concerning an objection by a present co-habitant after *Georgia v. Randolph*, 547 U.S. 103 (2006). With the exception of the 9th circuit, the other circuits appear uniform in applying a literal approach to the *Georgia v. Randolph* mandate that for an objection of a co-habitant to be effective to overrule consent given by other co-habitants, the objector must be a co-habitant, present, and object. (See Milazzo, Carl, *The State of Third Party Consent After Georgia v. Randolph, The Informer*, October 2008, from which several footnotes below were obtained.) This part of this lesson plan incorporates by reference LGD training on the 4th Amendment and instructors should only review consent basics and not completely re-teach it. Only the most current issues are reviewed here..**

2) **When a person who is not present at home objects to a search of a computer in the home, officers may obtain valid consent from the spouse who is at home with the computer**.[84]

3) **After one cohabitant objects, officers may return later when the objecting cohabitant is not present and obtain valid consent from a present cohabitant**.[85] This is the general rule in the circuits that have decided the matter, except for the 9th circuit.[86]

---

[84] In *U.S. v. Hudspeth, 518 F.3d 954 (8th Cir. 2008),* the police discovered child pornography on the defendant's business computer during the execution of a search warrant. He refused consent to search his home computer for additional evidence and was arrested. Other officers went to his home and, after informing his wife why he had been arrested, she refused consent to search the home. The officers then asked if they could take the home computer. She asked what would happen if she refused and was told that an officer would remain behind to make sure no evidence was destroyed while another left to obtain a search warrant. She then consented and more evidence was discovered on the home computer.

[85] *U.S. v. Groves, 530 F.3d 506 (7th Cir. 2008*). In this case, police strategically planned to avoid the presence of a potentially objecting co-tenant. Officers were initially called to the neighborhood for shots fired. Upon arrival they spoke to the defendant, a convicted felon. He admitted to shooting off fireworks but denied having a firearm and repeatedly refused consent to search his apartment. A search warrant application was denied, and officers returned to the residence three weeks later when they determined the defendant would be away at work but his live in girlfriend would be home. After she signed a consent to search form, officers discovered the necessary evidence to charge the defendant with being a felon in possession of a firearm. The court ruled that the police played, "no active role" in removing the defendant from the premises. Since he was not, "objecting at the door" as required by *Randolph*, the search was valid.

[86] *United States v. Murphy*, 516 F.3d 1117 (9th Cir. 2008) holding that "when a co-tenant objects to a search and another party with common authority subsequently gives consent to that search in the absence of the first co-tenant the search is invalid as to the objecting co-tenant."

4) **When defendant is arrested and removed from the home for reasons other than to avoid his objection, consent of a remaining cohabitant is valid**.[87]

5) In United States v. Hudspeth, 518 F.3d 954 (8th Cir. 2008)(en banc), the 8th Circuit held that the Fourth Amendment's reasonableness requirement does not require an officer, in asking a wife for consent to search a computer that she shared with her husband, to inform her of her non-present husband's earlier refusal to consent to the search of that shared computer.

6) **Girlfriend's consent to search computer containing boyfriend's hard drive.** After being arrested on an unrelated warrant, a woman granted consent to the search of her computer. Her boyfriend, who was present, objected to the agents taking his hard drive which was installed in the girlfriend's computer. The 3rd Circuit held that co-habitant assume the risk that the other may consent to that which they share access. The Court declined to extend the holding in Georgia v. Randolph to personal property and held that the boyfriend's objection was insufficient to overcome his girlfriend's consent to search her computer. United States v. King, 2010 WL 1729733 (3rd Cir. 2010).

e. **Terms of consent – search or just seize?** When obtaining consent to search a computer, agents must be careful that they are not asking simply for consent to seize or take the computer. At least one court has held that consent to take a computer with them is not the equivalent of consent to search it. United States v. Andracek, 2007 U.S. Dist. LEXIS 39177 (D. Wis. 2007) (Main opinion unpublished.)

---

[87] In *United States v. Henderson*, 536 F.3d 776 (7th Cir. 2008), the police were called to a home for a domestic assault. They met the wife outside where she told them her husband choked her and had a history of gun and drug arrests. Using a key provided by her teenage son, the officers entered the home, and the husband unequivocally ordered them out. Instead, they arrested him for domestic battery. The wife then signed a consent to search form and officers seized a number of weapons and drugs. The court held that, "Both presence *and* objection by the tenant are required to render a consent search unreasonable as to him. Here, it is undisputed that [the husband] objected to the presence of the police in his home. Once he was validly arrested for domestic battery and taken to jail, however, his objection lost its force, and [his wife] was free to authorize a search of the home." A similar result occurred in *United States v. McKerrell*, 491 F.3d 1221 (10th Cir. 2007). When officers arrived at a home to arrest the defendant on outstanding felony drug charges he quickly retreated into the home and barricaded himself inside. His wife quickly came out of the house, leaving their young child inside. After a number of telephone conversations the defendant came outside and surrendered peacefully. He was arrested and transported to the police station. Officers then asked the wife for consent to search and she signed a written authorization. Affirming the search, the court found that merely barricading oneself in a home to avoid arrest on a warrant is not the functional equivalent of an express refusal of consent to search the home.

f. **Warrantless Access by System Administrators.**

1) **Authority of system administrators**. Every computer network is managed by a "system administrator" or "system operator" whose job is to keep the network running smoothly, monitor security, and repair the network when problems arise. Their access to the systems they administer effectively grants them master keys to open any account and read any file on their systems. When investigators suspect that a network account contains relevant evidence, they may want to seek the system administrator's consent to search the contents of that account. As a practical matter, the primary barrier to searching a network account pursuant to a system administrator's consent may be statutory, not constitutional. System administrators for "provider[s] of electronic communication service to the public" are subject to the Electronic Communications Privacy Act ("ECPA"), Title 18 U.S.C. §§ 2701-11. ECPA regulates both voluntary and compelled disclosures to law enforcement of the contents of electronic communications and other account information stored by such "providers." *See* Title 18 U.S.C. § 2702-03.

2) **Compliance with ECPA may be required**. Accordingly, any attempt to obtain a system administrator's consent to search an account must comply with ECPA. To the extent that the ECPA authorizes system administrators to consent to searches, the resulting consent searches will in most cases comply with the Fourth Amendment. The first reason is that individuals may not retain a reasonable expectation of privacy in the remotely stored files and records that their network accounts contain. If an individual does not retain a constitutionally reasonable expectation of privacy in his remotely stored files, it will not matter whether the system administrator has the necessary joint control over the account needed to satisfy the Matlock test because a subsequent search will not violate the Fourth Amendment. In the event that a court holds that an individual does possess a reasonable expectation of privacy in remotely stored account files, whether a system administrator's consent would satisfy Matlock should depend on the circumstances. Clearly, the system administrator's access to all network files does not by itself provide the common authority that triggers authority to consent. In the pre-Matlock case of Stoner v. California, 376 U.S. 483 (1964), the Supreme Court held that a hotel clerk lacked the authority to consent to the search of a hotel room. Although the clerk was permitted to enter the room to perform his duties, and the guest had left his room key with the clerk, the Court concluded that the clerk could not consent to the search. If the hotel guest's protection from unreasonable searches and seizures "were left to depend on the unfettered discretion of an employee of the hotel," Justice Stewart reasoned, it would "disappear." Id. at 490. Of course, the hotel clerk analogy may be inadequate in some circumstances. For example, an employee generally does not have the same relationship with the system administrator of his company's network as a customer of a private ISP such as AOL might have with the ISP's system administrator. The company may grant the system administrator of the company network full rights to access employee accounts for any work-related reason, and the employees may know that the system administrator has such access. In circumstances such as this, the system administrator would likely have sufficient common authority over the

accounts to be able to consent to a search.

3) **Implied Consent and Pre-Computer Banner Cases.** Individuals often enter into agreements with the government in which they waive some of their Fourth Amendment rights. For example, prison guards may agree to be searched for drugs as a condition of employment, and visitors to government buildings may agree to a limited search of their person and property as a condition of entrance. Similarly, users of computer systems may waive their rights to privacy as a condition of using the systems. This is accomplished through the use of devices such as written employment policies or network "banners." Banners are written notices that greet users before they log on to a computer or computer network. When individuals who have waived their rights are then searched and challenge the searches on Fourth Amendment grounds, courts typically focus on whether the waiver eliminated the individual's reasonable expectation of privacy against the search. *See, e.g.,* American Postal Workers Union, Columbus Area Local AFL-CIO v. United States Postal Service, 871 F.2d 556, 56-61 (6th Cir. 1989)(holding that postal employees retained no reasonable expectation of privacy in government lockers after signing waivers). A few courts have approached the same problem from a slightly different direction and have asked whether the waiver established implied consent to the search. According to the doctrine of implied consent, consent to a search may be inferred from an individual's conduct. For example, in United States v. Ellis, 547 F.2d 863 (5th Cir. 1977), a civilian visiting a naval air station agreed to post a visitor's pass on the windshield of his car as a condition of bringing the car on the base. The pass stated that "[a]cceptance of this pass gives your consent to search this vehicle while entering, aboard, or leaving this station." Id. at 865 n.1. During the visitor's stay on the base, a station investigator who suspected that the visitor had stored marijuana in the car approached the visitor and asked him if he had read the pass. After the visitor admitted that he had, the investigator searched the car and found 20 plastic bags containing marijuana. The Fifth Circuit ruled that the warrantless search of the car was permissible, because the visitor had impliedly consented to the search when he knowingly and voluntarily entered the base with full knowledge of the terms of the visitor's pass. *See* id. at 866-67. Ellis notwithstanding, it must be noted that several

circuits have been critical of the implied consent doctrine in the Fourth Amendment context. Despite the Fifth Circuit's broad construction, other courts have proven reluctant to apply the doctrine absent evidence that the suspect actually knew of the search and voluntarily consented to it at the time the search occurred. *See* McGann v. Northeast Illinois Regional Commuter R.R. Corp., 8 F.3d 1174, 1179 (7th Cir. 1993)("Courts confronted with claims of implied consent have been reluctant to uphold a warrantless search based simply on actions taken in the light of a posted notice."); Securities and Law Enforcement Employees, District Council 82 v. Carey, 737 F.2d 187, 202 n.23 (2d Cir. 1984)(rejecting argument that prison guards impliedly consented to search by accepting employment at prison where consent to search was a condition of employment). Absent such evidence, these courts have preferred to examine general waivers of Fourth Amendment rights solely under the reasonable-expectation-of-privacy test. *See* id.

g. **Computer banner cases.**

1) A computer banner - also called a log-on banner - informs users of a computer and the network about the conditions of using the computer. Well-written banners tell the user that others can look at the data that passes through the computer or over the network. The wording of banners varies greatly, and as one would expect, the precise wording of the banner can make all the difference whether a warrant or other authority is required to search for information placed on a computer or a network. Well written banners can permit warrantless searches in three situations:

a) Monitoring. Monitoring the system to keep it running smoothly (network administrator permission as indicated above). This type of monitoring will not permit searches for evidence of crime, though evidence seen in plain view may be lawfully seized.

b) Destruction of expectation of privacy. The banner destroys the user's 4th Amendment expectation of privacy and so the 4th Amendment is not implicated. (When this is the case, a search warrant may not be required. When looking for email, however, destroying an expectation of privacy alone may be insufficient to overcome requirements of ECPA and the Stored Electronic Communications Act.)

c) Consent. The best banners cause computer and network users to consent to governmental or other searches of the computer or network.

2) b. Case notes:

a) **Banners are reasonable, and employers can impose any condition**. In Muick v. Glenayre Elecs, 280 F.3d 741 (7th Cir. 2002), the corporation (Glenayre) loaned a laptop computer to an employee. At law enforcement request, the corporation retrieved the computer and held it until a search warrant was obtained. The laptop contained child pornography. The court held: "The laptops were Glenayre's property and it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions; but the abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible."

b) **No REP in Employer-Owned Computers (Known Monitoring**.) In United States v. Ziegler, 456 F.3d 1138 (9th Cir. 2006), the court held that employees do not have REP in workplace computers owned by the corporation. The private employer discovered that the defendant was using his workplace computer to access child pornography sites and alerted the FBI. The FBI believed that the company technicians had already copied the defendant's hard drive, however the company claimed that the hard drive was copied at the FBI's request. The court held it didn't matter whether the search was governmental or private because the defendant had no REP in the computer because the computer was company-owned, there was a known monitoring policy, and prohibitions against private use. The analysis for this holding was insightful. [88]

c) **Banners can destroy the user's subjective expectation of privacy**. "[The defendant], a reasonably well educated person, had no expectation of privacy in the work computer owned by someone else because every time he accessed the work computer he physically acknowledged that he was giving consent to search the computer. Such repeated warnings about consent to search, followed by such repeated acknowledgments, categorically and without more defeat [the defendant's] claim of privacy." United States v. Bailey, 272 F. Supp. 2d 822 (D. Neb. 2003).

[88] The court held, "Thus, given the nature of our constitutional inquiry, we think the California court's reasoning is compelling. Social norms suggest that employees are not entitled to privacy in the use of workplace computers, which belong to their employers and pose significant dangers in terms of diminished productivity and even employer liability. Thus, in the ordinary case, a workplace computer simply "do[es] not provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from government interference or surveillance." (Citations omitted.) ("[T]he abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible."). Employer monitoring is largely an assumed practice, and thus we think a disseminated computer-use policy is entirely sufficient to defeat any expectation that an employee might nonetheless harbor."

d) **Banner permitted audits of all internet activities – Destroyed employees REP**. In United States v. Simons, 206 F.3d 392 (4th Cir. 2000), the defendant, Simons, worked for the CIA. The network banner[89] permitted "electronic auditing." Through the auditing, a systems administrator discovered sex-related internet activity on Simons' computer by remotely accessing that computer. Law enforcement officers (IGs) were alerted and they further explored the defendant's computer remotely and discovered that the computer contained child pornography. The court held: "Simons did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of the .... Internet policy. The policy clearly stated that [the contractor] would 'audit, inspect, and/or monitor' employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, 'as deemed appropriate.' .... This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private. Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after [the contractor] notified him that it would be overseeing his Internet use.

[89] The banner read: " Audits. Electronic auditing shall be implemented within all FBIS unclassified networks that connect to the Internet or other publicly accessible networks to support identification, termination, and prosecution of unauthorized activity. These electronic audit mechanisms shall . . . be capable of recording: - Access to the system, including successful and failed login attempts, and logouts; - Inbound and outbound file transfers; - Terminal connections (telnet) to and from external systems; - Sent and received e-mail messages; - Web sites visited, including uniform resource locator (URL) of pages retrieved; - Date, Time, and user associated with each event." The policy also stated that "users shall . . . understand FBIS will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate.

e) **Broadly written banner destroyed REP in Internet files**. (United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002). Angevine was suspected of having downloaded child pornography from a computer and network provided by the university where he worked as a professor. Agents obtained a search warrant for Angevine's computer. At trial, the defense moved to suppress the images found on the computer and requested a Franks hearing to challenge the affidavit. The District court held: (1) That the banner[90] destroyed any reasonable expectation that a computer and network user would have in internet files when using the computer. (2) That Angevine himself could not have had REP in the files because he was warned that anything he downloaded or passed through the network was publicly available, and (3) The files law enforcement obtained were deleted files recovered by special hardware. Since the files were not accessible to Angevine when found, they were not in his control or possession.

[90] The court described the banner as follows: "Oklahoma State University policies and procedures prevent its employees from reasonably expecting privacy in data downloaded from the Internet onto University computers. The University computer-use policy reserved the right to randomly audit Internet use and to monitor specific individuals suspected of misusing University computers. The policy explicitly cautions computer users that information flowing through the University network is not confidential either in transit or in storage on a University computer. Under this policy, reasonable Oklahoma State University computer users should have been aware network administrators and others were free to view data downloaded from the Internet. The policy also explicitly warned employees legal action would result from violations of federal law. Furthermore, the University displayed a splash screen warning of "criminal penalties" for misuse and of the University's right to conduct inspections to protect business-related concerns. These office practices and procedures should have warned reasonable employees not to access child pornography with University computers."

f) **"Monitoring only," narrowly written banner and agency interpretation defeats banner**. In United States v. Long, 64 M.J. 57 (C.A.A.F. 2006), military superiors directed the system administrator, pursuant to a system banner,[91] to provide certain emails for the purposes of a criminal investigation. The system administrator obliged. During testimony on a motion to suppress, the system administrator testified that the purpose of the banner was to related to the security monitoring program and it was general policy to avoid examining e-mails and their content because it was a "privacy issue." The court concluded "that while the log-on banner may have qualified [the defendant's] expectation of privacy in her e-mail, it did not extinguish it. Simply put, in light of all the facts and circumstance in this case, the "monitoring" function detailed in the log-on banner did not indicate to [the defendant] that she had no reasonable expectation of privacy in her e-mail." Problematic in this holding was the idea that requirement for the defendant to change her password every 90 days was somehow related to the defendant's REP, when in fact, the password change was to protect the system. *See*, Garrity v. John Hancock Mut. Life Ins. Co., 2002 U.S. Dist. LEXIS 8343 (D. Mass. 2002).

g) ***United States v. Long* modified.** A year after *Long* was decided, the Court of Appeals for the Armed Forces substantially modified its view in *Long* holding that accused was informed that his use of the government computer could be monitored, and he had no expectation of privacy in documents he stored on the computer. United States v. Larson, 66 M.J. 212 (CAAF, 2008).

[91] This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

h) In Ontario v. Quon,, __U.S.___ (slip op. 08-1332, June 17, 2010), a police supervisor ordered the review of Quon's agency-issued cell phone account to see if Quon had been unnecessarily paying for official text messages rather than just his personal ones as had been required by agency policy. Quon's supervisor had allowed him to use the cell phone for personal messages but Quon had also been told that monitoring of his use of the phone was subject to possible monitoring. The review of Quon's cell phone text records revealed that many of Quon's messages contained sexually-explicit text to Quon's wife and girlfriend. His employer disciplined him and Quon filed suit alleging a violation of his Fourth Amendment rights. The Supreme Court declined to address Quon's argument that his government employer had intruded on his REP in the content of his personal text messages. Second, the court said that, even if Quon had REP in those messages, he had been warned of the possibility of monitoring and the review of his text messages by his employer was pursuant to a legitimate work-related purpose.

h. **Exigent Circumstances.** Under the "exigent circumstances" exception to the warrant requirement, agents can search without a warrant if the circumstances "would cause a reasonable person to believe that entry ... was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." *See* United States v. Alfonso, 759 F.2d 728, 742 (9th Cir. 1985).

1) **Determining Whether Exigent Circumstances Exist.** In determining whether exigent circumstances exist, agents should consider:

a) The degree of urgency involved,

b) The amount of time necessary to obtain a warrant,

c) Whether the evidence is about to be removed or destroyed,

d) The possibility of danger at the site,

e) Information indicating the possessors of the contraband know the police are on their trail, and

f) The ready destructibility of the contraband.

*See* United States v. Reed, 935 F.2d 641, 642 (4th Cir. 1991).

2) **Exigent Circumstances in Computer Cases.** Exigent circumstances often arise in computer cases because electronic data is perishable. Computer commands can destroy data in a matter of seconds, as can humidity, temperature, physical mutilation, or magnetic fields created, for example, by passing a strong magnet over a disk. For example, in United States v. David, 756 F. Supp. 1385 (D. Nev. 1991), agents saw the defendant deleting files on his computer memo book, and seized the computer immediately. The district court held that the agents did not need a warrant to seize the memo book because the defendant's acts had created exigent circumstances. Similarly, in United States v. Romero-Garcia, 991 F. Supp. 1223, 1225 (D. Or. 1997), aff'd on other grounds, 168 F.3d 502 (9th Cir. 1999), a district court held that agents had properly accessed the information in an electronic pager in their possession because they had reasonably believed that it was necessary to prevent the destruction of evidence. The information stored in pagers is readily destroyed, the court noted: incoming messages can delete stored information, and batteries can die, erasing the information. Accordingly, the agents were justified in accessing the pager without first acquiring a warrant. *See* id. *See also* paragraph G 5 f of this lesson plan concerning searches incident to arrest.

3) **The Existence of Exigent Circumstances Depends On the Specific Facts of the Case.** Of course, in computer cases, as in all others, the existence of exigent circumstances is absolutely tied to the facts. *Compare* Romero-Garcia, 911 F. Supp. at 1225 *with* David, 756 F. Supp at 1392 n.2 (dismissing as "lame" the government's argument that exigent circumstances supported search of a battery-operated computer because the agent did not know how much longer the computer's batteries would live) and United States v. Reyes, 922 F. Supp. 818, 835-36 (S.D.N.Y. 1996) (concluding that exigent circumstances could not justify search of a pager because the government agent unlawfully created the exigency by turning on the pager).

4) **Once the Exigency Ends, the Right to Search Without a Warrant Ends.**

a) **The seizure of computer hardware to prevent the destruction of information it contains will not ordinarily support a subsequent search of that information without a warrant.** *See* David, 756 F. Supp. at 1392.The existence of exigent circumstances does not permit agents to search or seize beyond what is necessary to prevent the destruction of the evidence. When the exigency ends, the right to conduct warrantless searches does as well: the need to take certain steps to prevent the destruction of evidence does not authorize agents to take further steps without a warrant. *See* United States v. Doe, 61 F.3d 107, 110-11 (1st Cir. 1995).

b) If officers seize a computer or other items that contain data to prevent the destruction of evidence, the officers should quickly move to obtain a warrant to search the computer of container/media on which the data is stored. They should not search without a warrant unless they have proper consent.

i. **Plain View.** Evidence of a crime may be seized without a warrant under the plain view exception to the warrant requirement. To rely on this exception, the agent must be in a lawful position to observe and access the evidence, and its incriminating character must be immediately apparent. *See* Horton v. California, 496 U.S. 128, 136-37 (1990). For example, if an agent conducts a valid search of a hard drive and comes across evidence of an unrelated crime while conducting the search, the agent may seize the evidence under the plain view doctrine.

1) **The Plain View Exception Does Not Justify a Violation of a Person's Expectation of Privacy.** Importantly, the plain view exception cannot justify violations of an individual's reasonable expectation of privacy.

a) **The exception merely permits the seizure of evidence that has already been viewed in accordance with the Fourth Amendment.** In computer cases, this means that the government cannot rely on the plain view exception to justify opening a closed computer file. The contents of a file that must be opened to be viewed are not in "plain view." *See* United States v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996). This rule accords with decisions applying the plain view exception to closed containers. *See, e.g.,* United States v. Villarreal, 963 F.2d 770, 776 (5th Cir. 1992)(concluding that labels fixed to opaque 55-gallon drums do not expose the contents of the drums to plain view). ("[A] label on a container is not an invitation to search it. If the government seeks to learn more than the label reveals by opening the container, it generally must obtain a search warrant.").

b) **Encountering evidence of a different crime when conducting a search – get a second warrant.**

(1) It is not uncommon for those searching computers and media to encounter evidence of a completely different crime than the search warrant addresses. For example, while looking for evidence of fraud pursuant to a warrant, agents may find evidence of a completely different crime - typically possession of child pornographic images. A proper application of the plain view doctrine would make the first image encountered admissible under plain view. The harder question is whether subsequently discovered images are admissible. This, in turn, depends on how the agent continues the search. (See the *Carey* and *Hudspeth* case comparisons in this section infra.)

(2) **The best rule for this situation is for officers to stop the search and obtain a warrant for the evidence of the different crime.**

c) A case comparison.

(1) In United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999), a police detective searching a hard drive with a warrant for drug trafficking evidence opened a "jpg" file and discovered child pornography. He spent the next five hours accessing and downloading several hundred other "jpg" files in a search for more child pornography. The defendant moved to suppress the child pornography files on the ground that they were beyond the scope of the warrant. The government argued that the "jpg" files had been in plain view and were thus properly seized. The Tenth Circuit disagreed except for the first "jpg" file the detective discovered. The court held that, while agents may certainly seize incriminating evidence in plain view, they may not infringe on a suspect's right to privacy to put his property into plain view. Thus, the detective's seizure of the first "jpg" file while executing the search warrant was proper under plain view, but not the search for additional "jpg" files on the defendant's computers that were beyond the scope of the warrant.

(2) In United States v. Hudspeth, 459 F.3d 922 (8th Cir. 2006) officers with a search warrant for business records pertaining to the distribution of meth, found child pornographic images. They stopped the search and obtained a second warrant to search for child pornography. The *Hudspeth* court upheld the procedure of obtaining a second warrant.

**Caution: All the cases cited below precede *Arizona v. Gant*, U.S. _____, 129 S. Ct. 1710; 173 L. Ed. 2d 485 (2009). This lesson plan author does not believe that *Gant* affects the below cases with respect to SIAs of persons, but when the cell phone is found in the passenger compartment or within the arrestee's lunging area, *Gant* made significant changes. The author has left these "old cases" in the lesson plan until such time as the full contours of *Gant* are decided. Consult the LGD 4th Amendment lesson plan for the current application of *Gant*.**

j. **Search Incident to Arrest.** It has long been recognized that a search conducted incident to a lawful custodial arrest "is not only an exception to the warrant requirement of the Fourth Amendment, but is also a 'reasonable' search under that Amendment." United States v. Robinson, 414 U.S. 218, 235 (1973).

1) **The Rationale for Conducting a Search Incident to Arrest.** In Robinson, the Supreme Court noted "two historical rationales for the search incident to arrest exception:

a) The need to disarm the suspect in order to take him into custody, and

b) The need to preserve evidence for later use at trial. Id.

2) **The Permissible Scope of a Search Incident to Arrest: weapons, means of escape, and any evidence of any crime.** The permissible scope of a search incident to arrest was outlined by the Supreme Court in the 1969 case of Chimel v. California, 395 U.S. 752 (1969) as headnoted above and set forth in the foot note for those who wish to review the principle.[92]

3) **The Requirements for a Search Incident to Arrest.** A search incident to arrest may only be conducted when two requirements have been met.

a) **A Lawful Custodial Arrest.** First, there must have been a lawful custodial arrest. At a minimum, this requires that (1) probable cause exist to believe that the arrestee has committed a crime and (2) an arrest is actually made. A search incident to arrest may not be conducted in a situation where an actual arrest does not take place.[93]

---

[92] *"When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction. And the area into which an arrestee might reach in order to grab a weapon or evidence items must, of course, be governed by a like rule. A gun on a table or in a drawer in front of one who is arrested can be as dangerous to the arresting officer as one concealed in the clothing of the person arrested. There is ample justification, therefore, for a search of the arrestee's person and the area 'within his immediate control' – construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence."*

[93] *See* Robinson, 414 U.S. at 235; McCardle v. Haddad, 131 F.3d 43, 47-50 (2d Cir. 1997)(search incident to arrest not valid where 10-minute detention in backseat of patrol vehicle did not amount to an arrest).

b) **The Search Must Be "Substantially Contemporaneous" With the Arrest.** The second requirement for a lawful search incident to arrest is that the search must be "substantially contemporaneous" with the arrest. For a review of this principles in the non-computer world, see the footnote. [94]

(1) **Whether the Search Was "Substantially Contemporaneous" is Based on the Totality of the Circumstances.** See the footnote for a review of this basic principle covered in 4th Amendment instruction. [95]

(2) **Factors to Determine Whether the Search Was "Contemporaneous" With the Arrest.** Among the factors to be considered in determining whether a search was "contemporaneous" with the arrest are:

(a) Where the search was conducted;

(b) When the search was conducted in relation to the arrest; and

(c) Whether the defendant was present at the scene of the arrest during the search.

---

[94] *See* Stoner v. California, 376 U.S. 483, 486 (1964) and Preston v. United States, 376 U.S. 364, 367-368 (1964). Unfortunately, what exactly is meant by this phrase is open to interpretation. In United States v. Turner, 926 F.2d 883 (9th Cir.), cert. denied, 502 U.S. 830 (1991), the court stated that a search incident to arrest must be conducted "at about the same time as the arrest." Id. at 887. While very general, this comment reiterates the Supreme Court's mandate that, when a search is too remote in time or place from the arrest, the search cannot be justified as incident to the arrest. Preston, 376 U.S. at 367 ("Once an accused is under arrest and in custody, then a search made at another place, without a warrant, is simply not incident to the arrest").

[95] Whether a search was "substantially contemporaneous," is an issue that must be reviewed in light of the Fourth Amendment's general reasonableness requirement, taking into consideration all of the circumstances surrounding the search. Thus, while a search conducted 15 minutes after an arrest might be valid in one case, Curd v. City of Judsonia, 141 F.3d 839, 842-44 (8th Cir.), cert. denied, 525 U.S. 888 (1998)(Warrantless search of purse at police station found to be valid as incident to arrest even though search occurred 15 minutes after the defendant's arrest at home), a search 30 to 45 minutes after the arrest might be invalid in another. United States v. Vasey, 834 F.2d 782, 785-88 (9th Cir. 1987) (Warrantless search held not incident to arrest and invalid when the search took place 30 to 45 minutes after the defendant had been arrested, handcuffed, and placed in patrol vehicle).

4) **Scope of a Search Incident to Arrest of Pagers. Courts Consistently Allow an SIA of Digital Display Pagers.** The justification is that the numbers stored on the pager are "dynamic." If the pager receives a call after the arrest and the queue is full, then an old call is deleted to make room for the new one and the old call (evidence) is destroyed. [96]

5) **The courts are in disagreement about whether searches incident to arrest of cell-phone "received calls" data are permissible**. Some courts have held that an officer may lawfully conduct a warrantless search of a cell phone in a suspects' possession at the time of his arrest. The basis for these cases is the same as for pagers – the dynamic and easily destructible nature, of the data.

   (1) Courts have had no problem finding that the received calls log may be searched SIA because this information is "dynamic" – evidence can be destroyed. [97]

   (2) The courts' rationale is well articulated in United States v. Uriel Montejano Zamora, 2006 U.S. Dist. LEXIS 8196 (D. Ga. 2006) [98]

6) **Searches incident to arrest of cell-phones beyond the call received log.**

[96] *See, e.g.*, United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993); United States v. Ortiz, 84 F.3d 977, 984 (7th Cir), cert. denied, 519 U.S. 900 (1996)(citations omitted); United States v. Lynch, 908 F. Supp. 284, 288 (D.V.I. 1995); United States v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996); United States v. Thomas, 114 F.3d 403, 404-06 (3d Cir. 1997)(dicta); Yu v. United States, 1997 U.S. Dist. LEXIS 10884 at *4-*5 (S.D.N.Y. 1997).

[97] United States v. Parada, 289 F. Supp. 2d 1291 (D. Kan. 2003); United States v. Brookes, 2005 U.S. Dist. LEXIS 16844 (D.V.I. 2005);and United States v. Uriel Montejano Zamora, 2006 U.S. Dist. LEXIS 8196 (D. Ga. 2006)

[98] "In this case the phones were reasonably believed by the investigating agents to be dynamic, subject to change without warning by a call simply being made to the instrument. With each call is the risk that a number stored would be deleted, including the loss of calls made to or from the instrument in connection with the transportation and ultimate secured storage of the [drugs] at issue here. These numbers would have significant evidentiary value. It was the function and limitation of the cell-phone technology which motivated the investigating agents to conduct an immediate search of the phones, rather than seek a warrant." . . . The [defendant's arrest] . . . being proper, so were the searches incident to their arrests, and exigent circumstances otherwise authorized the seizure of the cell phones and the search of their electronic contents."

a) In 2007, the 5th Circuit decided United States v. Finley, 477 F.3d 250 (5th Cir.), cert. denied,127 S. Ct. 2065, 167 L. Ed. 2d 790, 2007 U.S. LEXIS 4168 (2007)). This is the first Circuit court case to squarely uphold a search incident to arrest of a cell phone involving both the call log and text messages. (Instructors might note that there is a very high degree of privacy associated with text messages.) The court did not address other data that might be on the phone such as the calendar, photos, videos, notes and the like. Even under *Finley*, searching voice mail is beyond the scope of an SIA because while the voice mail is *accessible* from the phone, it is not *on* the phone but stored on the cell phone provider's voicemail server.

~~b)~~ Several Circuit Courts have followed the general holding in *Finley*. *United States v. Pineda-Areola,* 2010 U.S. App. LEXIS 7685 (7th Cir. April 6, 2010); *United States v. Young*, 278 Fed. Appx. 242 (4th Cir., 2008), *cert. denied*, 2008 U.S. LEXIS 8016;*United States v. Murphy*, 552 F.3d 405 (4th Cir. 2009)and *Silvan W. v. Briggs*, 2009 U.S. App. LEXIS 1520 (10th Cir. 2009).

~~c)~~ Several important caveats have emerged from these progeny of *Finley*.

(1) **The "contemporaniety" requirement.**

- Searches incident to arrest must be performed contemporaneously with the custodial arrest. For cell phone searches, this means that the phone should be searched SIA as soon as it is safe following the arrest. United States v. Mercado-Nava, 486 F. Supp. 2d 1271 (D. Kan. 2007).
- Searching the phone after the arrestee has been taken to the station is too late to be justified as an SIA. United States v. Lasalle, 2007 U.S. Dist. LEXIS 34233 (D. Haw. 2007) (2 hours, 15 minutes later), and United States v. Park, 2007 U.S. Dist. LEXIS 40596 (D. Cal. 2007) (1 hour, 45 minutes later).

(2) **Subject no longer has access to the phone**. The body of SIA law has, in recent years, questioned the justification for an SIA once the arrestee has been secured and cannot get to evidence to destroy it. United States v. Park, 2007 U.S. Dist. LEXIS 40596 (D. Cal. 2007). But, an SIA of the arrestee's person is permitted even if the arrestee has been secured, and usually a subject's cell phone is on his person. If the cell phone is found in a vehicle of which the arrestee is an occupant or recent occupant, then the bright-line rule of *Belton* would apply. If the cell phone is found on neither the arrestee or in the vehicle, some Circuits will not be friendly to an SIA justification and either a warrant or another exception – such as consent or *Carroll* – should be considered.

(3) **Cell-phone forensics**.

Some cases have specifically mentioned that the data on the phone was immediately downloaded on the scene. (United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1273 (D. Kan. 2007) and United States v. Espinoza, 2007 U.S. Dist. LEXIS 25263 (D. Kan. 2007)). This was done using "cell phone forensics" rather than scrolling through the phone and writing down the information. Those trained in cell-phone forensics are able to connect the phone to a computer and capture all the data on the phone. Such an approach has several distinct advantages:

(a) There is little danger that data could be accidentally deleted or altered as could happen when an agent manually searches the phone.

(b) The exact data is captured reducing the chance that an agent looking at the phone might inaccurately record the data he or she sees.

(c) If the data needs to be presented in court and the government does not have the actual phone or the data, a witness will have to offer testimony as to the contents of a "writing," as what is displayed on the phone meets the Federal Rules of Evidence definition of a writing. Because the original or a proper duplicate of the writing is not available, a best evidence objection is likely. United States v. Bennett, 363 F.3d 947 (9th Cir.), cert. denied 543 U.S. 950 (2004) (GPS display viewed by agents where the device or photos of it were not available at trial) and United States v. Jackson, 2007 U.S. Dist. LEXIS 23298 (D. Neb. Mar. 28, 2007) (*Summaries* of Internet chat logs inadmissible as contrary to the best evidence rule.)

(d) If the phone itself is available, or the data can be displayed to the fact-finder, a best evidence objection can be defeated.

(e) Where cell-phone forensics is not possible, agents should be prepared to take photos of the relevant information on the device.

(f) **A summarized record of internet chat does not satisfy best evidence concerns.** The court granted defendant's motion in limine to exclude the inadmissible cut-and-paste transcript as not authentic under Fed. R. Evid. 901(a) and as not the best evidence under Fed. R. Evid. 1002, 1001(3), and 1004 because, given the missing data, timing sequences that did not make sense, and editorial information and the testimony that the transcript was altered, it did not accurately represent the entire conversations that took place between defendant and a federal agent. The court did not allow the government to use the transcript, which was not a computer printout or record, to refresh the agent's memory. United States v. Jackson, 2007 U.S. Dist. LEXIS 23298 (D. Neb. Mar. 28, 2007)

~~d)~~ Other courts, both federal and state, have rejected *Finley. United States v. Park,* 2007 U.S. Dist. LEXIS 40596 (NDCA May 23, 2007)*; United States v. Wall,* 2008 U.S. Dist. LEXIS 103058 (SDFL December 22, 2008); *State of Ohio v. Smith,* 920 N.E.2d 949 (2009).[99] Until the Supreme Court resolves the conflicting case law on this issue, agents should always consult an AUSA before conducting a warrantless search of a cell phone incident to an arrest of its owner.

e) **Investigative tips to avoid SIA issues**. Agents may often have probable cause that the phone contains evidence of a crime. When this occurs, either a search warrant can be obtained in advance, or the phone can be seized at the time of arrest and retained until a warrant can be obtained. Examples of probable cause of evidence of crime on the phone might be:

[99] On May 11, 2010, the State of Ohio filed a Petition for Writ of Certiorari with the U.S. Supreme Court in the case of *State of Ohio v. Smith*, 2010 WL 1932620. The U.S. Supreme Court has not yet ruled on that Petition.

(1) An undercover officer or informant may have made a call to, or received a call from, the subject's cell phone. In most cases, this would mean the cell phone's call log or telephone book may contain corroborating information that the call was received or made.

(2) If the subject is seen talking on the phone during the commission of an offense, who the subject might have been talking to may lead to an accomplice or co-conspirator.

(3) In many crimes – especially those involving vandalism, children, stalking, other sex offenses - subjects take photographs of their targets or deeds. When there is probable cause that was done, then there is probable cause there is evidence of a crime on the phone.

(4) Instead of immediately searching an arrestee's cell-phone, officers may obtain consent to look at the phone's data. Once the agents see something that is evidence of a crime, the phone can be seized and a warrant obtained.

f) **Extending *Finley* to other devices with more data-storage capacity.** *Finley* has opened the door wider on the question of whether the SIA justification might apply to other devices that have the ability to store enormous amounts of data such as a notebook computer or a Personal Digital Assistant (PDA). The courts have already signaled a reluctance to extend the scope of an SIA from the physical world to huge amounts of personal information people are now able to carry on their person in electronic form. One court observed:

"A laptop and its storage devices have the potential to contain vast amounts of information. People keep all types of personal information on computers, including diaries, personal letters, medical information, photos and financial records. Attorneys' computers may contain confidential client information. Reporters' computers may contain information about confidential sources or story leads. Inventors' and corporate executives' computers may contain trade secrets. In this case, Arnold kept child pornography on his laptop and in his storage devices; however, "[i]t is a fair summary of history to say that the safeguards of liberty have frequently been forged in controversies involving not very nice people." *Montoya de Hernandez,* 473 U.S. at 548 (Brennan, J., dissenting) (quoting *United States v. Rabinowitz,* 339 U.S. 56, 69, 70 S. Ct. 430, 94 L. Ed. 653 (1950) (Frankfurter, J., dissenting)." United States v. Arnold, 454 F. Supp. 2d 999 (D. Cal. 2006)

k. **Carroll doctrine permits search of cell phones.** The Carroll doctrine applies to cell phones located in a vehicle where there is probable cause that the phone contains evidence of a crime. United States v. James, 2008 U.S. Dist. LEXIS 34864 (E.D. Mo. Apr. 29, 2008); United States v. De Jesus Fierros-Alavarez, 547 F. Supp. 2d 1206 (D. Kan. 2008); United States v. James, 2008 U.S. Dist. LEXIS 34864 (E.D. Mo. Apr. 29, 2008); United States v. Rocha, 2008 U.S. Dist. LEXIS 77973 (D. Kan. Oct. 2, 2008).

l. **Inventory Searches.** Inventory searches are a "well-defined exception to the warrant requirement of the Fourth Amendment." Colorado v. Bertine, 479 U.S. 367, 371 (1987). Where evidence is found during a lawfully conducted inventory search, it may be used against the defendant in a later trial.

1) **The Three Justifications for Allowing Inventory Searches.** In South Dakota v. Opperman, 428 U.S. 364 (1976), the Supreme Court outlined three justifications for allowing law enforcement officers to inventory lawfully impounded property without first obtaining a warrant.

a) **Protection of the Owner's Property.** First, there is a need for law enforcement to protect the owner's property while it remains in police custody.

b) **Protection of Police Against False Claims of Lost or Stolen Property.** Second, an inventory protects the police against claims or disputes over lost or stolen property.

c) **Protection of Society From Hidden Dangers.** And third, an inventory is necessary for the protection of the police from potential dangers that may be located in the property.

2) **The Requirements For Conducting An Inventory Search.** There are two requirements for conducting a valid inventory search.

a) **The Property Must Be Lawfully Impounded.** First, the property that is being inventoried must have lawfully come into the possession of law enforcement officers.

b) **There Must Also Be a Standardized Policy That Governs the Conduct of the Inventory.** The second requirement of a valid inventory search is that it be conducted in accordance with the searching agency's standardized inventory policy aimed at accomplishing the justifications for inventory searches. [100]

[100] As noted in Bertine: "The underlying rationale for allowing an inventory exception to the Fourth Amendment warrant rule is that police officers are not vested with discretion to determine the scope of the inventory search. This absence of discretion ensures that inventory searches will not be used as a purposeful and general means of discovering evidence of crime." Id. at 376 (Blackmun, J., concurring)(citation omitted). *See also* United States v. Bullock, 71 F.3d 171, 177 (5th Cir. 1995), cert. denied, 517 U.S. 1126 (1996)("In order to prevent inventory searches from concealing such unguided rummaging, Supreme Court has dictated that a single familiar standard is essential to guide police officers, who have only limited time and expertise to reflect on and balance the social and individual interests involved in the specific circumstances they confront")(quotation and citation omitted).

(1) **Written Inventories Are Not Required.** While the law enforcement agency involved must have a "standardized" inventory policy, several courts have upheld unwritten standardized policies if the government offers sufficient testimony of the prior existence of that policy.[101] Nonetheless, as a practical matter, the best way for a law enforcement agency to avoid difficult with this particular requirement would be to reduce their standardized inventory policy to writing.

(2) **Law Enforcement Agencies May Establish Their Own Policies.** Finally, law enforcement agencies may establish their own standardized policies, so long as they are reasonably constructed to accomplish the goals of inventory searches and are conducted in good faith.

3) **Inventory Searches and Computers and Cell Phones.**

a) While case law on the issue is sparse, it is unlikely that the inventory search exception to the warrant requirement would support a search through seized computer files or the contents of a cell phone.[102] One District Court has held that the purposes of an inventory are not served to inventory electronic devices. United States v. Park, 2007 U.S. Dist. LEXIS 40596 (D. Cal. 2007)

[101] *See, e.g.*, United States v. Thompson, 29 F.3d 62 (2d Cir. 1994); United States v. Arango-Correa, 851 F.2d 54, 59 (2d Cir. 1988); United States v. Frank, 864 F.2d 992 (3d Cir. 1988), cert. denied, 490 U.S. 1095 (1989); United States v. Ford, 986 F.2d 57 (4th Cir. 1993); Bullock, supra.

[102] *See* United States v. O'Razvi, 1998 U.S. Dist. LEXIS 10860 (S.D.N.Y. 1998), aff'd without opinion 173 F. 3d 847 (2d Cir. 1999) (noting the difficulties of applying the inventory search requirements to computer disks).

b) **Inventory searches cannot justify examining electronic devices or storage media.** Even assuming that standard procedures authorized such a search, the legitimate purposes served by inventory searches in the physical world do not translate well into the when it comes to inventorying digital devices or stored data. Information does not need to be reviewed to be protected, and does not pose a risk of physical danger. Although an owner could claim that his computer files were altered or deleted while in police custody, examining the contents of the files would offer little protection from tampering. Accordingly, agents will generally need to obtain a search warrant in order to examine seized computer files held in custody.[103]

## H. EPO # 8: DESCRIBE SPECIAL CONSIDERATIONS IN PREPARING A SEARCH WARRANT TO SEARCH AND/OR SEIZE COMPUTERS

**Important: Instructors must be careful to distinguish between searches and seizures in the electronic world. If officers have probable cause that media or a computer contains evidence of a crime, they may seize it for a reasonable period of time in order to obtain a warrant to search the computer or media. Or, if there is an applicable exception to the requirement of a search warrant, such as consent, an officer may proceed with a warrantless search. The fact that an officer has the authority to seize a computer or other electronic media, either with a warrant or pursuant to an exception to the warrant requirement, does not necessarily mean that the item may also be searched.**

**An excellent resource for preparing to teach the EPO's relating to computer searches in the August 24,2009, publication by the DOJ's Computer Crimes and Intellectual Property Section entitled "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations."[104]**

1. **Traditional Searches Differ From Those Searches That Target Computers and Data.** Searches for traditional physical evidence, such as contraband or stolen property, are different than those that target computers and other electronic devices or media for data stored on them. An overview of those differences are:

   a. **The Form of What is Being Sought.** Looking for data is different than objects or paper.

[103] *See* United States v. Flores, 122 F. Supp. 2d 491 (D.N.Y. 2000) (rejecting inventory search justification for warrantless search of seized cellular telephone).

[104] An electronic copy of this manual may be downloaded from http://www.cybercrime.gov.

b. **Data Searches May Require Specific Information about the Target and how the Target Uses Computers.** Pre-search warrant execution information must be collected to identify the type of equipment and software to conduct a search for data.

c. **The need to particularly identify WHAT is to be searched for.**

d. **The need to particularly identify WHERE the search may be conducted.**

e. **The requirement to describe some aspects of HOW the search is to be executed (off-site search justification.)**

2. **The form of the evidence (data) sought.**

a. In traditional searches, agents are looking for a particular physical item in a particular location. The search for data is different. Because data consist of electrical impulses that can be stored anywhere and instantly moved or deleted, agents may not know where computer files are stored or in what form. The data can be on the computer one is searching, but electronically hidden from view. The filenames can be anything the suspect wants them to be. The data can be instantly erased, modified, or sent to a confederate. The same data can exist in identical form in many different places.

b. The courts have recognized that data can be easily hidden and manipulated.

1) "Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent." United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998).

2) "Defendants may legitimately have checked to see that the contents of the directories corresponded to the labels placed on the directories. Suspects would otherwise be able to shield evidence from a search simply by 'misfiling' it in a directory labeled 'e-mail. '" Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001). See also United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000)

3. **The need for pre-search information**. In computer searches, there is certain technical information the team must know so agents know where to look. If agents were to execute a search warrant of a large tract of land, they would want to know as much about the area beforehand. In computer searches, the team must also know the terrain where the evidence might be concealed.

a. **At a minimum, agents must know**:

1) What types of computers and operating systems are involved?

2) What types of software does the suspect use?

3) Is the computer connected to a network? Where is the computer network server located? In the same District as the computer? Is the server located in a foreign country?

4) Can the evidence safely and effectively be searched for on-site, or must the computer be moved to another location to conduct the search?

b. **How to Gather System Information.** Gathering this information may involve some measures not usually done in a non-computer search.

1) **Interviews.** Interview of the system administrator of the targeted network and those familiar with the network. This might be done in an undercover capacity.

2) **Visits.** On-site visits (often undercover) that at least reveal some elements of the hardware involved.

4. **Determining Particularly - What to Search for and Where the Evidence is Located - The Fourth Amendment.** The Fourth Amendment mandates that no search warrants "shall issue but upon probable cause, supported by oath or affirmation, and ***particularity describing the*** place to be searched, and the person or ***thing to be seized***." Complying with the 4th Amendment in computer searches can be more difficult than in traditional searches.

5. **Articulating WHERE to look and the "independent component doctrine."** Agents must be particular where they want to look for data. Each component that agents want to search must be viewed independently. Agents must have PC to search or seize each component and must consider, plan for, and include in the search warrant each component and item that agents wish to seize, and set out the probable cause for each. For example, to say that agents want to search or seize a "computer" can be both too broad and too narrow. It rarely meets the Fourth Amendment particularity requirement. **Instead, agents must view each component of a computer independently and develop probable cause for each.**

1) Media and external storage devices. Much data is not stored on the computer itself or the hard drive in the computer case, but on removable media such as diskettes, flash memory devices such as thumb drives, memory chips, zip drives, CDs/DVDs, and the like. Since 2003, external USB (Universal Serial Bus) external hard drives have become very affordable, reliable, and an excellent choice for storing, moving, protecting and concealing data.

2) If a keyboard, monitor, printed, or other devices or peripherals need to be seized, they should be independently listed and their seizure justified. The reasons for such seizures are listed in the "hardware only searches" materials below.

3) Modem, printers, scanners, drawing tablets, cables and anything else attached to or capable of being attached to the computer;

**NOTE: Digital evidence may be set to only print to certain devices. Some input devices code the source on the output they create.**

6. **Case note - Warrant particularly described evidence that could be found on iPod and computer, and therefore searching these devices was within the scope of the warrant.** United States v. Corleto, 2009 U.S. Dist. LEXIS 10826 (D. Utah Feb. 5, 2009). ATF obtained a warrant to search his home for a variety of evidence re his weapons purchases. None of the 16 Glocks were found, but a computer and an iPhone were seized. A forensic analysis was performed of the computer and iPhone, which disclosed pictures of the defendant carrying one of his beloved Glocks. A second warrant was obtained to perform a more in depth review of the computer and iPhone for evidence of firearms violations. The court ruled that the warrant supporting the original search provided adequate PC and adequate particularity to justify the seizure of the computer and iPhone, and that the search subsequently conducted of these devices, pursuant to a second warrant, was also appropriate. *(Practice note: The court ruled that the computer and iPhone were properly seized pursuant to the first warrant. The scope of evidence sought in the second warrant seems to be the same information sought in the first. Thus, it is not clear why the second warrant was required and what additional authority to search it provided.)*

7. Other items to search for:

   a. Computer manuals, so we know how to get around encryption and passwords;

b. Original software and manuals. Much original software have distinct numbers and we can determine whether the software on a machine came from a particular copy of the software;

c. Notes and journals that might contain passwords, encryption, e-mail addresses, Internet URLs (addresses), indexes of storage media and the like.

8. **Articulating WHAT to look for.** In most computer or data searches, what agents really want is the data. Sometimes, however, retrieving only the actual computers is the purpose of the search.

a. **Hardware only searches**.

1) In rare situations, agents want to seize only the actual computer and other hardware and components – and not the data. This might be the case when the computer is stolen (contraband or fruits of a crime) or used in the commission of a crime (instrumentalities) such as where a computer was used to prepare a letter, spreadsheet, or send an e-mail.

2) Hardware only searches should be considered rare because whenever a computer is involved in a crime, the computer was probably used to create, receive, transmit, or otherwise manipulate data, and so not only is possession of the computer important, the data is as well.

3) Even in searches where the target is only data, hardware seizures may also be part of the search warrant and affidavit.

a) A list of items to consider searching for is included in paragraph 5 above.

b) Also consider that any c*omponent required for the computer to operate should be searched for because c*omponents of the computer being seized might require certain peripherals to be attached for the computer to run properly (such as a specialty keyboard) or to read specialty media (such as proprietary zip drives and the like.). Those devices should be addressed in the search warrant affidavit.

c) *Printers*. If agents have a document and wish to determine whether a specific printer printed that document, the agents would need to seize the printer.

b. **Data Searches. Computer Searches Generally Target Data.** In most computer searches, what the officers want is the data, and not just the computer. Certainly agents must find the computer and components to be able to search for the data, but the objective of the search is really the data.

a) ***Articulating probable cause to search for data***. When agents want data, they should be prepared to articulate the probable cause that the data exists, and to describe what that data is.

(1) Ensure that what is to be looked for includes "records in any form" to include paper and electronic whether stored on computers or not.

(2) **"All Records" Requests Are Generally Overbroad.** Agents cannot simply request permission to seize "all records" from an operating business unless agents have probable cause to believe that the criminal activity under investigation pervades the entire business. Instead, the description of the files to be seized should include limiting phrases that can modify and limit the "all records" search. For example, agents may specify the crime under investigation, the target of the investigation if known, and the time frame of the records involved.

b) **Staleness, data warrants, and deleted files.**

(1) To obtain a warrant, agents must have probable cause not only that the data used to be on the computer to be searched, but is still on that computer. Courts have recognized that users often keep their data for extraordinarily long periods because, unlike trying to make room in a filing cabinet, users find there is no need to delete old data from a computer. Computers, in this sense, are viewed by users as a very large filing cabinet allowing people to archive old data for long periods at no expense or inconvenience. This recognition is even more important in child pornography cases because those that have such files tend to keep their files forever. United States v. Hay, 231 F.3d 630 (9th Cir. 2000), cert. denied, 534 U.S. 858 (2001).

(2) In addition, the act of deleting a file from a computer does not actually erase the data but instead simply deletes the file name from the directory of files. The actual data remains on the hard drive unless special, advanced steps are taken. The best analogy is a card catalog in a library. If one were to remove a card from the catalog and destroy it, the book itself remains on the shelf unless it is physically removed. Deleting a data file only removes the "card" and the data remains on the hard drive until the computer needs the space occupied by the file to store other data. This fact should be stated in a search warrant affidavit in showing the information agents have is not stale. United States v. Streetman, 207 Fed. Appx. 414 (5th Cir. 2006)

9. **HOW to Search: Articulating the need for off-site searches of seized computers, media, and devices.** In some instances, the data that agents want to search for can be obtained at the location where the media or computer is found. When this is possible, the computer system and the peripheral devices do not have to be taken from the scene. As the use of computers and their sophistication increases, law enforcement has become less able to conduct safe and meaningful searches on scene and must resort to removing computers and media to be searched elsewhere. Removing the computer, media, and other devices to be searched off-site has come to the attention of the courts with mixed results.

   a. **If agents want to remove computers, devices, or computer media off-site to be searched, that need and the justification must be articulated in the search warrant affidavit.** (See the appendix for sample language from various agencies.)

   b. **Justification for removal of computers, devices, and media to be searched off-site.**

      1) **Must search to determine media contents**. Agents cannot tell what storage media contains by looking at it the container; each container (hard drive, floppy disk, CD or other media) must be examined.

      2) **Time required**. It may take days or weeks to find the specific information described in the warrant because computer storage devices can contain extraordinary amounts of information.[105] Searching on scene may be more intrusive because of time officers would have to remain on premises.

      3) **Labeling, intentional mislabeling, and hiding data**. Even if the agents know specific information about the files they seek, the data may be mislabeled, encrypted, stored in hidden directories, or embedded in "slack space" that a simple file listing will not reveal. Images can be hidden in all manner of files and it may take special skills and equipment to find it.

      4) **Availability of necessary tools**. On-site tools may not be sophisticated enough to defeat security and encryptions measures.

      5) **Proper environment**. The lack of a controlled and clean environment to conduct the search.

[105] Agents cannot reasonably be expected to spend more than a few hours searching for materials on-site, and in some circumstances (such as executing a search at a suspect's home) even a few hours may be unreasonable. *See* United States v. Santarelli, 778 F.2d 609, 616 (11th Cir. 1985).

6) **Lack of On-Site Technical Expertise.** Attempting to search files on-site may even risk damaging the evidence itself in some cases. The computer may use an uncommon operating system or software that the on-site technical specialist does not fully understand. Off-site searches also may be necessary if agents have reason to believe that the computer has been "booby trapped" with a self-destruct feature.

7) **Preserving the Evidence.** In an on-site search, the target or confederates could momentarily access the computer to delete or destroy data. This is especially true if the computer is attached to a network because a network command to the computer to be searched might be sent from any computer on the network.

8) **Safety of the Officers and Preserving Law Enforcement Techniques and Methods.** A lengthy search in the target's home or business place may unnecessarily expose the officers to risk.

United States v Hill, 459 F.3d (9th Cir. 2006); United States v. Adjani, 452 F.3d 1140 (9th Cir. 2006); United States v. Walser, 275 F.3d 981(10th Cir. 2001); and United States v. Hay, 231 F.3d 630 (9th Cir. 2000).

c. **If removal of computers, devices and media has not been addressed in the affidavit, and agents determine that an off-site search is necessary,** agents should seize the items and not search them until a new search warrant has been obtained justifying the seizure.

~~d.~~ **No legal requirement that the search strategy be set forth in the search warrant.**

1) While a computer search warrant must describe "with particularity the objects of their search, it is not necessary that a computer search warrant application, or a computer search warrant itself, contain a search protocol (a list of steps the investigator is required to undertake in examining the computer). United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005). In United States v. Khanani, 502 F.3d 1281, 1290-91 (11th Cir. 2007), the Eleventh Circuit rejected the argument that a warrant should have included a search protocol, pointing in part to the careful steps agents took to ensure compliance with the warrant.[106]

[106] *See also United States v. Cartier*, 543 F.3d 442, 447-48 (8th Cir. 2008) ("While we acknowledge that there may be times that a search methodology or strategy may be useful or necessary, we decline to make a blanket finding that the absence of a search methodology or strategy renders a search warrant invalid per se"); *United States v. Upham*, 168 F.3d 532, 537 (1st Cir. 1999) ("The warrant process is primarily concerned with identifying what may be searched or seized—not how").

2) Though a specific protocol need not be set forth in a search warrant, the scope of the search warrant must be clear and the agents executing that warrant must remain within its scope. In United States v. Payton, ___ F.3d ___, 2009 WL 2151348, at *3-5 (9th Cir. July 21, 2009), that Court invalidated a computer search at a residence where there was no basis to conclude that records falling within the scope of the warrant would be found on the computer.

10. **Identifying the Need For Multiple Warrants (Network Searches)**

a. **Data in Multiple Locations.** If agents have reason to believe that data subject to seizure pursuant to a search warrant is stored in multiple districts, they should obtain a warrant in each affected district.

b. **The Federal Rule.** F.R.Cr.P. 41(b)(2) authorizes a magistrate judge located in one judicial district to issue a search warrant for "a search of property … within the district," or "a search of property . . . outside the district if the property … is within the district when the warrant is sought but might move outside the district before the warrant is executed." Thus, if the search warrant application demonstrates the possibility that the items to be seized may move or be moved to another district, the search warrant may authorize the search to occur in the other district.

c. **Nationwide search warrants for stored electronic communications. (See EPO # 5 and paragraph E 1 B of this lesson plan**.) As an exception to the federal rule stated above, the USA PATRIOT Act expanded the scope federal warrants for stored electronic communications. Rather than limiting federal magistrates and judges to issue warrants within their districts, a judicial official with "jurisdiction over the offense under investigation" can issue a warrant that can be enforced nationwide. Under this change, if a suspect in the Eastern District of Virginia had stored electronic communications on a server in California and Texas, a Federal judge in the Eastern District of VA could issue a search warrant for the stored emails in California, and Texas. Depending on the nature of the crime, Federal judges in other Districts where there is venue could also issue the same warrant.

d. **"Property" Includes Intangible Property.** The Supreme Court has held that "property" as described in Rule 41 includes intangible property such as computer data. *See* United States v. New York Tel. Co., 434 U.S. 159, 169-70 (1977). Although the courts have not directly addressed the matter, the language of Rule 41, combined with the Supreme Court's interpretation of "property," may limit searches of computer data to data that resides in the district in which the warrant was issued. *Cf.* United States v. Walters, 558 F. Supp. 726, 730-31 (D. Md. 1980)(suggesting such a limit in a case involving telephone records).

e. **Territorial Limits on Searches for Data.** A territorial limit on searches for data poses problems for law enforcement because computer data stored in a computer network can be located anywhere in the world. Even worse, it may be impossible for agents to know when they execute their search whether the data they are seizing has been stored within or outside the district. Agents may in some cases be able to learn where the data is located before the search, but in others they will be unable to know the storage site of the data until after the search has been completed.

f. **Evidence Located in More Than One District.** When agents ~~can~~ learn prior to the search that some or all of the data described by the warrant is stored remotely from where the agents will execute the search, the best course of action depends upon where the remotely stored data is located. When the data is stored remotely in two or more different places within the United States and its territories, agents should obtain additional warrants for each location where the data resides to ensure compliance with a strict reading of Rule 41(b).

g. **Evidence Stored in a Foreign Country.** When agents seek to seize data stored remotely outside of the United States, they likely will not be able lawfully to do so by remote access to that data from within the United States. Rather, agents and prosecutors may be required to take actions ranging from an informal agency-to-agency request for assistance to a formal request under a Mutual Legal Assistance Request made through the Department of Justice and State Department. In such a situation, agents and prosecutors should contact the Department of Justice Computer Crimes Intellectual Property Section and Office of International Affairs at (202) 514-0000 for assistance with these questions.

h. **When Agents Do Not Know They Are Accessing Data in Another District.** When agents do not and even cannot know that data searched from one district is actually located outside the district, evidence seized remotely from another district ordinarily should not lead to suppression of the evidence obtained. The reasons for this are twofold.

1) **Unintentional Collection.** First, courts may conclude that agents sitting in one district who search a computer in that district and unintentionally cause intangible information to be sent from a second district into the first have complied with Rule 41(a). *Compare* United States v. Ramirez, 112 F.3d 849, 851-52 (7th Cir. 1997); United States v. Denman, 100 F.3d 399, 402 (5th Cir. 1996); United States v. Rodriguez, 968 F.2d 130, 135-36 (2d Cir. 1992).

2) **Violation of the Rule Does Not Automatically Result in Suppression.** Even if courts conclude that the search violates Rule 41(a), the violation will not lead to suppression of the evidence unless the agents intentionally and deliberately disregarded the Rule, or the violation leads to "prejudice" in the sense that the search might not have occurred or would not have been so "abrasive" if the Rule had been followed. *See* United States v. Burke, 517 F.2d 377, 384-87 (2d Cir. 1975); United States v. Martinez-Zetas, 857 F.2d 122, 136-37 (3d Cir. 1988). Under the widely adopted Burke test, courts generally deny motions to suppress based on a violation of Rule 41 that was inadvertent rather than deliberate unless to deny that motion would result in unfair prejudice to the defendant. Accordingly, evidence acquired from a network search resulting in seizure of data stored in another district would ordinarily not be subject to suppression. *See generally* United States v. Trots, 152 F.3d 715, 722 (7th Cir. 1998)("[I]t is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the fourth amendment, that would call for suppression.").

## I. EPO # 9: DESCRIBE SPECIAL CONSIDERATIONS IN EXECUTING A SEARCH WARRANT TO SEARCH AND/OR SEIZE COMPUTERS

1. **Technical Assistance During Execution of a Search Warrant.**

a. **Generally.** The participation of a computer forensics expert is essential to planning the execution of a computer search warrant. In many, if not most, instances, it is advisable that the technical expert also participate in the execution of such a warrant. Not having a computer expert involved may jeopardize the admissibility of the evidence seized from a computer. ***The assistance of non-law enforcement officer in the execution of a warrant is permitted under 18 U.S.C. §3105.***

b. **Title 18 U.S.C. § 3105.** During execution, agents must comply with Title 18 U.S.C. § 3105, which provides:

*"A search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution."*

~~c.~~ **Violation of the Statute.** If bringing in a computer forensics expert, name the person in the warrant or state that one will be needed to aid in the search. Where an agent violates Title 18 U.S.C. § 3105, he or she may be subject to civil liability.

2. **General Rule – Before Entering a Dwelling to Serve Warrants, Officers Must Comply** with Title 18 U.S.C. § 3109. "Police acting under a warrant usually are required to announce their presence and purpose, including by knocking, before attempting forcible entry, unless circumstances exist which render such an announcement unreasonable." United States v. Sergeant, 319 F.3d 4, 8 (1st Cir. 2003). The Supreme Court has found that absent exigent circumstances, it is unreasonable for officers to enter a dwelling without first knocking and announcing their presence. Wilson v. Arkansas, 514 U.S. 927, 936 (1995). Of course, during the execution of search or arrest warrants, a law enforcement officer may obtain consent to gain entry into particular premises. However, where consent is not a viable option for law enforcement officers, forced entry may be required. In sum, there are two situations in which a law enforcement officer may use force to gain entry to execute a search or arrest warrant:

a. **The Statute.** Title 18 U.S.C. § 3109 is the Federal "knock and announce" statute. Titled "Breaking Doors or Windows for Entry or Exit," the statute provides as follows:

*The officer may break open any outer or inner door or window of a house, or any part of a house, or anything therein, to execute a search warrant, if, after notice of his authority and purpose, he is refused admittance or when necessary to liberate himself or a person aiding him in the execution of the warrant.*

b. **When Exigent Circumstances Exist, a Law Enforcement Officer May Dispense With the Requirements of § 3109.** The rule laid out in § 3109 is not absolute, however. Law enforcement officers may also use force to enter a residence when exigent circumstances exist. In such cases, the officers may dispense with the notice and authority requirements of § 3109. In Richards v. Wisconsin, 520 U.S. 385 (1997), the Supreme Court held that agents can dispense with the knock-and-announce requirement if they have

*"a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, would be dangerous or futile, or that it would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence."* Id. at 394.

The Court stated that this showing was "not high, but the police should be required to make it whenever the reasonableness of a no-knock entry is challenged." Id. at 394-95. Such a showing satisfies both the Fourth Amendment and the statutory knock-and-announce rule of Title 18 U.S.C. § 3109. *See* United States v. Ramirez, 523 U.S. 65, 71-73 (1998).

c. **Exigent Circumstances and Computers.** There are no reported Federal cases where an exception to this statute was claimed in a case where computers or electronic evidence was the object of the search. Technically adept suspects may "hot wire" their computers in an effort to destroy evidence using "hot keys" that destroy evidence with a keystroke combination. Less sophisticated users know how to delete files quickly. In many cases, turning off the computer can destroy some evidence, in particular the file that the user was working on at the time of the shut down. The time between when an agent announces his presence until that reasonable period the target opens the door leaves sufficient time to destroy a lot of evidence.

d. **Agents May Request "No-Knock" Warrants.** When agents have reason to believe that knocking and announcing their presence would allow the destruction of evidence, would be dangerous, or would be futile, agents should request that the magistrate judge issue a no-knock warrant. Even if a no-knock warrant is not obtained, the knock-and-announce statute does not prevent agents from conducting a no-knock search. If upon arrival at the search location agents develop reasonable suspicion that evidence will be destroyed, officers need not comply with the statute. In Richards, the Supreme Court made clear that "the reasonableness of the officers' decision [to dispense with the knock-and-announce rule] . . . must be evaluated as of the time they entered" the area to be searched. Richards, 510 U.S. at 395. Accordingly, agents may "exercise independent judgment" and decide to conduct a no-knock search when they execute the search, even if they did not request such authority or the magistrate judge specifically refused to authorize a no-knock search. Id. at 396 n.7. The question in all such cases is whether the agents had "a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, would be dangerous or futile, or that it would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence." Id. at 394.

**Note to Instructors: The below paragraph 3 to the end of this EPO is a "cutting edge" issue that is being heavily litigated by DOJ. It is not testable. Instructors should not teach the below materials, but they are welcome to mention that some magistrates have insisted that whatever is seized be imaged and actually searched within a certain period of time, and that time can be as short as ten days.**

3. **Time Frames Governing Retention and Forensic Examination of Seized Computers.** The forensic examination of seized computers may take months to complete because of their capability to store enormous amounts of data. Neither Federal Rule of Criminal Procedure 41 nor the Fourth Amendment imposes any specific limitation on the time period of the government's forensic examination. The government ordinarily may retain the seized computer and examine its contents in a careful and deliberate manner without legal restrictions, subject only to Rule 41(e)'s authorization that a "person aggrieved" by the seizure of property may bring a motion for the return of the property

a. **Some Magistrates Have Begun Imposing Timeframes on When Computers Must Be Searched.** A few magistrate judges have refused to sign search warrants authorizing the seizure of computers unless the government conducts the forensic examination in a short period of time, as short as seven days. The reasoning cited by these judges is that it might be constitutionally "unreasonable" under the Fourth Amendment for the government to deprive individuals of their computers for more than a short period of time. Other magistrates have suggested that Rule 41's requirement that agents execute a "search" within 10 days of obtaining the warrant might apply to the forensic analysis of the computer as well as the initial search and seizure. *See* F.R.Cr.P. 41(c)(1). While the law does not expressly authorize magistrate judges to issue warrants that impose time limits on law enforcement's examination of seized evidence, agents must be prepared to provide the information - and justification - if the magistrate judge requires.

b. **The Ten-Day Rule.** Rule 41(c)(1) requires that the agents who obtain a warrant must "search, within a specified period of time not to exceed 10 days, the person or place named for the property or person specified." This rule directs agents to search the place named in the warrant and seize the property specified within 10 days so that the warrant does not become 'stale' before it is executed. *See* United States v. Sanchez, 689 F.2d 508, 512 n.5 (5th Cir. 1982). Some magistrates have applied this rule to require agents to complete their forensic evaluation within the ten day period. An analogy to paper documents may be helpful. A Rule 41 warrant that authorizes the seizure of a book requires that the book must be seized from the place described in the warrant within 10 days. However, neither the warrant nor Rule 41 requires law enforcement to examine the book and complete any forensic analysis of its pages within the same 10-day period. *Cf.* Commonwealth v. Ellis, 1999 Mass. Super. LEXIS 368 at *32 (Mass. Super. 1999)(interpreting analogous state law provision)("The ongoing search of the computer's memory need not have been accomplished within the … period required for return of the warrant.").

c. **Rule 41(e)(2)(B).** Unless otherwise specified in the warrant, Rule 41(e)(2)(B) separates the concept of the execution of a warrant and the seizure of electronically stored information from a later forensic review of the media or information on which such data have been copied or "cloned." Under this rule, the time for executing the warrant…refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

d. **One Court Has Determined Suppression is the Appropriate Remedy For Violating Court-Imposed Time Limits.** At least one court has adopted the severe position that suppression is appropriate when the government fails to comply with court-imposed limits on the time period for reviewing seized computers.

1) **The Case.** In United States v. Brunette, 76 F. Supp. 2d 30 (D. Me. 1999), aff'd, 256 F.3d 14 (2001), a magistrate judge permitted agents to seize the computers of a child pornography suspect on the condition that the agents searched through the computers for evidence "within 30 days." The agents executed the search five days later, and seized several computers. A few days before the thirty-day period elapsed, the government applied for and obtained a thirty-day extension of the time for review. The agents then reviewed all but one of the seized computers within the thirty-day extension period, and found hundreds of images of child pornography. However, the agents did not begin reviewing the last of the computers until two days after the extension period had elapsed. The defendant moved for suppression of the child pornography images found in the last computer, on the ground that the search outside of the sixty-day period violated the terms of the warrant and subsequent extension order. The court agreed, stating that "because the Government failed to adhere to the requirements of the search warrant and subsequent order, any evidence gathered from the … computer is suppressed." Id. at 42.

2) **The Analysis.** The result in Brunette makes little sense either under Rule 41 or the Fourth Amendment. Even assuming that a magistrate judge has the authority to impose time constraints on forensic testing in the first place, it seems incongruous to impose suppression for violations of such conditions when analogous violations of Rule 41 itself would not result in suppression. *Compare* Brunette with United States v. Twenty-Two Thousand, Two Hundred Eighty Seven Dollars ($22,287.00), U.S. Currency, 709 F.2d 442 (6th Cir. 1983)(rejecting suppression when agents began search "shortly after" 10 p.m., even though Rule 41 states that all searches must be conducted between 6:00 a.m. and 10 p.m.). This is especially true when the hardware to be searched was a container of contraband child pornography, and therefore was itself an instrumentality of crime that was not subject to return.

## J. EPO# 10: DESCRIBE SPECIAL ISSUES INVOLVING AUTHENTICATION OF INFORMATION CONTAINED ON COMPUTERS

**Note to instructors.**

**Section 1, below, is taken directly from the Courtroom Evidence lesson plan, master EPO 1121-6. For those students who do not have grounding in evidentiary foundations, these *optional* paragraphs may be necessary.**

1. **Optional Introductory Material**

   a. Evidence must be authenticated to be admissible. There is a general legal requirement that evidence must be authenticated before it can be admitted into evidence at a trial.

   b. Authentication shows there is some evidence to prove that the item is what the person offering it claims it to be.

   c. The process of authenticating evidence is called "laying a foundation."

   d. In court, the AUSA will lay a foundation authenticating the evidence.

   e. The facts the AUSA uses to lay a foundation are those collected by agents and officers.

   f. Laying a foundation - the big picture. The goal is to collect and handle evidence in such a way that it will satisfy the Rules of Evidence and be admitted into evidence. If a proper foundation cannot be laid, the evidence is not admissible, no matter how valuable it might be.

g. A foundation must be laid for all physical evidence offered in court through the testimony of a witness with personal knowledge. The exception would be that evidence which is self-authenticating - certain government documents or business records - that will be discussed later in some programs.

h. Legal admissibility and "the weight of the evidence."

1) Even if the judge admits an item into evidence, it does not mean the jury has to accept it or place any value on it. For example, though a judge may admit a gun into evidence, it does not mean the jury has to accept that the gun was the one that was found at the scene or the one that killed the victim.

2) The judge only decides whether to admit the evidence. The jury decides what weight, if any, to place on it.

3) LEOs must remember that in collecting evidence, they need not only satisfy technical rules of admissibility, they should also collect and preserve evidence in such a way that the jury will accept it as THE item.

4) Laying a foundation for physical evidence in court by the AUSA - the process.

a) Exhibit marked. When the prosecution or the defense wants to have a physical object admitted into evidence, it is marked as an exhibit.

b) Foundation with witness who has personal knowledge. The party offering the exhibit into evidence is then required to lay a foundation for that exhibit using a witness with personal knowledge. When agents seize evidence, they are usually the ones who will testify to lay the foundation.

i. Satisfying the legal admissibility requirements (FRE). A proper foundation consists of evidence - usually in the form of testimony - that the item is what the party offering claims it to be. In other words, the lawyer cannot simply claim, "This is the gun that was found at the scene," or "The defendant prepared this fraudulent document." There must be some evidence that the exhibit is what it is claimed to be.

2. **Issues Surrounding the Authentication of "Digital Evidence."** Let's call the data that is pulled from computer "digital evidence." Remember that the actual digital evidence is nothing but an electronic series of 0s and 1s that are interpreted by a computer program. Below are some of the special, significant challenges in having digital evidence admitted into court:

   a. Were the records altered, manipulated, or damaged after they were created?

   b. Who was the author of the record?

   c. Was the program that converted the digital evidence to words or graphics reliable?

3. **A Proper Foundation Can Defeat Claims of Alteration.** To have any evidence admitted in court, it must be authenticated. Authentication means there is information that can be presented in court to prove that what the person offering the evidence claims it to be is what it in fact is. If there is sufficient information that the jury could conclude the evidence is what the offeror claims, it is admitted and the jury may consider it.

4. **Establishing Authorship of the Record**

   a. Where was the storage device (drive, disk, or other medium) found?

   b. What was the access of others to the storage devices/medium?

   c. Trace evidence on storage devices/computer components.

   d. Passwords/screen names/chat names and who owned or had access to them.

   e. Names of folders and labels upon which the data was contained.

   f. Authorship tools that embed names of people who created or modified documents.

   g. Source of e-mails that contain attachments.

   h. Circumstantial evidence that the alias used is attributable to a particular person. *See, e.g.*, United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998)(identity of suspect as chat room person accomplished by associating what the suspect told the FBI with corroboration that suspect accessed the Internet at the times of the chats).

5. **Reliability of the Computer Program.** Computer records can be altered easily, and opposing parties may allege that computer records lack authenticity because they have been tampered with or changed after they were created. A few things can be done to reduce this possibility.

   a. **Metadata.** A computer not only creates files in which data are stored, while it is doing so it also creates “metadata” files. Metadata is defined as “data about data.” Metadata includes such information as when a particular file was created, by which user of a computer, and whether the file has been subsequently accessed or altered. It will also associate certain file types with the software designed to create and read them. It is, therefore, important to seize the computer software to show computer generated "associations" between particular file types and software. Having the program that creates the data goes a long way to prove the same program will accurately print it out.

   b. **Hashing Codes.** A hashing code is an algorithm. More simply, it is a method by which the metadata associated with a file may be ascertained. Hashing codes are like a fingerprint that, as of the creation of an electronic file, becomes permanent until such time as that file is later altered. Hashing software is especially useful in demonstrating, for purposes of evidence authentication, that the electronic file being offered as evidence at trial is the same file that was previously seized by the government.

   c. **The Requirement of Trustworthiness.** The claim that the programs are unreliable can be overcome, so long as "the government provides sufficient facts to warrant a finding that the records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof …." United States v. Briscoe, 896 F.2d 1476, 1494 (7th Cir.), cert. denied sub nom. Usman v United States, 498 U.S. 863 (1990). Do users actually rely on the program that created the data?

6. **The Best Evidence Rule Requirement for an "Original."**

   a. Is the digital data (the 0s and 1s) an original so to satisfy the Best Evidence Rule? According to FRE 1001(3), the answer to that question is yes. This rule provides that, “[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an ‘original.’” *See, e.g.*, Doe v. United States, 805 F. Supp. 1513, 1517 (D. Hawaii 1992)(finding an accurate printout of computer data satisfies the Best Evidence Rule).

b. **Data + writing + proving contents of a writing = best evidence rule implications**.

1) The best evidence rule provides that to prove the contents of a writing, one must have the original. The original of data will be a writing, and when officers go to court to offer data into evidence, they must have either a printout of the data or in some other way be able to show the data to the judge or jury.

2) Officers cannot come to court and say (unless there is a best evidence rule exception), "I saw an email on the computer screen and here is what it said." The officer must have either the email, or do something to display the data to the judge or jury in visible form.

3) *Case examples*:

a) In United States v. Bennett, 363 F.3d 947 (9th Cir.), cert. denied 543 U.S. 950 (2004). In *Bennett*, the defendant was charged with importing drugs into the U.S. on a vessel. Law enforcement did not see the vessel cross from Mexican to U.S. waters. When the vessel was boarded, agents discovered a GPS device on board and called up the "back-track" feature which provided a display of where the vessel had recently been. An agent testified about what he saw on the GPS display to support the importation charge because the device showed the vessel had moved into U.S. waters. The actual device (original), a printout of the data (also defined as an original), or data downloaded from the device (also an original or duplicate depending on how it was done) was neither offered into evidence nor its absence explained. The court found that what the witness saw on the GPS display was a graphical representation - the equivalent of a writing - and therefore subject to the best evidence rule. Since the witness' testimony was to prove the contents of the writing (the GPS display), the best evidence rule applied. Since neither an original nor a duplicate was offered, and the absence of the original or duplicate was inadequately addressed, the trial court erroneously overruled the defense best evidence objection. On appeal, the importation charged was reversed and the possession charge upheld.

b) In United States v. Jackson, 488 F. Supp. 2d 866 (D. Neb. 2007), agents were engaged in Internet chat sessions with the defendant. At trial, only certain portions of the chat log (cut and paste) were offered. Since these logs did not accurately reflect the chat-conversation (the writing on the computer screen), they were inadmissible in the face of a best evidence objection.

7. **Hearsay and Computer Evidence.** To admit the documents retrieved into evidence for the "truth of the matter asserted," we must find a hearsay exception. Whether the hearsay rules apply depends on whether the document is one generated by a computer or contains statements of a human being.

a. **Statements of Human Beings on a Computer.** Documents by human beings stored on a computer are potentially hearsay if the document is offered into evidence for the "truth of the matter asserted." Of course, if the document is a statement of the defendant, it is excluded from the definition of hearsay. The Federal officer must still prove it was the defendant's statement.

b. **Records Generated By a Computer Are NOT Hearsay.** Hearsay rules apply only to statements of human beings. A record generated by a computer from computer data (phone billings, bank statements and the like) are admissible if they are authenticated as business records.

c. **Other "Statements" Seized From a Computer.** Other "statements" that are seized from a computer must meet a hearsay exception or the author who can authenticate and testify to the statement is located. Therefore, a letter found on the computer from someone other than the defendant must meet hearsay exceptions before the contents of the letter can be admitted for the truth of the matter asserted.

## K. EPO # 11: DESCRIBE SPECIAL CONSIDERATIONS SHOULD PRIVILEGED INFORMATION OR PRIVACY PROTECTION ACT MATERIALS BE SOUGHT OR ENCOUNTERED DURING A SEARCH OF COMPUTERS.

1. **Privileged Matters Generally.** Certain communications between an attorney and client, and between a member of the clergy and their communicants, are privileged. In addition, under the policy of the Department of Justice, the communications between physicians and their patients (and not just between psychotherapists and their patients) are given a privileged status.

a. **Privileged Materials of People Unconnected to the Investigation.** In searching a computer, law enforcement officers may encounter privileged materials pertaining to people or matters that are unconnected to the matter under investigation. For example, if investigating a patient for fraudulent Medicare claims, agents may seize the computer of the target's treating physician where the physician is not a knowing participant in the target's activities. The data on the computer, however, may contain the medical records of legitimate patients whose billings were not fraudulent. If privileged matters unconnected to the investigation might be seized, special precautions must be taken to ensure that agents seize or review only those matters that are relevant to the investigation and within the scope of the search warrant. Those precautions should include:

1) **The Attorney General's Regulations.** Agents should ensure that the search will not violate the Attorney General's regulations relating to obtaining confidential information from disinterested third parties.

2) **A Strategy for Ensuring No Breach of the Regulations Occurs.** Agents should devise a strategy for reviewing the seized computer files following the search so that no breach of a privilege occurs.

b. **Disinterested Parties.** Federal Rule of Criminal Procedure 41(b) and Warden v. Hayden, 387 U.S. 294 (1967) permit law enforcement officers to seize "mere evidence" of a crime to include evidence in the hands of an innocent person who might not have committed a criminal act. For example, if a criminal sent a letter to an innocent friend admitting to criminal conduct, law enforcement could obtain a warrant to seize the letter from the innocent friend as evidence of a crime committed by another. In some investigations, law enforcement officers may wish to search the computers of persons who they do not believe have committed a crime but whose computers contain evidence of a crime. When these "non-targets" (disinterested parties) of such a search are attorneys, physicians, or members of the clergy, agents must follow special precautions to obtain and execute the warrant. This is because the computers or other files of innocent persons may contain privileged information or information that is given other special protection.

c. **The Attorney General's Regulations Relating to Searches of Disinterested Lawyers, Physicians, and Clergymen.** Agents must be careful if they plan to search the office of a doctor, lawyer, or member of the clergy who is not implicated in the crime under investigation. At Congress's direction, the Attorney General has issued guidelines for federal officers who want to obtain documentary materials from such disinterested third parties. *See* Title 42 U.S.C. § 2000aa-11(a); 28 C.F.R. § 59.4(b) (Attachment 8).

1) **When Search Warrants Should Be Used.** Under these rules, federal law enforcement officers should not use a search warrant to obtain documentary materials believed to be in the private possession of a disinterested third party physician, lawyer, or clergyman where the material sought or likely to be reviewed during the execution of the warrant contains confidential information on patients, clients, or parishioners. *See* 28 C.F.R. § 59.4(b). The regulation does contain a narrow exception. A search warrant can be used if:

a) **Using less intrusive means would substantially jeopardize the availability or usefulness of the materials sought;**

b) **Access to the documentary materials appears to be of substantial importance to the investigation; and**

c) **The application for the warrant has been recommended by the U.S. Attorney and approved by the appropriate Deputy Assistant Attorney General.** *See* 28 C.F.R. § 59.4(b)(1) and (2).

2) **Factors to Decide the Process to Be Used.** 28 C.F.R. 59.4 lists factors to decide whether a subpoena or other means must be used before obtaining a search warrant is attempted. Those factors are:

a) **Whether Service Will Have An Adverse Result.** Whether it appears that the use of a subpoena or other alternative which gives advance notice of the government's interest in obtaining the materials would be likely to result in the destruction, alteration, concealment, or transfer of the materials sought. Considerations, among others, that may bear on this issue include:

(1) Whether a suspect has access to the materials sought;

(2) Whether there is a close relationship of friendship, loyalty, or sympathy between the possessor of the materials and a suspect;

(3) Whether the possessor of the materials is under the domination or control of a suspect;

(4) Whether the possessor of the materials has an interest in preventing the disclosure of the materials to the government;

(5) Whether the possessor's willingness to comply with a subpoena or request by the government would be likely to subject him to intimidation or threats of reprisal;

(6) Whether the possessor of the materials has previously acted to obstruct a criminal investigation or judicial proceeding or refused to comply with or acted in defiance of court orders; or

(7) Whether the possessor has expressed an intent to destroy, conceal, alter, or transfer the materials.

b) **The Immediacy of the Government's Need to Obtain the Materials.** Considerations, among others, that may bear on this issue include:

(1) Whether the immediate seizure of the materials is necessary to prevent injury to persons or property;

(2) Whether the prompt seizure of the materials is necessary to preserve their evidentiary value;

(3) Whether delay in obtaining the materials would significantly jeopardize an ongoing investigation or prosecution; or

(4) Whether a legally enforceable form of process, other than a search warrant, is reasonably available as a means of obtaining the materials.

3) **Follow the Guidelines.** When planning to search the offices of a lawyer under investigation, agents should follow the guidelines offered in the United States Attorney's Manual, and should consult the Office of Enforcement Operations at (202) 514-3684. *See* United States Attorney's Manual, § 9-13.420 (Attachment 7).

4) **Strategies For Reviewing Privileged Computer Files of Disinterested Persons.** Agents contemplating a search that may result in the seizure of legally privileged computer files should devise a *post-seizure strategy* for screening out the privileged files and should describe that strategy in the affidavit. The goal is to minimize, as much as possible, the amount of privileged material that will be turned over to agents and prosecutors. This strategy must be included in the warrant not only to properly secure Department of Justice approval, but also to ensure the judge issuing the search warrant knows the efforts being taken to avoid divulging privileged information about others.

a) **The United States Attorney's Manual.** The United States Attorney's Manual, § 9-13.420, establishes guidelines that must be followed when agents seize a computer that contains legally privileged files. The provision requires that a trustworthy third party comb through the files to separate those files within the scope of the warrant from files that contain privileged material. After reviewing the files, the third party will offer those files within the scope of the warrant to the prosecution team. Preferred practices for determining who comb through the files will vary widely among different courts. There are three options.

(1) ***In Camera* Review.** First, the court itself may review the files *in camera*, that is, where the judge will review the files by himself or herself in the privacy of chambers. This is done infrequently. *See* Black v. United States, 172 F.R.D. 511, 516-17 (S.D. Fla. 1997)(accepting *in camera* review given unusual circumstances); United States v. Skeddle, 989 F. Supp. 890, 893 (N.D. Ohio 1997)(declining *in camera* review).

(2) **Appointment of a "Special Master."** Second, the presiding judge may appoint a neutral third party known as a "special master" to the task of reviewing the files. This can often take a very long time to accomplish, and prosecutors try to avoid this process.

(3) **Use of a "Taint" Team.** Third, a team of prosecutors who are not working on the case may form a "taint team" or "privilege team" to help execute the search and review the files afterwards. The taint team sets up a so-called "Chinese Wall" between the evidence and the prosecution team, permitting only unprivileged files that are within the scope of the warrant to slip through the wall. Most prosecutors will prefer to use a taint team if the court consents because a taint team can usually screen through the seized computer files fairly quickly. Some courts, however, have expressed discomfort with taint teams. *See* United States v. Neill, 952 F. Supp. 834, 841 n.14 (D.D.C. 1997); United States v. Hunter, 13 F. Supp.2d 574, 583 n.2 (D. Vt. 1998) (stating that review by a magistrate judge or special master "may be preferable" to reliance on a taint team). Although no single standard has emerged, these courts have generally indicated that evidence screened by a taint team will be admissible only if the government shows that its procedures adequately protected the defendants' rights and no prejudice occurred.

b) **The Composition of Taint Teams.** Taint teams need skilled and neutral technical experts to assist in sorting, identifying, and analyzing the evidence to identify what is within the scope of the warrant and what is privileged and will not be further divulged. The agents who seized the evidence or are engaged in the investigation, as well as the prosecutors who are assigned to the case, will not be on the taint team. Agents working the actual case must be careful not to learn of information, even inadvertently, that the taint team does not release. Doing so can jeopardize the investigation and prosecution.

d. **Targets.** If the person who holds the documents sought is not "disinterested," but is, instead, a target of the investigation, the rules are different. In the case of a search of the target's computer, agents may get a warrant to search the files for confidential information (regardless of whether that information is technically "privileged" under Federal law), but the warrant should be drawn as narrowly as possible to include only information specifically about the case under investigation.

1) **Where the Target Has Complete Control Over the Computer to Be Searched.** When the target of an investigation has complete control of the computer to be searched (such as a stand-alone PC), it may be difficult to find all the evidence without examining the entire disk drive or storage diskettes. Even in situations like these, it may be possible to get other people in the suspect's office to help locate the pertinent files without examining everything. When a computer must be removed from the target's premises to examine it, agents must take care that other investigators avoid reading confidential files unrelated to the case. Before examining everything on the computer, analysts should try to use other methods to locate only the material described in the warrant.

2) **Privileged Information Regarding Others.** Just as searches of computers of disinterested persons that might reveal privileged information requires a post-seizure search strategy, so does a warrant involving searching a target's computer that might contain privileged material of another. If agents anticipate encountering privileged files of person not connected to the crime under investigation, agents must arrange for the privileged files to be reviewed by a neutral, third party as previously described.

2. **The Privacy Protection Act (PPA), Title 42 U.S.C. § 2000aa.** The PPA was passed because of Congressional concern about the ability and willingness of law enforcement officers to seize information held by the media. For example, if the media published a story saying that a certain person committed a crime, agents were able to subpoena the information or obtain a search warrant to locate it. The original intent of the statute was to afford some protections to those engaged in First Amendment activities with respect to freedom of the press. The statute, however, has been interpreted and applied more expansively.

a. **The Intent of the PPA.** As indicated, the PPA was intended to grant publishers certain statutory rights to discourage law enforcement officers from targeting publishers simply because they often gathered "mere evidence" of crime. As the legislative history indicates, "the purpose of this statute is to limit searches for materials held by persons involved in First Amendment activities **who are themselves not suspected of participation in the criminal activity for which the materials are sought**, and not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation." (Emphasis supplied)

b. **Searches That Implicate the PPA.** When agents have reason to believe that a search may result in a seizure of materials relating to First Amendment activities, such as publishing or posting materials on the World Wide Web, they must consider the effect of the Privacy Protection Act , Title 42 U.S.C. § 2000aa. Every federal computer search that implicates the PPA must be approved by the Deputy Assistant Attorney General of the Criminal Division, coordinated through the Computer Crime and Intellectual Property Section at (202) 514-1026.

c. **An Overview of the PPA.** It is essential that agents remember that the PPA protects people involved in First Amendment activities, and not persons who themselves are suspected of criminal activity. Subject to certain exceptions, the PPA makes it unlawful for a government officer "to search for or seize" materials if they fall into one of two categories:

1) **Work Product Materials.** Subject to certain exceptions, the PPA makes it unlawful for a government officer "to search for or seize" materials when:

a) **Public Communications.** The materials are "work product materials" prepared, produced, authored, or created "in anticipation of communicating such materials to the public," (newspaper, books, broadcasts, or similar forms of public communication.)

b) **Mental Impressions.** The materials include "mental impressions, conclusions, or theories" of its creator ("work product" defined); ***and***

c) **Possessor Intends to Disseminate.** The materials are possessed for the purpose of communicating the material to the public by a person "reasonably believed to have a purpose to disseminate to the public" some form of "public communication."

d) **Examples of PPA/Work Product Materials**:

(1) A newspaper article the creator intends to have published - draft or final.

(2) A web page the creator intends to post to the Internet.

(3) A speech a person intends to give on radio or TV.

(4) A letter to the editor the creator intends to send to his local newspaper.

(5) A draft of a newsletter to fellow members of the local garden club.

2) **"Documentary Materials."** Subject to certain exceptions, the PPA makes it unlawful for a government officer "to search for or seize" materials when:

a) **Information Within.** The materials are "documentary materials" that contain "information"

b) **Possessor Intends to Disseminate.** The materials are possessed by a person "in connection with a purpose to disseminate to the public" some form of "public communication."

c) **"Documentary Materials" – Defined.** Documentary materials are those "upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, motion picture films, negatives, video tapes, audio tapes, and other mechanically, magnetically or electronically recorded cards, tapes, or disks."

d. **Exceptions to the PPA.** As with any rule, there are exceptions. The following are exceptions to the PPA.

1) **Rule 41(c) Materials.** Neither documentary materials nor work product materials include "contraband or the fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or which has been used, as the means of committing a criminal offense."

2) **Prevention of Death or Serious Bodily Injury.** There is reason to believe that the immediate seizure of such materials is necessary to prevent death or serious bodily injury.

3) **Probable Cause Possessor Has Committed or is Committing a Crime.** There is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate.

4) **A Subpoena Has Proven Inadequate.** In a search for or seizure of "documentary materials," a subpoena has proven inadequate or there is reason to believe that a subpoena would not result in the production of the materials, *see* § 2000aa(b)(3)-(4).

5) **Examples of Exceptions.** Examples applying the exceptions when the target's computer contains:

   a) Child pornography images for posting on the Internet or in a magazine.

   b) A web page or newsletter promoting a fraud scheme.

   c) An advertisement to sell software to manufacture false identification documents.

e. **Remedies for Violating the PPA.** Violations of the PPA do not result in suppression of the evidence, but can result in civil damages against the government whose officers or employees execute the search. *See* § 2000aa-6(a),(d),(e); Davis v. Gracey, 111 F.3d 1472, 1482 (10th Cir. 1997).

f. **Application of the PPA to Computer Searches and Seizures.** PPA issues frequently arise in computer cases because of the wide-spread use of computers for publishing and the Internet - which is a form of "publishing." Today, anyone with a computer and access to the Internet may be a publisher who possesses PPA-protected materials on his or her computer. In addition, PPA issues arise frequently in computer cases in that the language of the statute does not explicitly rule out liability following *incidental* seizures of PPA-protected materials, and such seizures may inevitably result when agents search for and seize computer-stored contraband or evidence of crime that is commingled with PPA-protected materials.

1) **Incidental Seizures and Commingled Files.** Searches for child pornography images being published over the Internet have revealed that such businesses frequently support other publishing materials - such as drafts of adult pornography - that may be PPA-protected. The PPA protection can interfere with the ability to seize the contraband child pornography because the contraband may be commingled with PPA-protected materials on the business's computers. Seizing the computer for the contraband would necessarily result in the seizure of the PPA-protected materials. There is the concern the courts can interpret the statute to not only deter law enforcement from targeting innocent publishers for their evidence, but also affirmatively protects individuals from the incidental seizure of property that may be used in part for First Amendment activities.

2) **Some Courts Have Given a Broad Reading to the PPA.** Some courts have decided that the PPA language "to which the materials relate" should be read quite broadly and will allow incidental seizures of PPA materials. *See* United States v. Hunter, 13 F. Supp. 2d 574, 582 (D. Vt. 1998)(concluding that materials for weekly legal newsletter published by the defendant from his law office "relate" to the defendant's alleged involvement in his client's drug crimes when the former was inadvertently seized in a search for evidence of the latter).

a) **The PPA and "Incidental" Seizures.** At least one court has held law enforcement liable under the PPA for the ***incidental*** seizure of (and more particularly, failure to return) PPA-protected materials stored on a seized computer. In Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), aff'd on other grounds, 36 F.3d 457 (5th Cir. 1994), a district court held the United States Secret Service liable for the inadvertent seizure of PPA-protected materials possessed by Steve Jackson Games, Inc. ("SJG"). Although SJG was primarily a publisher of role-playing games, it also operated a network of thirteen computers that provided its customers with e-mail, published information about SJG products, and stored drafts of upcoming publications. The Secret Service executed a search of SJG's computers after learning that a system administrator of SJG's computers had been linked to a computer hacking incident under Secret Service investigation. Believing that the system administrator had stored evidence of the crime on SJG's computers, the Secret Service obtained a warrant and seized two of the thirteen computers connected to SJG's network, in addition to other materials. The Secret Service did not know that SJG's computers contained publishing materials until the day after the search. However, the Secret Service did not return the computers it seized until months later. At no time did the Secret Service believe that SJG itself was involved in the crime under investigation. The district court in Steve Jackson Games ruled that the Secret Service violated the PPA by continuing to hold SJG's seized property after it learned that the property included materials that SJG intended to disseminate to the public, including drafts of a book and magazine articles. Although the Secret Service had executed the search to find evidence of computer hacking, the incidental seizure and then retention of PPA-protected material constituted a prohibited seizure of "work product materials" and "documentary materials" according to Title 42 U.S.C. § 2000aa. Unfortunately, the boundaries of the PPA remain quite uncertain

in the wake of Steve Jackson Games.

b) **Searches That Could Implicate the PPA.** Agents and prosecutors who have reason to believe that a search may implicate the PPA should contact the Computer Crime and Intellectual Property Section at (202) 514-1026 or the Assistant U.S. Attorney designated as a Computer-Telecommunications Coordinator (CTC) in each district for more specific guidance.

## III. SUMMARY

### A. REVIEW OF PERFORMANCE OBJECTIVES

**NOTE: The instructor should review only those EPOs associated with the program.**

### B. REVIEW OF TEACHING POINTS

1. Summarize teaching points.
2. Plan time for asking and answering questions.

## IV. APPLICATION

### A. LABORATORY:

CITP students have a 2-hour "Data Warrant Lab." The Lab follows the 6-hour lecture. Instructions for completing the Data Warrant Lab are in the "Student Guide for Preparing Criminal Complaints, Arrest Warrants, and Search Warrants."

### B. PRACTICAL EXERCISE:

NONE

## TEST ITEM CONTROL SHEET (TICS)

**COURSE NUMBER:** 1380 **COURSE TITLE: ELECTRONIC LAW AND EVIDENCE**

**POINT OF CONTACT AND EXTENSION:** (b)(6) **Date**: Jun 2007

**Instructions:** If a course is taught in sessions, put the EXAM number (E01, E02, E03, etc…) that the EPO will be tested on in the EDT. If all EPO's are tested on one exam, place an X in each box instead of the exam number. Using the test item numbers EAD has provided, complete the table below. Every EPO tested by multiple choice exam must be represented in each set with **one** test item If an EPO is tested by PE or not tested at all put PE or NA in that corresponding EPO row in the program box. A TICS and EDT is required for all courses tested at all FLETC locations. Use more than one form if necessary.

### Exam Distribution Table (EDT)

Programs testing each EPO by multiple choice exam or PE

| EPO | Set A | Set B | Set C | Set D | SET E | UPTP | LMPT | CITP | ICE_D |
|---|---|---|---|---|---|---|---|---|---|
| 1. | 06025 | 06026 | 06027 | 10441 | | NA | NA | E05 | NA |
| 2. | 10444 | 06030 | 10442 | 06032 | | NA | NA | E05 | NA |
| 3. | 06033 | 06034 | 06035 | 06521 | | NA | NA | E05 | NA |
| 4. | 06037 | 06038 | 10446 | 06040 | | NA | NA | E05 | NA |
| 5. | 06041 | 06042 | 06043 | 10447 | | NA | NA | E05 | NA |
| 6. | NOT TESTED | | | | | NA | NA | NA | NA |
| 7. | 10440 | 06462 | 10445 | 06464 | | NA | NA | E05 | NA |
| 8. | 06465 | 06466 | 10438 | 10443 | | NA | NA | E05 | NA |
| 9. | 06469 | 06470 | 06471 | 06472 | | NA | NA | E05 | NA |
| 10. | 06473 | 06474 | 06475 | 06476 | | NA | NA | E05 | NA |
| 11. | NOT TESTED | | | | | NA | NA | NA | NA |

Implementation Instructions for EAD:

| Program Name | Date for item implementation | Use in all classes after class # | Special Instructions |
|---|---|---|---|
| **CITP** | **6-18-07** | **721** | |

## TABLE OF AUTHORITIES

## STATUTORY CITATIONS

All Writs Act, codified at Title 28 U.S.C. § 1651
Federal Rules of Criminal Procedures Rule 41
Federal Rules of Criminal Procedures Rule 54
Federal Rules of Evidence, 901
Federal Rules of Evidence, 1002-1004
18 USCS § 2510
18 USCS § 2701 et. seq.
Title 18 U.S.C. § 3105
Title 18 U.S.C. §3109
Title 18 U.S.C. § 3121 et seq.
Title 42 U.S.C. § 2000aa

## OTHER RULES AND OFFICIAL POLICY

28 C.F.R. Sec. 59.1.
US Attorney's Manual, Sec. 9-13.420

**CASE CITATIONS**


Abraham v. County of Greenville, 237 F.3d 386 (4th Cir. 2001)

Adams v. City of Battle Creek, 250 F.3d 980 (6th Cir. 2001)

American Postal Workers Union, Columbus Area Local AFL-CIO v. United States Postal Service, 871 F.2d 556 (6th Cir. 1989)

Andresen v. Maryland, 427 U.S. 463 (1976)

Arizona v. Gant, ____ U.S. _____, 129 S. Ct. 1710; 173 L. Ed. 2d 485 (2009)

Bartnicki v. Vopper, 532 U.S. 514 (2001)

Black v. United States, 172 F.R.D. 511 (S.D. Fla. 1997)

Brannum v. Overton County Sch. Bd., 516 F.3d 489 (6th Cir. 2008)

Brown v. Waddell, 50 F.3d 285 (4th Cir. 1995)

Campbell v. Price, 2 F. Supp. 2d 1186 (E.D. Ark. 1998)

Cardwell v. Lewis, 417 U.S. 583 (1974)

Chambers v. Maroney, 399 U.S. 42 (1970)

Chimel v. California, 395 U.S. 752 (1969)

Colorado v. Bertine, 479 U.S. 367 (1987)

Commonwealth v. Ellis, 1999 Mass. Super. LEXIS 368 (Mass. Super. 1999)

Company v. United States (In re United States), 349 F.3d 1132 (9th Cir. 2003)

Cornelius v. State, No. A03-704, 2004 Minn. App. LEXIS 149 (Minn. Ct. App. February 10, 2004)

Couch v. United States, 409 U.S. 322 (1973)

Curd v. City of Judsonia, 141 F.3d 839 (8th Cir.), cert. denied, 525 U.S. 888 (1998)

Dalia v. United States, 441 U.S. 238 (1979)

Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997)

Doe v. United States, 805 F. Supp. 1513 (D. Hawaii 1992)

Edwards v. Bardwell, 632 F. Supp. 584 (M.D. La.), aff'd without opinion 808 F.2d 54 (1986)

Fischer v. Mount Olive Lutheran Church, Inc., 207 F. Supp. 2d 914 (W.D. Wis. 2002)

Florida v. Jimeno, 500 U.S. 248 (1991)

Florida v. Wells, 495 U.S. 1 (1990)

Fountain v. United States, 384 F.2d 624 (5th Cir. 1968), cert. denied, 390 U.S. 1005 (1968)

Georgia v. Randolph, 126 S. Ct. 1515 (U.S. 2006)

Gouled v. United States, 255 U.S. 298 (1921)

Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001)

Hoffa v. United States, 385 U.S. 293 (1966)

Horton v. California, 496 U.S. 128 (1990)

Illinois v. Andreas, 463 U.S. 765 (1983)

Illinois v. Lafayette, 462 U.S. 640 (1983)

Illinois v. Rodriguez, 497 U.S. 177 (1990)

In re Application of the United States ("White Truck"), 155 F.R.D. 401 (D. Mass. 1994)

In re Askin, 47 F.3d 100 (4th Cir.), cert. denied, 516 U.S. 944 (1995)

In re Grand Jury Subpoena (Boucher), 2009 U.S. Dist. LEXIS 13006 (D. Vt. Feb. 19, 2009)

In re United States of America, 10 F.3d 931 (2d Cir. 1993), cert. denied, 513 U.S. 812 (1994)

Jacks v. Duckworth, 651 F.2d 480 (7th Cir. 1981), cert. denied, 454 U.S. 1147 (1982)

Katz v. United States, 389 U.S. 347 (1967)

Kee v. City of Rowlett, 247 F.3d 206 (5th Cir.), cert. denied, 534 U.S. 892 (2001)

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002), cert. denied, 537 U.S. 1193 (2003)

Lopez v. United States, 373 U.S. 427 (1963)

Mary Beth G. v. City of Chicago, 723 F.2d 1263 (7th Cir. 1983)

McCardle v. Haddad, 131 F.3d 43 (2d Cir. 1997)

McGann v. Northeast Illinois Regional Commuter R.R. Corp., 8 F.3d 1174 (7th Cir. 1993)

McKamey v. Roach, 55 F.3d 1236 (6th Cir. 1995)

Michigan v. Tyler, 436 U.S. 499 (1978)

Nat'l City Trading Corp. v. United States, 635 F.2d 1020 (2d Cir. 1980)

New York v. Class, 475 U.S. 106 (1986)

Olmstead v. United States, 277 U.S. 438 (1928)

Ontario v. Quon, __U.S.___ (slip op. 08-1332, June 17, 2010),

Pollock v. Pollock, 154 F.3d 601 (6th Cir. 1998)

Preston v. United States, 376 U.S. 364 (1964)

Price v. Turner, 260 F.3d 1144 (9th Cir. 2001)

Richards v. Wisconsin, 520 U.S. 385 (1997)

Roviaro v. United States, 353 U.S. 53 (1957)

Schneckloth v. Bustamonte, 412 U.S. 218 (1973)

Scott v. United States, 436 U.S. 128 (1978)

Securities and Law Enforcement Employees, District Council 82 v. Carey, 737 F.2d 187 (2d Cir. 1984)

Shell v. United States, 448 F.3d 951 (7th Cir. 2006)

Silvan W. v. Briggs, 2009 U.S. App. LEXIS 1520 (10th Cir. 2009)
Smith v. Maryland, 442 U.S. 735 (1979)
State of Ohio v. Smith, 920 N.E.2d 949 (2009).
South Dakota v. Opperman, 428 U.S. 364 (1976)
Spetalieri v. Kavanaugh, 36 F. Supp. 2d 92 (N.D.N.Y. 1998)
Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), aff'd on other grounds, 36 F.3d 457 (5th Cir. 1994)
Stoner v. California, 376 U.S. 483 (1964)
Swain v. Spinney, 117 F.3d 1 (1st Cir. 1997)
Thompson v. Dulaney, 838 F. Supp. 1535 (D. Utah 1993)
Tyler v. Berodt, 877 F.2d 705 (8th Cir. 1989)(per curiam), cert. denied, 493 U.S. 1022 (1990)
United States v. Adjani, 452 F.3d 1140 (9th Cir. 2006)
United States v. Alfonso, 759 F.2d 728 (9th Cir. 1985)
United States v. Andrus, 483 F.3d 711 (10th Cir. 2007)
United States v. Apodaca, 820 F.2d 348 (10th Cir. 1987)
United States v. Arnold, 454 F. Supp. 2d 999 (D. Cal. 2006)
United States v. Baftiri, 263 F.3d 856 (8th Cir. 2001)
United States v. Baltas, 236 F.3d 27 (1st Cir. 2001)
United States v. Barth, 26 F. Supp. 2d 929 (W.D. Texas 1998)
United States v. Bellosi, 501 F.2d 833 (D.C. Cir. 1974)
United States v. Bennett, 363 F.3d 947 (9th Cir.), cert. denied 543 U.S. 950 (2004)
United States v. Bianco, 998 F.2d 1112 (2d Cir. 1993), cert. denied, 511 U.S. 1069 (1994)
United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986), cert. denied, 479 U.S. 827 (1986)
United States v. Blackmon, 273 F.3d 1204 (9th Cir. 2001)
United States v. Blas, 1990 U.S. Dist. LEXIS 19961 (E.D. Wis. 1990)
United States v. Block, 590 F.2d 535 (4th Cir. 1978)
United States v. Brathwaite, 458 F.3d 376 (5th Cir. 2006)
United States v. Branch, 970 F.2d 1368 (4th Cir. 1992)
United States v. Briscoe, 896 F.2d 1476 (7th Cir.), cert. denied sub nom. Usman v United States, 498 U.S. 863 (1990)
United States v. Brookes, 2005 U.S. Dist. LEXIS 16844 (D.V.I. 2005)
United States v. Brown, 303 F.3d 582 (5th Cir. 2002), cert. denied, ___ U.S. ___, 123 S. Ct. 1003 (2003)
United States v. Brunette, 76 F. Supp. 2d 30 (D. Me. 1999), aff'd, 256 F.3d 14 (2001)

United States v. Bryant, 480 F.2d 785 (2d Cir. 1973)

United States v. Buckner, 473 F.3d 551 (4th Cir.), cert. denied cert. denied 550 U.S. 913.

United States v. Bullock, 71 F.3d 171 (5th Cir. 1995), cert. denied, 517 U.S. 1126 (1996)

United States v. Burke, 517 F.2d 377 (2d Cir. 1975)

United States v. Burkeen, 350 F.2d 261 (6th Cir.), cert. denied sub nom. Matlock v. United States (1965)

United States v. Burns, 624 F.2d 95 (10th Cir.), cert. denied, 449 U.S. 954 (1980)

United States v. Butts, 710 F.2d 1139 (5th Cir. 1983), rev'd en banc, 729 F.2d 1514 (5th Cir. 1984), cert. denied, 469 U.S. 855 (1984)

United States v. Campos, 221 F.3d 1143 (10th Cir. 2000)

United States v. Capers, 61 F.3d 1100 (4th Cir. 1995), cert. denied, 517 U.S. 1211 (1996)

United States v. Carey, 172 F.3d 1268 (10th Cir. 1999)

United States v. Caron, 474 F.2d 506 (5th Cir. 1973)

United States v. Carr, 805 F. Supp. 1266 (E.D.N.C. 1992)

United States v. Chan, 830 F. Supp. 531 (N.D. Cal. 1993)

United States v. Caymen, 404 F.3d 1196 (9th Cir. 2005)

United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997)

United States v. Charles, 213 F.3d 10 (1st Cir.), cert. denied, 531 U.S. 915 (2000)

United States v. Cintolo, 818 F.2d 980 (1st Cir.), cert. denied, 484 U.S. 913 (1987)

United States v. Cline, 2003 U.S. App. LEXIS 23792 (10th Cir. 2003)

United States v. Clark, 22 F.3d 799 (8th Cir. 1994)

United States v. Clark, 986 F.2d 65 (4th Cir. 1993)

United States v. Corleto, 2009 U.S. Dist. LEXIS 10826 (D. Utah Feb. 5, 2009)

United States v. Cote, 2005 U.S. Dist. LEXIS 11725 (D. Ill. 2005)

United States v. Craig, 573 F.2d 455 (7th Cir. 1977), cert. denied, 439 U.S. 820 (1978)

United States v. Cruz-Pagan, 537 F.2d 554 (1st Cir. 1976)

United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987)

United States v. David, 756 F. Supp. 1385 (D. Nev. 1991)

United States v. De Jesus Fierros-Alavarez, 547 F. Supp. 2d 1206 (D. Kan. 2008)

United States v. Denman, 100 F.3d 399 (5th Cir. 1996)

United States v. Doe, 61 F.3d 107 (1st Cir. 1995)

United States v. Donovan, 429 U.S. 413 (1977)

United States v. Dornblut, 261 F.2d 949 (2d Cir. 1958), cert. denied, 360 U.S. 912 (1959)

United States v. Dumes, 313 F.3d 372 (7th Cir. 2002)

United States v. Durham, 1998 U.S. Dist. LEXIS 15482 (D. Kan. 1998)

United States v. Echavarria-Olarte, 904 F.2d 1392 (9th Cir. 1990)

United States v. Edwards, 69 F.3d 419 (10th Cir. 1995), cert. denied, 517 U.S. 1243 (1996)

United States v. Ellis, 547 F.2d 863 (5th Cir. 1977)

United States v. Escobar-de Jesus, 187 F.3d 148 (1st Cir. 1999), cert. denied, 528 U.S. 1176 (2000).

United States v. Espinoza, 2007 U.S. Dist. LEXIS 25263 (D. Kan. 2007)

United States v. Falls, 34 F.3d 674 (8th Cir. 1994)

United States v. Finley, 477 F.3d 250 (5th Cir.), cert. denied,127 S. Ct. 2065, 167 L. Ed. 2d 790, 2007 U.S. LEXIS 4168 (2007)).

United States v. Flores, 122 F. Supp. 2d 491 (S.D.N.Y. 2000)

United States v. Ford, 986 F.2d 57 (4th Cir. 1993)

United States v. Foster, 100 F.3d 846 (10th Cir. 1996)

United States v. Frank, 864 F.2d 992 (3d Cir. 1988), cert. denied, 490 U.S. 1095 (1989)

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

United States v. Fudge, 325 F.3d 910 (7th Cir. 2003)

United States v. Fuentes, 105 F.3d 487 (9th Cir. 1997)

United States v. Gambino, 734 F. Supp. 1084, 1106 (S.D.N.Y. 1990)

United States v. Garcia, No. 05-CR-0155-C-01, 2006 U.S. Dist. LEXIS 6424 (W.D. Wis. February 16, 2006)

United States v. Garcia, No. 05-CR-155-C, 2006 U.S. Dist. LEXIS 29596 (W.D. Wis. May 10, 2006).

United States v. Garcia, No. 05-CR-155-C, 2006 U.S. Dist. LEXIS 4642 (W.D. Wis. February 3, 2006)

United States v. Garcia-Vallalba, 585F.3d 1223 (9th Cir. 2009)

United States v. Garcia, 474 F.3d 994 (7th Cir., 2007), certiorari denied, 2007 U.S. LEXIS 10567 (U.S., Oct. 1, 2007)

United States v. Gawrysiak, 972 F. Supp. 853 (N.J. 1997), aff'd without opinion 178 F.3d 1281 (1999)

United States v. Gaytan, 74 F.3d 545 (5th Cir. 1996)

United States v. Gbemisola, 225 F.3d 753 (D.C. Cir., 2000)

United States v. Giordano, 416 U.S. 505 (1974)

United States v. Gonzalez-Acosta, 989 F.2d 384 (10th Cir. 1993)

United States v. Gonzales-Benitez, 537 F.2d 1051 (9th Cir.), cert. denied, 429 U.S. 923 (1976)

United States v. Gordon, 688 F.2d 42 (8th Cir. 1982)

United States v. Gray, 78 F. Supp. 2d 524 (E.D. Va. 1999)

United States v. Griffiths, 47 F.3d 74 (2d Cir. 1995)

United States v. Groves, 530 F.3d 506 (7th Cir. 2008)

United States v. Hall, 142 F.3d 988 (7th Cir. 1998)

United States v. Hall, 583 F. Supp. 717 (E.D. Va. 1984)

United States v. Hallmark, 911 F.2d 399 (10th Cir. 1990)\

United States v. Hamilton, 334 F.3d 170 (2d Cir.), cert. denied, ___ U.S. ___, 124 S.Ct 502 (2003)

United States v. Hammond, 286 F.3d 189 (4th Cir), cert. denied, ___ U.S. ___, 123 S. Ct. 215 (2002)

United States v. Hargus, 128 F.3d 1358 (10th Cir. 1997), cert. denied, 523 U.S. 1079 (1998)

United States v. Harley, 682 F.2d 1018 (D.C. Cir. 1982)

United States v. Harris, No. 99-5435, 2001 U.S. App. LEXIS 3918 (6th Cir. March 7, 2001)

United States v. Hay, 231 F.3d 630 (9th Cir. 2000), cert. denied, 534 U.S. 858 (2001)

United States v. Henderson, 536 F.3d 776 (7th Cir. 2008)

United States v. Henson, 848 F.2d 1374 (6th Cir.1988), cert. denied, 488 U.S. 1005 (1989)

United States v. Hill, 459 F.3d (9th Cir. 2006)

United States v. Hoffman, 832 F.2d 1299 (1st Cir. 1987)

United States v. Holton, 116 F.3d 1536 (D.C. Cir. 1997), cert. denied, 522 U.S. 1067 (1998)

United States v. Hudspeth, 518 F.3d 954 (8th Cir. 2008)

United States v. Hufford, 539 F.2d 32 (9th Cir.), cert. denied, 429 U.S. 1002 (1976)

United States v. Hughes, 895 F.2d 1135 (6th Cir. 1990)

United States v. Hunter, 13 F. Supp. 2d 574 (D. Vt. 1998)

United States v. Inman, 558 F.3d 742 (8th Cir. Mo. 2009)

United States v. Jackson, 488 F. Supp. 2d 866 (D. Neb. 2007),

United States v. Jackson, 2007 U.S. Dist. LEXIS 23298 (D. Neb. Mar. 28, 2007)

United States v. Jacobsen, 466 U.S. 109 (1984)

United States v. James, 2008 U.S. Dist. LEXIS 34864 (E.D. Mo. Apr. 29, 2008)

United States v. Jones, 2006 U.S. Dist. LEXIS 56473 (D.D.C. 2006)

United States v. Kahn, 415 U.S. 143 (1974)

United States v. Karo, 468 U.S. 705 (1984)

United States v. Kennedy, 81 F. Supp. 2d 1103 (D. Kan. 2000)

United States v. Khanani, 502 F.3d 1281, 1290-91 (11th Cir. 2007)

United States v. Kimbrough, 69 F.3d 723 (5th Cir. 1995), cert. denied, 517 U.S. 1157 (1996)

United States v. King, 509 F.3d 1338 (11th Cir. 2007)

United States v. King, 2010 WL 1729733 (3rd Cir. 2010)

United States v. Knotts, 460 U.S. 276 (1983)

United States v. Koyomejian, 970 F.2d 536 (9th Cir.), cert. denied, 506 U.S. 1005 (1992)

United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996).

United States v. Lambert, 771 F.2d 83 (6th Cir.), cert. denied, 474 U.S. 1034 (1985)

*United States v. Larson*, 66 M.J. 212 (CAAF, 2008).

United States v. Lasalle, 2007 U.S. Dist. LEXIS 34233 (D. Haw. 2007)

United States v. Lavin, 1992 U.S. Dist. LEXIS 18163 (S.D.N.Y. 1992)

United States v. Le, 173 F.3d 1258 (10th Cir. 1999)

United States v. London, 66 F.3d 1227 (1st Cir. 1995), cert. denied, 517 U.S. 1155 (1996)

United States v. Longo, 70 F. Supp. 2d 225 (W.D.N.Y. 1999)

United States v. Longoria, 177 F.3d 1179 (10th Cir.), cert. denied, 528 U.S. 892 (1999)

United States v. Lopez, 300 F.3d 46 (1st Cir. 2002)

United States v. Lynch, 908 F. Supp. 284 (D.V.I. 1995)

United States v. Lyons, 992 F.2d 1029 (10th Cir. 1993)

United States v. Lyons, 2005 U.S. Dist. LEXIS 6963 (D. Kan. 2005)

United States v. Malekzadeh, 855 F.2d 1492 (11th Cir. 1988)

United States v. Mansoori, 304 F.3d 635 (7th Cir. 2002), cert. denied sub nom. Cox v. United States, ___ U.S. ___, 123 S. Ct. 1761 (2003)

United States v. Martin, 920 F.2d 393 (6th Cir. 1990)

United States v. Martinez-Zetas, 857 F.2d 122 (3d Cir. 1988)

United States v. Matias, 836 F.2d 744 (2d Cir. 1988)

United States v. Matlock, 415 U.S. 164 (1974)

United States v. Maxwell, 383 F.2d 437 (2d Cir. 1967), cert. denied, 389 U.S. 1043 (1968)

United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996)

United States v. Megahed, 2009 U.S. Dist LEXIS 24441 (M.D. Fla., 2009)

United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1273 (D. Kan. 2007)

United States v. McGuire, 307 F.3d 1192 (9th Cir. 2002)

United States v. McIntyre, 836 F.2d 467 (10th Cir. 1987)

United States v. Mitchell, 2009 U.S. App. LEXIS 8258 (11th Cir. Ga. Apr. 22, 2009)

United States v. McIver, 186 F.3d 1119 (9th Cir. 1999), cert. denied, 528 U.S. 1177 (2000)

United States v. McKeever, 169 F.Supp. 426 (S.D.N.Y. 1958), rev'd on other grounds, 271 F.2d 669 (2d Cir. 1959)

United States v. McKerrell, 491 F.3d 1221 (10th Cir. 2007), certiorari denied by McKerrell v. United States, 169 L. Ed. 2d 387, 2007 U.S. LEXIS 11967 (U.S., Nov. 5, 2007)

United States v. McKinnon, 985 F.2d 525 (11th Cir.), cert. denied, 510 U.S. 843 (1993)

United States v. Mercado-Nava, 486 F. Supp. 2d 1271 (D. Kan. 2007)

United States v. Merritt, 1998 U.S. App. LEXIS 7807 (4th Cir. 1998)

United States v. Mesa-Rincon, 911 F.2d 1433 (10th Cir. 1990)

United States v. Michael, 645 F.2d 252 (5th Cir.)(en banc), cert. denied, 454 U.S. 950 (1981)

United States v. Miller, 116 F.3d 641 (2d Cir. 1997), cert. denied, 524 U.S. 905 (1998)

United States v. Moore, 562 F.2d 106 (1st Cir. 1977)

United States v. Moran, 349 F. Supp. 2d 425 (D.N.Y. 2005)

United States v. Muniz-Melchor, 894 F.2d 1430 (5th Cir. 1990), cert. denied, 495 U.S. 923 (1990)

United States v. Murphy, 506 F.2d 529 (9th Cir. 1974)(per curiam)

United States v. Murphy, 516 F.3d 1117 (9th Cir. 2008)

United States v. Murphy, 552 F.3d 405 (4th Cir. 2009)

United States v. Nelson-Rodriguez, 319 F.3d 12 (1st Cir. 2003)

United States v. New York Tel. Co., 434 U.S. 159 (1977)

United States v. Park, 2007 U.S. Dist. LEXIS 40596 (NDCA May 23, 2007)

United States v. Payton, ___ F.3d ___, 2009 WL 2151348 (9th Cir. July 21, 2009)

United States v. Onori, 535 F.2d 938 (5th Cir. 1976)

United States v. O'Razvi, 1998 U.S. Dist. LEXIS 10860 (S.D.N.Y. 1998), aff'd without opinion 173 F. 3d 847 (2d Cir. 1999)

United States v. Ortiz, 84 F.3d 977 (7th Cir), cert. denied, 519 U.S. 900 (1996)

United States v. Ozar, 50 F.3d 1440 (8th Cir.), cert. denied, 516 U.S. 871 (1995)

United States v. Parada, 289 F. Supp. 2d 1291 (D. Kan. 2003)

United States v. Park, 2007 U.S. Dist. LEXIS 40596 (D. Cal. 2007)

United States v. Peterson, 294 F. Supp. 2d 797 (D.S.C. 2003), affirmed 145 Fed. Appx. 820 (4th Cir. 2005)

United States v. Petti, 973 F.2d 1441 (9th Cir. 1992), cert. denied, 507 U.S. 1035 (1993)

United States v. Pineda-Areola, 2010 U.S. App. LEXIS 7685 (7th Cir. April 6, 2010)

United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010)

United States v. Pinelli, 890 F.2d 1461 (10th Cir. 1989), cert. denied, 493 U.S. 960 (1990)

United States v. Price, 599 F.2d 494 (2d Cir. 1979)

United States v. Rascon-Ortiz, 994 F.2d 749 (10th Cir. 1993)

United States v. Radcliff, 331 F.3d 1153 (10th Cir. 2003)

United States v. Ramirez, 112 F.3d 849 (7th Cir. 1997)

United States v. Ramirez, 523 U.S. 65 (1998)

United States v. Ramirez-Encarnacion, 291 F.3d 1219 (10th Cir. 2002)

United States v. Reed, 935 F.2d 641 (4th Cir. 1991)

United States v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996)

United States v. Riley, 906 F.2d 841 (2d Cir. 1990)

United States v. Roberts, 86 F. Supp. 2d 678 (S.D. Tex. 2000)

United States v. Robertson, 15 F.3d 862 (9th Cir. 1994), rev'd on other grounds, 514 U.S. 945 (1995)

United States v. Robinson, 414 U.S. 218 (1973)

United States v. Rocha, 2008 U.S. Dist. LEXIS 77973 (D. Kan. Oct. 2, 2008)

United States v. Romero-Garcia, 991 F. Supp. 1223 (D. Or. 1997), aff'd on other grounds 168 F.3d 502 (9th Cir. 1999)

United States v. Ross, 456 U.S. 798 (1982)

United States v. Ross, 33 F.3d 1507 (11th Cir. 1994), cert. denied, 515 U.S. 1132 (1995)

United States v. Sanchez, 689 F.2d 508 (5th Cir. 1982)

United States v. Santarelli, 778 F.2d 609 (11th Cir. 1985)

United States v. Sergeant, 319 F.3d 4 (1st Cir. 2003)

United States v. Savides, 658 F. Supp. 1399 (N.D. Ill. 1987), aff'd in relevant part sub. nom. United States v. Pace, 898 F.2d 1218 (7th Cir. 1990)

United States v. Schandl, 947 F.2d 462 (11th Cir. 1991), cert. denied, 504 U.S. 975 (1992)

United States v. Shaffer, 472 F.3d 1219 (10th Cir. 2007)

United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998)

United States v. Skeddle, 989 F. Supp. 890 (N.D. Ohio 1997)

United States v. Smith, 27 F. Supp. 2d 1111 (C.D. Ill. 1998)

United States v. Smith, 31 F.3d 1294 (4th Cir. 1994), cert. denied, 513 U.S. 1181 (1995)

United States v. Smith, 978 F.2d 171 (5th Cir. 1992), cert. denied, 507 U.S. 999 (1993)

United States v. Solis-Jordan, 223 F.3d 676 (7th Cir. 2000)

United States v. Steiger, 318 F.3d 1039 (11th Cir.), cert. denied, 583 U.S. 1051 (2003)

United States v. Streetman, 207 Fed. Appx. 414 (5th Cir. 2006)

United States v. Strickland, 902 F.2d 937 (11th Cir. 1990)

United States v. Sumlin, 567 F.2d 684 (6th Cir. 1977)

United States v. Tamura, 694 F.2d 591 (9th Cir. 1982)

United States v. Tangeman, 30 F.3d 950 (8th Cir.), cert. denied, 513 U.S. 1009 (1994)

United States v. Thomas, 114 F.3d 403 (3d Cir. 1997)

United States v. Thompson, 936 F.2d 1249 (11th Cir. 1991), cert. denied, 502 U.S. 1075 (1992)

United States v. Torres, 751 F.2d 875 (7th Cir. 1984), cert. denied, 470 U.S. 1087 (1985)

United States v. Traficant, 558 F. Supp. 996 (N.D. Oh. 1983)

United States v. Trots, 152 F.3d 715 (7th Cir. 1998)

United States v. Turner, 209 F.3d 1198 (10th Cir.), cert. denied, 531 U.S. 887 (2000)

United States v. Turner, 169 F.3d 84 (1st Cir. 1999)

United States v. Turner, 926 F.2d 883 (9th Cir.), cert. denied, 502 U.S. 830 (1991)

United States v. Tutino, 883 F.2d 1125 (2d Cir. 1989), *cert. denied*, 493 U.S. 1081 (1990).

United States v. Upham, 168 F.3d 532 (1st Cir.), cert. denied, 527 U.S. 1011 (1999)

United States v. Uriel Montejano Zamora, 2006 U.S. Dist. LEXIS 8196 (D. Ga. 2006)

United States v. Uribe, 890 F.2d 554 (1st Cir. 1989)

United States v. Vanmeter, 278 F.3d. 1156 (10th Cir. 2002)

United States v. Van Horn, 789 F.2d 1492 (11th Cir.), cert. denied, 479 U.S. 854 (1986)

United States v. Vasey, 834 F.2d 782 (9th Cir. 1987)

United States v. Vastola, 670 F. Supp. 1244 (D.N.J. 1987)

United States v. Villarreal, 963 F.2d 770 (5th Cir. 1992)

United States v. Wall, 2008 U.S. Dist. LEXIS 103058 (SDFL December 22, 2008)

United States v. Walser, 275 F.3d 981(10th Cir. 2001)

United States v. Walters, 558 F. Supp. 726 (D. Md. 1980)

United States v. Webster, 750 F.2d 307 (5th Cir. 1984), cert. denied, 471 U.S. 1106 (1985)

United States v. West, 948 F.2d 1042 (6th Cir. 1991), cert. denied, 502 U.S. 1109 (1992)

United States v. White, 401 U.S. 745 (1972)

United States v. Wilkinson, 754 F.2d 1427 (2d Cir.), cert. denied, 472 U.S. 1019 (1984)

United States v. Workinger, 90 F.3d 1409 (9th Cir. 1996)

United States v. Yonn, 702 F.2d 1341 (11th Cir.), cert. denied, 464 U.S. 917 (1983)

United States v. Young, 877 F.2d 1099 (1st Cir. 1989)

United States v. Young, 278 Fed. Appx. 242 (4th Cir., 2008), cert. denied, 2008 U.S. LEXIS 8016

United States v. Zannino, 895 F.2d 1 (1st Cir.), cert. denied, 494 U.S. 1082 (1990)

United States v. Ziegler, 456 F.3d 1138 (9th Cir. 2006)

United States Telecom Ass'n v. Federal Communications Commission, 227 F.3d 450 (D.C. Cir. 2000)

Vaughn v. Baldwin, 950 F.2d 331 (6th Cir. 1991)

Vieux v. Pepe, 184 F.3d 59 (1st Cir. 1999)

Walter v. United States, 447 U.S. 649 (1980)

Warden v. Hayden, 387 U.S. 294 (1967)

Wheeler v. State, No. 05-94-01957-CR, 1996 Tex. App. LEXIS 2546 (Tex. App. June 26, 1996)

Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993)

Wilson v. Arkansas, 514 U.S. 927 (1995)

Wright v. Farmers Co-op, 681 F.2d 549 (8th Cir. 1982)

Yu v. United States, 1997 U.S. Dist. LEXIS 10884 (S.D.N.Y. 1997)

## BIBLIOGRAPHY


1. "Attachment or Use of Transponder (Beeper) to Monitor Location of Airplane or Automobile as Constituting 'Search' Within Fourth Amendment," 57 A.L.R. Fed. 646 (2000)

2. "Police Surveillance Privilege," 67 A.L.R. 5th 149 (2001)

3. "Cyber Crime Fighting: The Law Enforcement Officer's Guide to Online Crime," The National Cyber Crime Training Partnership (1996)

4. Fishman, Clifford S. and McKenna, Anne T. Wiretapping and Eavesdropping, 2d ed. New York: Clark, Boardman, Callaghan, 1995.

5. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice (January 2001)

6. United States Attorney's Manual (USAM), Chapter 9

7. Milazzo, Carl, T*he State of Third Party Consent After Georgia v. Randolph, The Informer*, October 2008

8. *Government Surveillance in Context, for E-mails, Location, and Video: Personal Privacy in the Face of Government Use of GPS,* 3 ISJLP 473 (2008)

## INDEX OF ATTACHMENTS

NOTE: Attachments 1-4, and attachment 6 were copied directly from the Department of Justice publication, “Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,” Computer Crime and Intellectual Property Section, Criminal Division (January 2001).

**Sample**

UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

| | | |
|---|---|---|
| | ) | |
| IN RE APPLICATION OF THE | ) | |
| UNITED STATES OF AMERICA FOR | ) | MISC. NO. _____ |
| AN ORDER PURSUANT TO | ) | |
| TITLE 18 U.S.C. § 2703(d) | ) | **Filed Under Seal** |

APPLICATION

[Name], an Assistant United States Attorney for the _____ District of _____, hereby files under seal this *ex parte* application for an order pursuant to Title 18 U.S.C. Section 2703(d) to require [Internet Service Provider], [mailing address], to provide records and other information pertaining to the [Internet Service Provider] network account that was assigned Internet Protocol address [xxx.xxx.xxx.xxx] on [date] and [time].

The records and other information requested are set forth as Attachment 1 to the Application and to the proposed Order. In support of this Application, the United States offers the following:

FACTUAL BACKGROUND

- The United States Government, including the Federal Bureau of Investigation and the Department of Justice, is investigating intrusions into a number of computers in the United States and abroad that occurred on [date], and which may be continuing. These computer intrusions are being investigated as possible violations of Title 18 U.S.C. § 1030 (damage and unauthorized access to a protected computer) and § 2511 (unlawful interception of electronic communications). Investigation to date of these incidents provides reasonable grounds to believe that [Internet Service Provider] has records and other information pertaining to certain of its subscribers that are relevant and material to an ongoing criminal investigation.

- In particular, on [date], [victim] discovered an unauthorized intrusion into its computer system, and, specifically, into the following computers: _____. Investigation into this incident revealed that the intruder had obtained so-called "root" or system administrator level access into the _____ computer, effectively giving the intruder complete control of the system. The _____ computer is a "protected computer" according to Title 18 U.S.C. § 1030(e)(2). Accordingly, this unauthorized intrusion constitutes a criminal violation of Title 18 U.S.C. § 1030(a)(2).

- On [date], the intruder(s) again connected to the _____ computer, and again obtained unauthorized "root" access. During that intrusion, investigators recorded the unique Internet Protocol address of the source of the intrusion, [xxx.xxx.xxx.xxx]. Investigators later determined that this address belongs to [Internet Service Provider]. [Internet Service Provider] provides both electronic communications services (access to e-mail and the Internet) and remote computing services (access to computers for the storage and processing of data) to its customers and subscribers using a range of assigned Internet Protocol addresses that include the address of the intrusion.

- Obtaining the records of customer and subscriber information relating to the [Internet Service Provider] account that was assigned address [xxx.xxx.xxx.xxx] on [date] and [time], as well as the contents of electronic communications (no in electronic storage) associated with that account, will help government investigators identify the individual(s) who are responsible for the unauthorized access of the computer systems described above and to determine the nature and scope of the intruder's activities. In particular, the [Internet Service Provider] customer who was assigned this Internet Protocol address at that particular time may be the person responsible for the unauthorized intrusion. Alternatively, records of the customer's account may offer clues that will permit investigators to "trace back" the intrusion to its source.

## LEGAL BACKGROUND

- Title 18 U.S.C. § 2703 sets out particular requirements that the government must meet in order to obtain access to the records and other information in the possession of providers of "electronic communications services" and/or "remote computing services." [Internet Service Provider] functions both as an electronic communications service provider - that is, it provides its subscribers access to electronic communication services, including e-mail and the Internet - and as a remote computing service - it provides computer facilities for the storage and processing of electronic communications - as those terms are used in Title 18 U.S.C. § 2703. **[Note that because a "remote computing service" is public by definition, this statement must be modified if you are seeking information from a service provider who is not a provider to the public, such as, for example, a university.]**

- Here, the government seeks to obtain three categories of records: (1) basic subscriber information; (2) records and other information, including connection logs, pertaining to certain subscribers; and [Add only if the application seeks to obtain the contents of communications (such as e-mails) pursuant to Title 18 U.S.C. § 2703(b), as opposed to mere records pursuant to Title 18 U.S.C. § 2703(c).] (3) the content of electronic communications in a remote computing service (but not communications in electronic storage[107]).

- To obtain basic subscriber information, such as the subscriber's name, address, billing information, and other identifying records, the government needs only a subpoena; however, the government may also compel such information through an order issued pursuant to Title 18 U.S.C. § 2703(d). *See* Title 18 U.S.C. 2703(c)(1)(C). To obtain other types of records and information pertaining to the subscribers or customers of service providers, including connection logs and other audit information, the government must comply with the dictates of sections 2703(c)(1)(B) and 2703(d). Section 2703(c)(1)(B) provides, in pertinent part:

A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity only when the government entity ... obtains a court order for such disclosure under subsection (d) of this section;

- [Add only if the application seeks to obtain the contents of communications (such as e-mails) pursuant to § 2703(b), as opposed to mere records pursuant to § 2703(c).] To obtain the contents of electronic communications held by a remote computing service (but not the contents in "electronic storage," see n.1), the government must comply with Title 18 U.S.C. § 2703(b)(1)(B), which provides, in pertinent part:

A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph 2 of this subsection ... with prior notice from the government entity to the subscriber or customer if the governmental entity ... obtains a court order for such disclosure under subsection (d) of this section ... except that delayed notice may be given pursuant to section 2705 of this title.

Paragraph 2 of subsection 2703(b) applies with respect to any electronic communication that is held or maintained on a remote computing service –

[107] "Electronic Storage" is a term of art, specifically defined in Title 18 U.S.C. § 2510(17) as "(A)ny temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The government does not seek access to any such materials. Communications not in "electronic storage" include any e-mail communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.

A. On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

B. Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

Therefore, communications described by paragraph 2 of subsection 2703(b) include the content of electronic mail that has been opened, viewed, downloaded, or otherwise accessed by the recipient and is held remotely by the service provider on its computers.

- All of the information the government seeks from [Internet Service Provider] through this application may be compelled through an order that complies with section 2703(d). Section 2703(d) provides, in pertinent part:

A court order for disclosure under subsection ... (c) may be issued by any court that is a court of competent jurisdiction described in section 3127(2)(A)[108] and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the ... records or other information sought, are relevant and material to an ongoing criminal investigation.... A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Accordingly, this application sets forth facts showing there are reasonable grounds to believe that the materials sought are relevant and material to the ongoing criminal investigation.

GOVERNMENT'S REQUEST

- The government requests that [Internet Service Provider] be directed to produce all records described in Attachment 1 to this Application. This information is directly relevant to identifying the individual(s) responsible for the crime under investigation.

The information requested should be readily accessible to [Internet Service Provider] by computer search, and its production should not prove to be unduly burdensome.

---

[108] Title 18 U.S.C. § 3127(2)(A) defines the term "court of competent jurisdiction" as including " a district court of the United States (including a magistrate of such court) or a United States Court of Appeals. Because Title 18 U.S.C. § 2703(d) expressly permits "any" such court to issue an order, this Court may enter an order directing the disclosure of such information even if the information is stored outside the judicial District.

[Undersigned should check with the ISP before filing this document to ensure the accuracy of this statement.]

- The United States requests that this Application and Order be sealed by the Court until such time as the court directs otherwise.

- The United States further requests that pursuant to the preclusion of notice provisions of Title 18 U.S.C. § 2705(b), that [Internet Service Provider] be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this order for such period as the court deems appropriate. The United States submits that such an order is justified because notification of the existence of this order could seriously jeopardize the ongoing investigation. Such a disclosure could give the subscriber an opportunity to destroy evidence, notify confederates, or flee or continue his flight from prosecution.

- [Add only if the application seeks to obtain the contents of communications pursuant to Title 18 U.S.C. § 2703(b), as opposed to mere records pursuant to Title 18 U.S.C. § 2703(c).] The United States further requests, pursuant to the delayed notice provisions of Title 18 U.S.C. § 2705(a), an order delaying any notification to the subscriber or customer that may be required by Title 18 U.S.C. § 2703(b) to obtain the contents of communications, for a period of 90 days. Providing prior notice to the subscriber or customer could seriously jeopardize the ongoing investigation, as such disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution. [Optional Baker Act language to use if the ISP is a university: The United States further requests that [Internet Service Provider's] compliance with the delayed notification provisions of this Order shall be deemed authorized under Title 20 U.S.C. 1232g(b)(1)(j)(ii)(the "Baker Act"). *See* 34 C.F.R. § 99.31(a)(9)(i)(exempting requirement of prior notice for disclosures made to comply with a judicial order or lawfully issued subpoena where the disclosure is made pursuant to "any other subpoena issued for a law enforcement purpose and the court or other issuing agency has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed")].

WHEREFORE, it is respectfully requested that the Court grant the attached Order, (1) directing [Internet Service Provider] to provide the United States with the records and information described in Attachment 1; (2) directing that the Application and Order be sealed; (3) directing [Internet Service Provider] not to disclose the existence or content of the Order, except to the extent necessary to carry out the Orders; and [Use only if the application seeks to obtain the contents of communications pursuant to Title 18 U.S.C. § 2703(b)] (4) directing that the notification by the government otherwise required by Title 18 U.S.C. 2703(b) be delayed for ninety days.

Respectfully submitted,

_____

Assistant United States Attorney

ATTACHMENT 1 to lesson plan attachment 1

You are to provide the following information as printouts and as ASCII data files (on 8 mm helical scan tape for Unix host), if available:

- All customer or subscriber account information for any accounts registered to _____, or associated with _____. For each account, the information shall include:

• The subscriber's account and login name(s);

• The subscriber's address;

• The subscriber's telephone number or numbers;

• The subscriber's e-mail address;

• Any other information pertaining to the identity of the subscriber, including, but not limited to, billing information (including type and number of credit cards, student identification number, or other identifying information).

- User connection logs for:

• All accounts identified in the preceding paragraph;

• The I.P. address [xxx.xxx.xxx.xxx], for the time period beginning _____ through and including the date of this order, for any connections to or from _____;

• User connection logs should contain the following:

+ Connection time and date;

+ Disconnect time and date;

+ Method of connection to the system (e.g., SLIP, PPP, Shell);

+ Data transfer volume (e.g., bytes);

+ Connection information for other systems to which user connected, including:

  # Connection destination;

  # Connection time and date;

  # Disconnect time and date;

  # Method of connection to system (e.g., telnet, ftp, http);

  # Data transfer volume (e.g., bytes)

- [Add only if the application seeks to obtain the contents of communications (such as e-mails) pursuant to Title 18 U.S.C. § 2703(b), as opposed to mere records pursuant to Title 18 U.S.C. § 2703(c).] The contents of

electronic communications (not in electronic storage[1]) that were placed or stored in directories or files owned or controlled by the accounts identified in the first paragraph of this attachment at any time after [date] up through and including the date of this Order.

[1] "Electronic Storage" is a term of art, specifically defined in Title 18 U.S.C. § 2510(17) as "(A)ny temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The government does not seek access to any such materials. Communications not in "electronic storage" include any e-mail communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.

UNITED STATES DISTRICT COURT

FOR THE _____ DISTRICT OF _____

| | | |
|---|---|---|
| IN RE APPLICATION OF THE | ) | |
| UNITED STATES OF AMERICA FOR | ) | MISC. NO. _____ |
| AN ORDER PURSUANT TO | ) | |
| TITLE 18 U.S.C. § 2703(d) | ) | **Filed Under Seal** |

ORDER

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703(b) and (c), which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing [Internet Service Provider], an electronic communications service provider and a remote computing service, located at [mailing address], to disclose certain records and other information, as set forth in Attachment 1 to the Application, the court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice of this Order to any person of this investigation or this application and order by the government or [Internet Service Provider] would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that [Internet Service Provider] will, within [three] days of the date of this Order, turn over to agents of the Federal Bureau of Investigation the records and other information as set forth in Attachment 1 to this Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that [Internet Service Provider] shall not disclose the existence of the Application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person unless and until authorized to do so by the Court.

[Add only if the application seeks to obtain the contents of communications (such as e-mails) pursuant to § 2703(b), as opposed to mere records pursuant to § 2703(c)].

IT IS FURTHER ORDERED that the notification by the government otherwise required under Title 18 U.S.C. 2703(b)(1)(B) be delayed for ninety days.

[Optional Baker Act language if the ISP is a university]

Furthermore, [Internet Service Provider's] compliance with the non-disclosure provision of this Order shall be deemed authorized under Title 20 U.S.C. § 1232g(b)(1)(j)(ii).

_____

United States Magistrate Judge

_____

Date

**SAMPLE LANGUAGE**

[Internet Service Provider]

[Address]

VIA FAX to (xxx) xxx-xxxx

Dear Mr. [Name]:

I am writing to confirm our telephone conversation earlier today and to make a formal request for the preservation of records and other evidence pursuant to Title 18 U.S.C. § 2703(f) pending further legal process.

You are hereby requested to preserve, for a period of 90 days, the records described below currently in your possession, including records stored on backup media, in a form that includes the complete record. You also are requested not to disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. **If compliance with this request may result in a permanent or temporary termination of service to the accounts described below, or otherwise alert the subscriber or user of these accounts as to your actions to preserve the referenced files and records, please contact me before taking such actions**.

This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request.

This preservation request applies to the following records and evidence:

*[In a case involving an e-mail account]*

- All stored electronic communications and other files reflecting communications to or from the following electronic mail address: “JDoe@isp.com”;

- All records or other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with the e-mail address [JDoe@isp.com] or user name "JDoe," including, without limitation, subscriber names, user names, screen names or other identities, mailing addresses, residential addresses, business addresses, e-mail addresses and other contact information, telephone numbers or other subscriber number or identity, billing records, information about the length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form; and
- Any other records and other evidence relating to the e-mail address [JDoe@isp.com] or user name "JDoe." Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with user activity or relating to communications and any other activities to, through or from [JDoe@isp.com] or user name "JDoe," whether such records or other evidence are in electronic or other form.

*[In a case involving use of a specific I.P. address]*

All electronic records and other evidence relating to the use of the I.P. address 222.222.222.2 or domain name abc.wcom.net on September 5, 2000 at 04:28 and 04:32 GMT +02:00, and on September 7, 2000 at 00:19 GMT +02:00.

*[In a case involving activity of a user account]*

All connection logs and records of user activity for the user name "JDoe" or address "JDoe@isp.com," including:

- Connection time and date;
- Disconnect time and date;
- Method of connection (e.g., telnet. ftp, http);
- Data transfer volume;
- User name associated with the connection and other connection information, including the Internet Protocol address of the source of the connection;
- Telephone caller identification records; and

- Connection information for other computers to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination I.P. address, connection time and date, disconnect time and date, method of connection to the destination computer, the identities (account and screen names) and subscriber information, if known, for any person or entity to which such connection information relates, and all other information related to the connection from ISP or its subsidiaries.

All records and other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with [JDoe@isp.com], including, without limitation, subscriber names, user names, screen names or other identities, mailing addresses, residential addresses, business addresses, e-mail addresses and other contact information, telephone numbers or other subscriber number or identifier number, billing records, information about the length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form.

Any other records and other evidence relating to [JDoe@isp.com]. Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with or relating to postings, communications and any other activities to or through [JDoe@isp.com], whether such records or other evidence are in electronic or other form.

Very truly yours,

_____

Assistant United States Attorney

Note by (b)(6) FLETC Legal Division Senior Instructor. Though prepared for the signature of an AUSA, federal agents may also issue these letters.

The following is sample language for obtaining basic subscriber information with a subpoena, pursuant to Title 18 U.S.C. § 2703(c)(1)(C):

*"All customer or subscriber account information for any accounts registered to _____, or associated with _____. For each such account, the information shall include:*

- *The subscriber's name;*
- *The subscriber's address;*
- *The subscriber's local and long distance telephone toll billing records;*
- *The subscriber's telephone number or numbers, the e-mail address or addresses, account or login name or names, or any other information pertaining to the identify of the subscriber, including type and number of credit cards, student identification number, or other identifying information; and*
- *The types of services subscribed to or utilized by the subscriber and the lengths of such service."*

The following is sample language for obtaining the content of communications when permitted by the Electronic Communications Privacy Act, pursuant to Title 18 U.S.C. § 2703(a) and (b):

**"The contents of electronic communications not in 'electronic storage' (i.e., electronic mail that has already been opened by the user) currently held or maintained in the account associated with the address '_____@_____' (registered to _____) sent from or to the above account during the period _____ through _____ (inclusive)."**

**"The content of all electronic communications in 'electronic storage' for more than 180 days associated with accounts identified in Part A, that were placed or stored in _____ computer systems in directories or files owned or controlled by such accounts at any time up through and including the date of this subpoena."**

*"[ISP] should NOT produce any unopened incoming electronic communications (i.e., electronic communications in 'electronic storage') less than 181 days old."*

**"For purposes of this request, 'electronic storage' is defined in Title 18 U.S.C. § 2510(17) as '(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an electronic communication service for purposes of backup protection of such communication.' The government does not seek access to any such materials, unless it has been in storage for more than 180 days."**

In teaching this course, there are some commonly asked questions that interest students, but are not necessarily aspects of electronic law that we teach. To assist instructors in dealing with these questions, the following are provided.

1. **How do individuals use "nanny cams" without a Title III court order, considering that there is no consent given by the nanny or the child?**

The guardian of a minor child (usually a parent) may "vicariously consent" to the recording of conversations between the child and another. The seminal case on this issue is Pollock v. Pollock, 154 F.3d 601, 610 (6th Cir. 1998), where the court held that "as long as the guardian has a good faith, objectively reasonable basis for believing that it is necessary and in the best interest of the child to consent on behalf of his or her minor child to the taping of telephone conversations, the guardian may vicariously consent on behalf of the child to the recording." Other federal courts across the country have adopted the reasoning of the court in upholding the "vicarious consent" doctrine. *See, e.g.*, Thompson v. Dulaney, 838 F. Supp. 1535, 1544 (D. Utah 1993)("[A]s long as the guardian has a good faith basis that is objectively reasonable for believing that it is necessary to consent on behalf of her minor children to the taping of the phone conversations, vicarious consent will be permissible in order for the guardian to fulfill her statutory mandate to act in the best interests of the children"); Campbell v. Price, 2 F. Supp. 2d 1186, 1191 (E.D. Ark. 1998)("[A] defendant's good faith concern for his minor child's best interests may, without liability under Title III, empower the parent to intercept the child's conversations with her non-custodial parent").

2. **Is a Title III court order required to "clone" a digital-display pager? Alternatively, can this type of action by law enforcement be analogized to using a "pen register" or "trap and trace" device?**

This issue was addressed in Brown v. Waddell, 50 F.3d 285 (4th Cir. 1995). In Brown, a law enforcement officer wished to use a "pager clone" to monitor numeric messages being received on the target's pagers. He applied for and received a court order for the installation of a "pen register" on the pagers. Once the order was signed, the officer obtained two pagers programmed identically to the two pagers assigned to the target. This "cloning" allowed the officer to receive any numeric messages sent to the target's pagers at the same time that they were received and displayed on the pagers. In a later civil suit, the target alleged, among other things, that the officer had violated the Electronic Communications Privacy Act (ECPA) by intercepting electronic communications without a Title III court order. The lower court dismissed the entire case, holding that the use of the cloned pagers was effectively "the installation and use of a 'pen register.'" Because the officer had obtained a court order to clone the pagers, the court held that no violation of the ECPA had occurred. However, the Court of Appeals disagreed. First, the court noted that the clone used in this case did not meet the statutory definition of a "pen register." Title 18 U.S.C. § 3127(3)(stating that a "pen

register," by definition, is attached to the telephone line). Second, the court held that a digital-display pager was not intended to be treated like a pen register. Citing to the legislative history of the ECPA, the court noted that the function of a digital-display pager is "usually" to display telephone numbers. This was an implicit recognition by Congress that because a digital-display pager can also receive a much larger set of numbers, it can by that means receive and display an unlimited range of number-coded substantive messages. Thus, the use of pager clones to intercept numeric transmissions was an interception of an electronic communication, subject to the stringent requirements of Title III.

3. **Is the interception of a cordless telephone conversation governed by Title III?**

With enactment of the ECPA in 1986, Congress enlarged the coverage of Title III to prohibit the interception of "electronic" as well as oral and wire communications. Bartnicki v. Vopper, 532 U.S. 514 (2001). As amended, Title III defined a "wire communication" as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or other like connection between the point of origin and the point of reception ... ***but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit*.**" Title 18 U.S.C. § 2510(1)(emphasis added). An "electronic communication" was defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system ... but does not include – (A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit." Title 18 U.S.C. § 2510(12)(A). Prior to 1994, the courts that addressed the question of whether Title III protection was extended to cordless telephones agreed "overwhelmingly that cordless telephone transmissions [were] not 'wire' or 'electronic' communications covered by Title III." McKamey v. Roach, 55 F.3d 1236, 1238 (6th Cir. 1995). *See also* In re Askin, 47 F.3d 100, 103 (4th Cir.), cert. denied, 516 U.S. 944 (1995); United States v. Smith, 978 F.2d 171, 175 (5th Cir. 1992), cert. denied, 507 U.S. 999 (1993); and Tyler v. Berodt, 877 F.2d 705, 706 (8th Cir. 1989)(per curiam), cert. denied, 493 U.S. 1022 (1990). However, "in 1994, Congress amended the ECPA to remove the exception for cordless telephones from the definition of wire or oral communications ... and amended the penalty provisions to include the interception of cordless telephone conversations" Spetalieri v. Kavanaugh, 36 F. Supp. 2d 92, 113 (N.D.N.Y. 1998). This amendment was accomplished by "simply striking the above exceptions from Title 18 U.S.C. § 2510(1) and § 2510 (12)(A)." McKamey, supra at 1238 n.1. In expanding Title III protection to cordless telephones, "Congress found that cordless telephones play an integral part of our society, that people expect that such telephone calls will be private and, accordingly, amended § 2511 to protect cordless telephone calls." Spetalieri, supra at 113. Following these amendments, the Supreme Court has authoritatively held that "Title III now applies to the interception of conversations over both cellular and cordless phones." Bartnicki, 532 U.S. at 520.

Additionally, courts have uniformly rejected attempts by defendants to characterize conversations held over cordless phones as "oral" communications. As noted by one court: "Virtually every court to have faced the question of whether cordless phone conversations were oral communications under § 2510(2) answered in the negative." Askin, supra at 104 [*citing* Smith, supra; Tyler, supra; United States v. Carr, 805 F. Supp. 1266 (E.D.N.C. 1992); and Edwards v. Bardwell, 632 F. Supp. 584 (M.D. La.), aff'd without opinion 808 F.2d 54 (1986).] Title 18 U.S.C. § 2510(2) defines an "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." Because an oral communication must be one that is "uttered by a person," the plain language of the statute "removes cordless phone communications from the definition of 'oral communication.'" McKamey, supra at 1239 (*citing* Askin, supra and Smith, supra). As the courts have reasoned, it is not the actual "utterances" of the speakers that are being intercepted in these cases, but rather "the radio signal produced by the phone's handset and base unit. Therefore, the interception of a cordless phone transmission cannot be an interception of an oral utterance." Price v. Turner, 260 F.3d 1144, 1148 (9th Cir. 2001)(citations omitted). This view also appears to be supported by the legislative history of the 1986 amendments to Title III, which explained that "in essence, an oral communication is one carried by sound waves, not by an electronic medium." Smith, supra at 175-76 [*quoting* S.REP.NO 541, 99th Cong. 2d Sess. 13 (1986)].

**Sample Language for Search Warrants**

**and Accompanying Affidavits to Search and Seize Computers**

**This attachment is a direct reprint of Appendix F from the United States Department of Justice Computer Crime and Intellectual Property Section publication *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*.**

This appendix provides sample language for agents and prosecutors who wish to obtain a warrant authorizing the search and seizure of computers. The discussion focuses first on the proper way to describe the property to be seized in the warrant itself, which in turn requires consideration of the role of the computer in the offense. The discussion then turns to drafting an accompanying affidavit that establishes probable cause, describes the agent's search strategy, and addresses any additional statutory or constitutional concerns.

## I. DESCRIBING THE PROPERTY TO BE SEIZED FOR THE WARRANT

The first step in drafting a warrant to search and seize computers or computer data is to describe the property to be seized for the warrant itself. This requires a particularized description of the evidence, contraband, fruits, or instrumentality of crime that the agents hope to obtain by conducting the search.

Whether the 'property to be seized' should contain a description of information (such as computer files) or physical computer hardware depends on the role of the computer in the offense. In some cases, the computer hardware is itself contraband, evidence of crime, or a fruit or instrumentality of crime. In these situations, Fed. R. Crim. P. 41 expressly authorizes the seizure of the hardware, and the warrant will ordinarily request its seizure. In other cases, however, the computer hardware is merely a storage device for electronic files that are themselves contraband, evidence, or instrumentalities of crime. In these cases, the warrant should request authority to search for and seize the information itself, not the storage devices that the agents believe they must seize to recover the information. Although the agents may need to seize the storage devices for practical reasons, such practical considerations are best addressed in the accompanying affidavit. The 'property to be seized' described in the warrant should fall within one or more of the categories listed in Rule 41(b):

*(1) "property that constitutes evidence of the commission of a criminal offense"*

This authorization is a broad one, covering any item that an investigator

"reasonably could . . . believe" would reveal information that would aid in a particular apprehension or conviction. Andresen v. Maryland, 427 U.S. 463, 483 (1976). *Cf.* Warden v. Hayden, 387 U.S. 294, 307 (1967) (noting that restrictions on what evidence may be seized result mostly from the probable cause requirement). The word "property" in Rule 41(b)(1) includes both tangible and intangible property. *See* United States v. New York Tel. Co., 434 U.S. 159, 169 (1977)("Rule 41 is not limited to tangible items but is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause."); United States v. Biasucci, 786 F.2d 504, 509-10 (2d Cir.), cert. denied, 479 U.S. 827 (1986)(holding that the fruits of video surveillance are "property" that may be seized using a Rule 41 search warrant). Accordingly, data stored in electronic form is "property" that may properly be searched and seized using a Rule 41 warrant. *See* United States v. Hall, 583 F. Supp. 717, 718-19 (E.D. Va. 1984).

*(2) "contraband, the fruits of crime, or things otherwise criminally possessed"*

Property is contraband "when a valid exercise of the police power renders possession of the property by the accused unlawful and provides that it may be taken." Hayden, 387 U.S. at 302 (*quoting* Gouled v. United States, 255 U.S. 298, 309 (1921)). Common examples of items that fall within this definition include child pornography, *see* United States v. Kimbrough, 69 F.3d 723, 731 (5th Cir. 1995), cert. denied, 517 U.S. 1157 (1996), pirated software and other copyrighted materials, *see* United States v. Vastola, 670 F. Supp. 1244, 1273 (D.N.J. 1987), counterfeit money, narcotics, and illegal weapons. The phrase "fruits of crime" refers to property that criminals have acquired as a result of their criminal activities. Common examples include money obtained from illegal transactions, *see* United States v. Dornblut, 261 F.2d 949, 951 (2d Cir. 1958), cert. denied, 360 U.S. 912 (1959)(cash obtained in drug transaction), and stolen goods. *See* United States v. Burkeen, 350 F.2d 261, 264 (6th Cir.), cert. denied sub nom. Matlock v. United States (1965)(currency removed from bank during bank robbery).

*(3) "property designed or intended for use or which is or had been used as a means of committing a criminal offense"*

Rule 41(b)(3) authorizes the search and seizure of "property designed or intended for use or which is or had been used as a means of committing a criminal offense." This language permits courts to issue warrants to search and seize instrumentalities of crime. *See* United States v. Farrell, 606 F.2d 1341, 1347 (D.C. Cir. 1979). Computers may serve as instrumentalities of crime in many ways. For example, Rule 41 authorizes the seizure of computer equipment as an instrumentality when a suspect uses a computer to view, acquire, and transmit images of child pornography. *See* Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (stating in an obscenity case that "the computer equipment was more than merely a 'container' for the files; it was an instrumentality of the crime."); United States v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996). Similarly, a hacker's computer may be used as an instrumentality of

crime, and a computer used to run an illegal Internet gambling business would also be an instrumentality of the crime.

Here are examples of how to describe property to be seized when the computer hardware is merely a storage container for electronic evidence:

*(A) All records relating to violations of Title 21 U.S.C. § 841(a) (drug trafficking) and/or 21 U.S.C. § 846 (conspiracy to traffic drugs) involving [the suspect] since January 1, 1996, including lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions; any information related to sources of narcotic drugs (including names, addresses, phone numbers, or any other identifying information); any information recording [the suspect's] schedule or travel from 1995 to the present; all bank records, checks, credit card bills, account information, and other financial records.*

*The terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including floppy diskettes, hard disks, ZIP disks, CD-ROMs, optical discs, backup tapes, printer buffers, smart cards, memory calculators, pagers, personal digital assistants such as Palm Pilot computers, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).*

*(B) Any copy of the X Company's confidential May 17, 1998 report, in electronic or other form, including any recognizable portion or summary of the contents of that report.*

**(C) [For a warrant to obtain records stored with an ISP pursuant to Title 18 U.S.C. Section 2703(a)]** *All stored electronic mail of any kind sent to, from and through the e-mail address [JDoe@isp.com], or associated with the user name "John Doe," or account holder [suspect]. Content and connection log files of all account activity from January 1, 2000, through March 31, 2000, by the user associated with the e-mail address [JDoe@isp.com], including dates, times, methods of connecting (e.g., telnet, ftp, http), ports used, telephone dial-up caller identification records, and any other connection information or traffic data. All business records, in any form kept, in the possession of [Internet Service Provider], that pertain to the subscriber(s) and account(s) associated with the e-mail address [JDoe@isp.com], including records showing the subscriber's full name, all screen names associated with that subscriber and account, all account names associated with that subscriber, methods of payment, phone numbers, all residential, business, mailing, and e-mail addresses, detailed billing records, types and lengths of service, and any other identifying information.*

Here are examples of how to describe the property to be seized when the computer hardware itself is evidence, contraband, or an instrumentality of crime:

*(A) Any computers (including file servers, desktop computers, laptop computers, mainframe computers, and storage devices such as hard drives, Zip disks, and floppy disks) that were or may have been used as a means to provide images of child pornography over the Internet in violation of Title 18 U.S.C. § 2252A that were accessible via the World Wide Website address www.[xxxxxxxx].com.*

*(B) IBM Thinkpad Model 760ED laptop computer with a black case*

## II. DRAFTING AFFIDAVITS IN SUPPORT OF WARRANTS TO SEARCH AND SEIZE COMPUTERS

An affidavit to justify the search and seizure of computer hardware and/or files should include, at a minimum, the following sections: (1) definitions of any technical terms used in the affidavit or warrant; (2) a summary of the offense, and, if known, the role that a targeted computer plays in the offense; and (3) an explanation of the agents' search strategy. In addition, warrants that raise special issues (such as sneak-and-peek warrants, or warrants that may implicate the Privacy Protection Act, Title 42 U.S.C. § 2000aa) require thorough discussion of those issues in the affidavit. Agents and prosecutors with questions about how to tailor an affidavit and warrant for a computer-related search may contact either the local CTC, or the Computer Crime & Intellectual Property Section at (202) 514-1026.

### II. A. Background Technical Information

It may be helpful to include a section near the beginning of the affidavit explaining any technical terms that the affiant may use. Although many judges are computer literate, judges generally appreciate a clear, jargon-free explanation of technical terms that may help them understand the merits of the warrant application. At the same time, agents and prosecutors should resist the urge to pad affidavits with long, boilerplate descriptions of well-known technical phrases. As a rule, affidavits should only include the definitions of terms that are likely to be unknown by a generalist judge and are used in the remainder of the affidavit. Here are several sample definitions:

**Encryption.** *Encryption refers to the practice of mathematically scrambling computer data as a communications security measure. The encrypted information is called "ciphertext." "Decryption" is the process of converting the ciphertext back into the original, readable information (known as "plaintext"). The word, number or other value used to encrypt/decrypt a message is called the "key."*

**Data Compression.** *A process of reducing the number of bits required to represent some information, usually to reduce the time or cost of storing or transmitting it. Some methods can be reversed to reconstruct the original data exactly; these are used for faxes, programs and most computer data. Other methods do not exactly reproduce the original data, but this may be acceptable (for example, for a video conference).*

**Joint Photographic Experts Group (JPEG).** *JPEG is the name of a standard for compressing digitized images that can be stored on computers. JPEG is often used to compress photographic images, including pornography. Such files are often identified by the ".jpg" extension (such that a JPEG file might have the title "picture.jpg") but can easily be renamed without the ".jpg" extension.*

**Internet Service Providers ("ISPs").** *Many individuals and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.*

*ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data format and in written record format.*

*ISPs reserve and/or maintain computer disk storage space on their computer system for the use of the Internet service subscriber for both temporary and long-term storage of electronic communications with other parties and other types of electronic data and files. E-mail that has not been opened is stored temporarily by an ISP incident to the transmission of the e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," and the provider of such a service is an "electronic communications service" provider. A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is providing a "remote computing service."*

**Server.** *A server is a centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called "clients." In a large company, it is common for individual employees to have*

*client computers at their desktops. When the employees access their e-mail, or access files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network. Notably, server computers can be physically stored in any location: it is common for a network's server to be located hundreds (and even thousands) of miles away from the client computers.*

*In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."*

**IP Address.** *The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.*

> **Dynamic IP address.** *When an ISP or other provider uses dynamic IP addresses, the ISP randomly assigns one of the available IP addresses in the range of IP addresses controlled by the ISP each time a user dials into the ISP to connect to the Internet. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, however, that IP address becomes available to other customers who dial in at a later time. Thus, an individual customer's IP address normally differs each time he dials into the ISP.*
>
> **Static IP address** *A static IP address is an IP address that is assigned permanently to a given user or computer on a network. A customer of an ISP that assigns static IP addresses will have the same IP address every time.*

## II. B. Describe the Role of the Computer in the Offense

The next step is to describe the role of the computer in the offense, to the extent it is known. For example, is the computer hardware itself evidence of a crime or contraband? Is the computer hardware merely a storage device that may or may not

contain electronic files that constitute evidence of a crime? To introduce this topic, it may be helpful to explain at the outset why the role of the computer is important for defining the scope of your warrant request.

*Your affiant knows that computer hardware, software, and electronic files may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of crime. In this case, the warrant application requests permission to search and seize [images of child pornography, including those that may be stored on a computer]. These [images] constitute both evidence of crime and contraband. This affidavit also requests permission to seize the computer hardware that may contain [the images of child pornography] if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. Your affiant believes that, in this case, the computer hardware is a container for evidence, a container for contraband, and also itself an instrumentality of the crime under investigation.*

**II.B.1 When the Computer Hardware Is Itself Contraband, Evidence, And/or an Instrumentality or Fruit of Crime**

If applicable, the affidavit should explain why probable cause exists to believe that the tangible computer items are themselves contraband, evidence, instrumentalities, or fruits of the crime, independent of the information they may hold.

**Computer Used to Obtain Unauthorized Access to a Computer ("Hacking").** *Your affiant knows that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is "used as a means of committing [the] criminal offense" according to Rule 41(b )(3). In particular, the individual's computer is the primary means for accessing the Internet, communicating with the victim computer, and ultimately obtaining the unauthorized access that is prohibited by Title 18 U.S.C. § 1030. The computer is also likely to be a storage device for evidence of crime because computer hackers generally maintain records and evidence relating to their crimes on their computers. Those records and evidence may include files that recorded the unauthorized access, stolen passwords*

*and other information downloaded from the victim computer, the individual's notes as to how the access was achieved, records of Internet chat discussions about the crime, and other records that indicate the scope of the individual's unauthorized access.*

**Computers Used to Produce Child Pornography.** *It is common for child pornographers to use personal computers to produce both still and moving images. For example, a computer can be connected to a common video camera using a device called a video capture board: the device turns the video output into a form that is usable by computer programs. Alternatively, the pornographer can use a digital camera to take photographs or videos and load them directly onto the computer. The output of the camera can be stored, transferred or printed out directly from the computer. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. All of these devices, as well as the computer, constitute instrumentalities of the crime.*

### II.B.2. When the Computer Is Merely a Storage Device for Contraband, Evidence, And/or an Instrumentality or Fruit of Crime

When the computer is merely a storage device for electronic evidence, the affidavit should explain this clearly. The affidavit should explain why there is probable cause to believe that evidence of a crime may be found in the location to be searched. This does not require the affidavit to establish probable cause that the evidence may be stored specifically within a computer. However, the affidavit should explain why the agents believe that the information may in fact be stored as an electronic file stored in a computer.

**Child Pornography.** *Your affiant knows that child pornographers generally prefer to store images of child pornography in electronic form as computer files. The computer's ability to store images in digital form makes a computer an ideal repository for pornography. A small portable disk can contain hundreds or thousands of images of child pornography, and a computer hard drive can contain tens of thousands of such images at very high resolution. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection.*

**Illegal Business Operations.** *Based on actual inspection of [spreadsheets, financial records, invoices], your affiant is aware that computer equipment was used to generate, store, and print documents used in [suspect's] [tax evasion, money laundering, drug trafficking, etc.] scheme. There is reason to believe that the computer system currently located on [suspect's] premises is the same system used to produce and store the [spreadsheets, financial records, invoices], and that both the [spreadsheets, financial*

*records, invoices] and other records relating to [suspect's] criminal enterprise will be stored on [suspect's computer].*

## II. C. The Search Strategy.

The affidavit should also contain a careful explanation of the agents' search strategy, as well as a discussion of any practical or legal concerns that govern how the search will be executed. Such an explanation is particularly important when practical considerations may require that agents seize computer hardware and search it off-site when that hardware is only a storage device for evidence of crime. Similarly, searches for computer evidence in sensitive environments (such as functioning businesses) may require that the agents adopt an incremental approach designed to minimize the intrusiveness of the search. The affidavit should explain the agents' approach in sufficient detail that the explanation provides a useful guide for the search team and any reviewing court. It is a good practice to include a copy of the search strategy as an attachment to the warrant, especially when the affidavit is placed under seal. Here is sample language that can apply recurring situations:

### II.C.1. Sample Language to Justify Seizing Hardware and Conducting a Subsequent Off-site Search

*Based upon your affiant's knowledge, training and experience, your affiant knows that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:*

*(1) The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.*

*(2) Technical Requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a*

*search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.*

*In light of these concerns, your affiant hereby requests the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.*

### II.C.2. Sample Language to Justify an Incremental Search

*Your affiant recognizes that the [Suspect] Corporation is a functioning company with approximately [number] employees, and that a seizure of the [Suspect] Corporation's computer network may have the unintended and undesired effect of limiting the company's ability to provide service to its legitimate customers who are not engaged in [the criminal activity under investigation]. In response to these concerns, the agents who execute the search will take an incremental approach to minimize the inconvenience to [Suspect Corporation]'s legitimate customers and to minimize the need to seize equipment and data. This incremental approach, which will be explained to all of the agents on the search team before the search is executed, will proceed as follows:*

*A. Upon arriving at the [Suspect Corporation's] headquarters on the morning of the search, the agents will attempt to identify a system administrator of the network (or other knowledgeable employee) who will be willing to assist law enforcement by identifying, copying, and printing out paper [and electronic] copies of [the computer files described in the warrant.] If the agents succeed at locating such an employee and are able to obtain copies of the [the computer files described in the warrant] in that way, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.*

*B. If the employees choose not to assist the agents and the agents cannot execute the warrant successfully without themselves examining the [Suspect Corporation's] computers , primary responsibility for the search will transfer from the case agent to a designated computer expert. The computer expert will attempt to locate [the computer files described in the warrant], and will attempt to make electronic copies of those files. This analysis will focus on particular programs, directories, and files that are most likely to contain the evidence and information of the violations under investigation. The computer expert will make every effort to review and copy only those programs, directories, files, and materials that are evidence of the offenses described herein, and provide only those items to the case agent. If the computer expert succeeds at locating [the computer files described in the warrant] in that way, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.*

*C. If the computer expert is not able to locate the files on-site, or an on-site search proves infeasible for technical reasons, the computer expert will attempt to create an electronic "image" of those parts of the computer that are likely to store [the computer files described in the warrant]. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Imaging a computer permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer hardware. The computer expert or another technical expert will then conduct an off-site search for [the computer files described in the warrant] from the "mirror image" copy at a later date. If the computer expert successfully images the [Suspect Corporation's] computers, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.*

*D. If "imaging" proves impractical, or even impossible for technical reasons, then the agents will seize those components of the [Suspect Corporation's] computer system that the computer expert believes must be seized to permit the agents to locate [the computer files described in the warrant] at an off-site location. The components will be seized and taken in to the custody of the FBI. If employees of [Suspect Corporation] so request, the computer expert will, to the extent practicable, attempt to provide the employees with copies of any files [not within the scope of the warrant] that may be necessary or important to the continuing function of the [Suspect Corporation's] legitimate business. If, after inspecting the computers, the analyst determines that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it within a reasonable time.*

### II.C.3. Sample Language to Justify the Use of Comprehensive Data Analysis Techniques

*Searching [the suspect's] computer system for the evidence described in [Attachment A]*

*may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, agents may be able to execute a "keyword" search that searches through the files stored in a computer for special words that are likely to appear only in the materials covered by a warrant. Similarly, agents may be able to locate the materials covered in the warrant by looking for particular directory or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in [Attachment A].*

### II.D. Special Considerations

The affidavit should also contain discussions of any special legal considerations that may factor into the search or how it will be conducted. These considerations are discussed at length in Chapter 2. Agents can use this checklist to determine whether a particular computer-related search raises such issues:

1. Is the search likely to result in the seizure of any drafts of publications (such as books, newsletters, Web site postings, etc.) that are unrelated to the search and are stored on the target computer? If so, the search may implicate the Privacy Protection Act, Title 42 U.S.C. § 2000aa.

2. Is the target of the search an ISP, or will the search result in the seizure of a mail server? If so, the search may implicate the Electronic Communications Privacy Act, Title 18 U.S.C. §§ 2701-11.

3. Does the target store electronic files or e-mail on a server maintained in a remote location? If so, the agents may need to obtain more than one warrant.

4. Will the search result in the seizure of privileged files, such as attorney-client communications? If so, special precautions may be in order.

5. Are the agents requesting authority to execute a sneak-and-peek search?

6. Are the agents requesting authority to dispense with the “knock and announce” rule?

## 9-13.420 Searches of Premises of Subject Attorneys

**NOTE**: For purposes of this policy only, "subject" includes an attorney who is a "suspect, subject or target," or an attorney who is related by blood or marriage to a suspect, or who is believed to be in possession of contraband or the fruits or instrumentalities of a crime. This policy also applies to searches of business organizations where such searches involve materials in the possession of individuals serving in the capacity of legal advisor to the organization. Search warrants for "documentary materials" held by an attorney who is a "disinterested third party" (that is, any attorney who is not a subject) are governed by 28 C.F.R. 59.4 and USAM 9-19.221 et seq. *See also* Title 42 U.S.C. § 2000aa-11(a)(3).

There are occasions when effective law enforcement may require the issuance of a search warrant for the premises of an attorney who is a subject of an investigation, and who also is or may be engaged in the practice of law on behalf of clients. Because of the potential effects of this type of search on legitimate attorney-client relationships and because of the possibility that, during such a search, the government may encounter material protected by a legitimate claim of privilege, it is important that close control be exercised over this type of search. Therefore, the following guidelines should be followed with respect to such searches:

**A. Alternatives to Search Warrants.** In order to avoid impinging on valid attorney-client relationships, prosecutors are expected to take the least intrusive approach consistent with vigorous and effective law enforcement when evidence is sought from an attorney actively engaged in the practice of law. Consideration should be given to obtaining information from other sources or through the use of a subpoena, unless such efforts could compromise the criminal investigation or prosecution, or could result in the obstruction or destruction of evidence, or would otherwise be ineffective.

NOTE: Prior approval must be obtained from the Assistant Attorney General for the Criminal Division to issue a subpoena to an attorney relating to the representation of a client. *See* USAM 9-13.410.

**B. Authorization by United States Attorney or Assistant Attorney General.** No application for such a search warrant may be made to a court without the express approval of the United States Attorney or pertinent Assistant Attorney General. Ordinarily, authorization of an application for such a search warrant is appropriate when there is a strong need for the information or material and less intrusive means have been considered and rejected.

**C. Prior Consultation.** In addition to obtaining approval from the United States Attorney or the pertinent Assistant Attorney General, and before seeking judicial authorization for the search warrant, the federal prosecutor must consult with the Criminal Division.

NOTE: Attorneys are encouraged to consult with the Criminal Division as early as possible regarding a possible search of an attorney's office. Telephone No. (202) 514-5541; Fax No. (202) 514-1468.

To facilitate the consultation, the prosecutor should submit the attached form (*see* Criminal Resource Manual at 265) containing relevant information about the proposed search along with a draft copy of the proposed search warrant, affidavit in support thereof, and any special instructions to the searching agents regarding search procedures and procedures to be followed to ensure that the prosecution team is not "tainted" by any privileged material inadvertently seized during the search. This information should be submitted to the Criminal Division through the Office of Enforcement Operations. This procedure does not preclude any United States Attorney or Assistant Attorney General from discussing the matter personally with the Assistant Attorney General of the Criminal Division.

If exigent circumstances prevent such prior consultation, the Criminal Division should be notified of the search as promptly as possible. In all cases, the Criminal Division should be provided as promptly as possible with a copy of the judicially authorized search warrant, search warrant affidavit, and any special instructions to the searching agents.

The Criminal Division is committed to ensuring that consultation regarding attorney search warrant requests will not delay investigations. Timely processing will be assisted if the Criminal Division is provided as much information about the search as early as possible. The Criminal Division should also be informed of any deadlines.

**D. Safeguarding Procedures and Contents of the Affidavit.** Procedures should be designed to ensure that privileged materials are not improperly viewed, seized or retained during the course of the search. While the procedures to be followed should be tailored to the facts of each case and the requirements and judicial preferences and precedents of each district, in all cases a prosecutor must employ adequate precautions to ensure that the materials are reviewed for privilege claims and that any privileged documents are returned to the attorney from whom they were seized.

**E. Conducting the Search.** The search warrant should be drawn as specifically as possible, consistent with the requirements of the investigation, to minimize the need to search and review privileged material to which no exception applies.

While every effort should be made to avoid viewing privileged material, the search may require limited review of arguably privileged material to ascertain whether the material is covered by the warrant. Therefore, to protect the attorney-client privilege and to ensure that the investigation is not compromised by exposure to privileged material relating to the investigation or to defense strategy, a "privilege team" should be designated, consisting of agents and lawyers not involved in the underlying investigation.

Instructions should be given and thoroughly discussed with the privilege team prior to the search. The instructions should set forth procedures designed to minimize the intrusion into privileged material, and should ensure that the privilege team does not disclose any information to the investigation/prosecution team unless and until so instructed by the attorney in charge of the privilege team. Privilege team lawyers should be available either on or off-site, to advise the agents during the course of the search, but should not participate in the search itself.

The affidavit in support of the search warrant may attach any written instructions or, at a minimum, should generally state the government's intention to employ procedures designed to ensure that attorney-client privileges are not violated.

If it is anticipated that computers will be searched or seized, prosecutors are expected to follow the procedures set forth in *Federal Guidelines for Searching and Seizing Computers* (July 1994), published by the Criminal Division Office of Professional Training and Development.

**F. Review Procedures.** The following review procedures should be discussed prior to approval of any warrant, consistent with the practice in your district, the circumstances of the investigation and the volume of materials seized.

+ Who will conduct the review, i.e., a privilege team, a judicial officer, or a special master.
+ Whether all documents will be submitted to a judicial officer or special master or only those which a privilege team has determined to be arguably privileged or arguably subject to an exception to the privilege.
+ Whether copies of all seized materials will be provided to the subject attorney (or a legal representative) in order that: a) disruption of the law firm's operation is minimized; and b) the subject is afforded an opportunity to participate in the process of submitting disputed documents to the court by raising specific claims of privilege. To the extent possible, providing copies of seized records is encouraged, where such disclosure will not impede or obstruct the investigation.

+ Whether appropriate arrangements have been made for storage and handling of electronic evidence and procedures developed for searching computer data (i.e., procedures which recognize the universal nature of computer seizure and are designed to avoid review of materials implicating the privilege of innocent clients).

These guidelines are set forth solely for the purpose of internal Department of Justice guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter, civil or criminal, nor do they place any limitations on otherwise lawful investigative or litigative prerogatives of the Department of Justice.

*See* the Criminal Resource Manual at 265, for an attorney office search warrant form.

[Code of Federal Regulations]

[Title 28, Volume 2]

[Revised as of July **1**, 2001]

From the U.S. Government Printing Office via GPO Access

[**CITE**: **28CFR59**.**1**]

TITLE 28--JUDICIAL ADMINISTRATION

CHAPTER I--DEPARTMENT OF JUSTICE (Continued)

PART 59--GUIDELINES ON METHODS OF OBTAINING DOCUMENTARY MATERIALS HELD BY THIRD PARTIES--Table of Contents

Sec. 59.**1** Introduction.

(a) A search for documentary materials necessarily involves intrusions into personal privacy. First, the privacy of a person's home or office may be breached. Second, the execution of such a search may require examination of private papers within the scope of the search warrant, but not themselves subject to seizure. In addition, where such a search involves intrusions into professional, confidential relationships, the privacy interests of other persons are also implicated.

(b) It is the responsibility of federal officers and employees to recognize the importance of these personal privacy interests, and to protect against unnecessary intrusions. Generally, when documentary materials are held by a disinterested third party, a subpoena, administrative summons, or governmental request will be an effective alternative to the use of a search warrant and will be considerably less intrusive. The purpose of the guidelines set forth in this part is to assure that federal officers and employees do not use search and seizure to obtain documentary materials in the possession of disinterested third parties unless reliance on alternative means would substantially jeopardize their availability (e.g., by creating a risk of destruction, etc.) or usefulness (e.g., by detrimentally delaying the investigation, destroying a chain of custody, etc.). Therefore, the guidelines in this part establish certain criteria and procedural requirements which must be met before a search warrant may be used to obtain documentary materials held by disinterested third parties. The guidelines in this part are not intended to inhibit the use of less intrusive means of obtaining documentary materials such as the use of a subpoena, summons, or formal or informal request.

Sec. 59.**2** Definitions.

As used in this part--

(a) The term attorney for the government shall have the same meaning as is given that term in Rule 54(c) of the Federal Rules of Criminal Procedure;

(b) The term disinterested third party means a person or organization not reasonably believed to be--

(1) A suspect in the criminal offense to which the materials sought under these guidelines relate; or

(**2**) Related by blood or marriage to such a suspect;

(c) The term documentary materials means any materials upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, films or negatives, audio or video tapes, or materials upon which information is electronically or magnetically recorded, but does not include materials which constitute contraband, the fruits or instrumentalities of a crime, or things otherwise criminally possessed;

(d) The term law enforcement officer shall have the same meaning as the term ``federal law enforcement officer'' as defined in Rule 41(h) of the Federal Rules of Criminal Procedure; and

(e) The term supervisory official of the Department of Justice means the supervising attorney for the section, office, or branch within the Department of Justice which is responsible for the investigation or prosecution of the offense at issue, or any of his superiors.

Sec. 59.**3** Applicability.

(a) The guidelines set forth in this part apply, pursuant to section 201 of the Privacy Protection Act of 1980 (Sec. 201, Pub. L. 96-440, 94 Stat. 1879, (42 U.S.C. 2000aa-11)), to the procedures used by any federal officer or employee, in connection with the investigation or prosecution of a criminal offense, to obtain documentary materials in the private possession of a disinterested third party.

(b) The guidelines set forth in this part do not apply to:

(1) Audits, examinations, or regulatory, compliance, or administrative inspections or searches pursuant to federal statute or the terms of a federal contract;

(2) The conduct of foreign intelligence or counterintelligence activities by a government authority pursuant to otherwise applicable law;

(**3**) The conduct, pursuant to otherwise applicable law, of searches and seizures at the borders of, or at international points of entry into, the United States in order to enforce the customs laws of the United States;

(4) Governmental access to documentary materials for which valid consent has been obtained; or

(5) Methods of obtaining documentary materials whose location is known but which have been abandoned or which cannot be obtained through subpoena or request because they are in the possession of a person whose identity is unknown and cannot with reasonable effort be ascertained.

(c) The use of search and seizure to obtain documentary materials which are believed to be possessed for the purpose of disseminating to the public a book, newspaper, broadcast, or other form of public communication is subject to title I of the Privacy Protection Act of 1980 (Sec. 101, et seq., Pub. L. 96-440, 94 Stat. 1879 (42 U.S.C. 2000aa, et seq.)), which strictly prohibits the use of search and seizure to obtain such materials except under specified circumstances.

(d) These guidelines are not intended to supersede any other statutory, regulatory, or policy limitations on access to, or the use or disclosure of particular types of documentary materials, including, but not limited to, the provisions of the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401, et seq.), the Drug Abuse Office and Treatment Act of 1972, as amended (21 U.S.C. 1101, et seq.), and the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act of 1970, as amended (42 U.S.C. 4541, et seq.).

---

\1\ Notwithstanding the provisions of this section, any application for a warrant to search for evidence of a criminal tax offense under the jurisdiction of the Tax Division must be specifically approved in advance by the Tax Division pursuant to section 6-2.330 of the U.S. Attorneys' Manual.

---

(a) Provisions governing the use of search warrants generally. (1) A search warrant should not be used to obtain documentary materials believed to be in the private possession of a disinterested third party unless it appears that the use of a subpoena, summons, request, or other less intrusive alternative means of obtaining the materials would substantially jeopardize the availability or usefulness of the materials sought, and the application for the warrant has been authorized as provided in paragraph (a)(2) of this section.

(2) No federal officer or employee shall apply for a warrant to search for and seize documentary materials believed to be in the private possession of a disinterested third party unless the application for the warrant has been authorized by an attorney for the government. Provided, however, that in an emergency situation in which the immediacy of the need to seize the materials does not permit an opportunity to secure the authorization of an attorney for the government, the application may be authorized by a supervisory law enforcement officer in the applicant's department or agency, if the appropriate U.S. Attorney (or where the case is not being handled by a U.S. Attorney's Office, the appropriate supervisory official of the Department of Justice) is notified of the authorization and the basis for justifying such authorization under this part within 24 hours of the authorization.

(b) Provisions governing the use of search warrants which may intrude upon professional, confidential relationships. (1) A search warrant should not be used to obtain documentary materials believed to be in the private possession of a disinterested third party physician, \2\ lawyer, or clergyman, under circumstances in which the materials sought, or other materials likely to be reviewed during the execution of the warrant, contain confidential information on patients, clients, or parishioners which was furnished or developed for the purposes of

professional counseling or treatment, unless--

---

\2\ Documentary materials created or compiled by a physician, but retained by the physician as a matter of practice at a hospital or clinic shall be deemed to be in the private possession of the physician, unless the clinic or hospital is a suspect in the offense.

---

(i) It appears that the use of a subpoena, summons, request or other less intrusive alternative means of obtaining the materials would substantially jeopardize the availability or usefulness of the materials sought;

(ii) Access to the documentary materials appears to be of substantial importance to the investigation or prosecution for which they are sought; and

(iii) The application for the warrant has been approved as provided in paragraph (b)(2) of this section.

(2) No federal officer or employee shall apply for a warrant to search for and seize documentary materials believed to be in the private possession of a disinterested third party physician, lawyer, or clergyman under the circumstances described in paragraph (b)(1) of this

section, unless, upon the recommendation of the U.S. Attorney (or where a case is not being handled by a U.S. Attorney's Office, upon the recommendation of the appropriate supervisory official of the Department of Justice), an appropriate Deputy Assistant Attorney General has authorized the application for the warrant. Provided, however, that in an emergency situation in which the immediacy of the need to seize the materials does not permit an opportunity to secure the authorization of a Deputy Assistant Attorney General, the application may be authorized by the U.S. Attorney (or where the case is not being handled by a U.S. Attorney's Office, by the appropriate supervisory official of the Department of Justice) if an appropriate Deputy Assistant Attorney General is notified of the authorization and the basis for justifying such authorization under this part within 72 hours of the authorization.

(3) Whenever possible, a request for authorization by an appropriate Deputy Assistant Attorney General of a search warrant application pursuant to paragraph (b)(2) of this section shall be made in writing and shall include:

(i) The application for the warrant; and

(ii) A brief description of the facts and circumstances advanced as the basis for recommending authorization of the application under this part.

If a request for authorization of the application is made orally or if, in an emergency situation, the application is authorized by the U.S. Attorney or a supervisory official of the Department of Justice as provided in paragraph (b)(2) of this section, a written record of the request including the materials specified in paragraphs (b)(3) (i) and (ii) of this section shall be transmitted to an appropriate Deputy Assistant Attorney General within 7 days. The Deputy Assistant Attorneys General shall keep a record of the disposition of all requests for authorizations of search warrant applications made under paragraph (b) of this section.

(**4**) A search warrant authorized under paragraph (b)(2) of this section shall be executed in such a manner as to minimize, to the greatest extent practicable, scrutiny of confidential materials.

(5) Although it is impossible to define the full range of additional doctor-like therapeutic relationships which involve the furnishing or development of private information, the U.S. Attorney (or where a case is not being handled by a U.S. Attorney's Office, the appropriate

supervisory official of the Department of Justice) should determine whether a search for documentary materials held by other disinterested third party professionals involved in such relationships (e.g. psychologists or psychiatric social workers or nurses) would implicate the special privacy concerns which are addressed in paragraph (b) of this section. If the U.S. Attorney (or other supervisory official of the Department of Justice) determines that such a search would require review of extremely confidential information furnished or developed for the purposes of professional counseling or treatment, the provisions of this subsection should be applied. Otherwise, at a minimum, the requirements of paragraph (a) of this section must be met.

(c) Considerations bearing on choice of methods. In determining whether, as an alternative to the use of a search warrant, the use of a subpoena or other less intrusive means of obtaining documentary materials would substantially jeopardize the availability or usefulness of the materials sought, the following factors, among others, should be considered:

(1) Whether it appears that the use of a subpoena or other alternative which gives advance notice of the government's interest in obtaining the materials would be likely to result in the destruction, alteration, concealment, or transfer of the materials sought; considerations, among others, bearing on this issue may include:

(i) Whether a suspect has access to the materials sought;

(ii) Whether there is a close relationship of friendship, loyalty, or sympathy between the possessor of the materials and a suspect;

(iii) Whether the possessor of the materials is under the domination

or control of a suspect;

(iv) Whether the possessor of the materials has an interest in preventing the disclosure of the materials to the government;

(v) Whether the possessor's willingness to comply with a subpoena or request by the government would be likely to subject him to intimidation or threats of reprisal;

(vi) Whether the possessor of the materials has previously acted to obstruct a criminal investigation or judicial proceeding or refused to comply with or acted in defiance of court orders; or

(vii) Whether the possessor has expressed an intent to destroy, conceal, alter, or transfer the materials;

(2) The immediacy of the government's need to obtain the materials; considerations, among others, bearing on this issue may include:

(i) Whether the immediate seizure of the materials is necessary to prevent injury to persons or property;

(ii) Whether the prompt seizure of the materials is necessary to preserve their evidentiary value;

(iii) Whether delay in obtaining the materials would significantly jeopardize an ongoing investigation or prosecution; or

(iv) Whether a legally enforceable form of process, other than a search warrant, is reasonably available as a means of obtaining the materials.

The fact that the disinterested third party possessing the materials may have grounds to challenge a subpoena or other legal process is not in itself a legitimate basis for the use of a search warrant.

Sec. 59.**5** Functions and authorities of the Deputy Assistant Attorneys General.

The functions and authorities of the Deputy Assistant Attorneys General set out in this part may at any time be exercised by an Assistant Attorney General, the Associate Attorney General, the Deputy Attorney General, or the Attorney General.

Sec. 59.**6** Sanctions.

(a) Any federal officer or employee violating the guidelines set forth in this part shall be subject to appropriate disciplinary action by the agency or department by which he is employed.

(b) Pursuant to section 202 of the Privacy Protection Act of 1980 (sec. 202, Pub. L. 96-440, 94 Stat. 1879 (42 U.S.C. 2000aa-12)), an issue relating to the compliance, or the failure to comply, with the guidelines set forth in this part may not be litigated, and a court may not entertain such an issue as the basis for the suppression or exclusion of evidence.