Forward to the CLETP Text

January, 2003

The mission of the Federal Law Enforcement Training Center (FLETC) is to serve as the Federal government's leader for and provider of world-class law enforcement training. In keeping with this high standard, the FLETC's Legal Division consistently provides efficient tools to the law enforcement student of every experience level. The Legal Division maintains a web page, the Quarterly Review, and other published materials. In this spirit, we offer our CLETP student text in book format.

This book represents more than twenty years of continuous, diligent legal research and annual revision. Numerous Legal Division instructors from various backgrounds and experiences have contributed to the development and maintenance of this publication. The complete revision of the text for this year is one of several steps designed to make the CLETP more pertinent and valuable to officers and agents with field experience.

This text provides an exceptional refresher and review of important legal concepts. We encourage you to familiarize yourself with this book's content and then explore *The Quarterly Review* and other legal materials at our web site found at:

www.fletc.gov/legal/legal_home.htm

We hope you find this format easy to use and informative. If you have any suggestions or questions about this book or any other Legal Division instruction, program or product, contact us. Continued good luck in your studies and your career in law enforcement.

J. Alexander Atwood, JD
Legal Division Chief

The FLETC Mission

Our mission is to serve as the Federal government's leader for and provider of world-class law enforcement training. We prepare new and experienced law enforcement professionals to fulfill their responsibilities in a safe manner and at the highest level of proficiency. We also ensure that training is provided in the most cost-effective manner by taking advantage of economies of scale available only from a consolidated law enforcement training organization.

CONTINUING LEGAL EDUCATION TRAINING PROGRAM (CLETP)

Federal law enforcement officers and agents attending the CLETP receive a refresher in the legal subject matter presented in their basic training, updated by a review of recent court decisions and legislative changes to the laws that are applicable to the law enforcement officer/agent. This knowledge can help officers avoid being held liable for alleged improper conduct, prevent evidence admissibility problems and increase their investigative skills in gathering evidence. The CLETP is offered at the FLETC in Glynco and on an export basis.

******

Cases cited in the FOURTH AMENDMENT and SELF INCRIMINATION chapters are briefed in the companion text *LEGAL ISSUES SOURCE BOOK*. In all other chapters, case cites are provided in this text.

TABLE OF CONTENTS

4TH AMENDMENT 1

GOVERNMENT WORKPLACE SEARCHES 112

ELECTRONIC LAW AND EVIDENCE 125

SEARCHING AND SEIZING COMPUTERS 160

COURTROOM EVIDENCE 226

BRIBERY / GRATUITIES 263

FALSE STATEMENTS 269

THEFT, EMBEZZLEMENT AND CONVERSION 274

OFFICER LIABILITY 282

SELF-INCRIMINATION 321

LEGAL RESOURCE WEB SITES 346

CONTRIBUTORS

4th Amendment
Self-Incrimination

These chapters were contributed by **John Besselman**. John presently serves the Legal Division as the Branch Chief of Advanced Training. He has been a member of the division since 1997. John is a graduate of Kent State University and the Ohio State University College of Law. He can be contacted at (912) 267-2693 or jbesselm@fletc.treas.gov.

Electronic Law and Evidence
Government Workplace Searches
Searching and Seizing Computers

Bryan Lemons contributed Electronic Law and Evidence, Government Workplace Searches, and co-authored Searching and Seizing Computers. Bryan has been a member of the Legal Division since 1999 and presently serves the division as the Branch Chief for Basic Legal Training. Bryan served in the U.S. Marine Corps as an officer for ten years prior to joining the FLETC Legal Division. He is a graduate of the St. Louis University School of Law and can be contacted at (912) 267-2945 or blemons@fletc.treas.gov.

Courtroom Evidence
Searching and Seizing Computers

Keith Hodges contributed Courtroom Evidence and co-authored Searching and Seizing Computers. Keith is a graduate of Furman University (B.A.) and the University of South Carolina (J.D.). Prior to joining the Legal Division in August 2000, Keith served as a commander, prosecutor, defense counsel, Staff Judge Advocate, and Military Judge in the U.S. Army. He may be contacted at (912) 554-4757 or khodges@fletc.treas.gov.

Bribery/Gratuities
False Statements
Theft, Embezzlement and Conversion

These chapters were contributed by **Keith Hunsucker**. Keith is a Senior Legal Instructor at the Federal Law Enforcement Training Center. Prior to joining the Legal Division, he was an attorney with the United States Department of Justice for over ten years. Mr. Hunsucker was awarded the 1994 Commissioner's Award for Immigration and Naturalization Attorney of the Year. He is a graduate from the University of Akron and the University of Akron School of Law. He may be contacted at (912)267-2596 or khunsuck@fletc.treas.gov.

Officer Liability

This chapter was contributed by **Robert Cauthen**. Bob has been a member of the Legal Division since 1999 and presently serves as the Program Manager of the Continuing Legal Education Training Program and the editor of this student text and *The Quarterly Review*. He may be contacted at (912)267-2179 or rcauthen@fletc.treas.gov.

4TH AMENDMENT

I. INTRODUCTION 5
A. PERSONS COVERED 6
B. PERSONAL NON-TESTIMONIAL EVIDENCE 7
C. SEARCHES DEFINED 7
1. Reasonable Expectation of Privacy 8
2. "Papers and Effects" (personal property) 9
3. "Houses" 11
4. Curtilage and Open Fields 13
5. Surveillance vs. Privacy 15
6. Abandonment 16
D. SEIZURE DEFINED 18
1. Voluntary Contacts 18
2. Investigative Stop ("Investigative Detention" or "Terry Stop") 20
3. Arrest 21
4. The Two Different Seizures 21
a. Duration 22
b. Use of Force 23
E. LEVELS OF SUSPICION/STANDARDS OF PROOF 25
1. Mere Suspicion 25
2. Reasonable Suspicion 25
a. the suspect's reputation 26
b. report of a recent crime in the area 26
c. time of day 26
d. location 27
e. suspicious or unusual conduct 27
f. prior information 27
g. behavior upon seeing a law enforcement officer 27
h. running from the sight of police 28
i. profile of a known criminal type 28
3. Probable Cause 28
a. Aguilar test 29
b. Gates test 33
4. Reasonable Certainty 33
5. Proof Beyond a Reasonable Doubt 33
F. THE TERRY FRISK 34

1. Plain Touch Doctrine 37
2. Frisking Vehicles 37
3. Frisking Containers 38
4. Frisking Companions 38
5. Frisking the Opposite Sex 39
6. Related "Terry Stop" Points on Vehicle Stops 39

II. THE EXCLUSIONARY RULE 39
A. DEVELOPMENT OF THE RULE SINCE 1914 40
B. FRUIT OF THE POISONOUS TREE 40
C. EXCEPTIONS TO THE EXCLUSIONARY RULE 41
1. Standing 41
2. Independent Source 42
3. Inevitable Discovery 42
4. Good Faith Exception 43
5. Impeachment of Testimony 44
6. Grand Jury 44
7. Foreign Searches 45
8. Other Exceptions 45

III. ARREST 45
A. ARREST AUTHORITY GENERALLY 45
B. STATUS OF FEDERAL LAW ENFORCEMENT OFFICERS RESPONDING TO STATE CRIMES 46
C. ARRESTS BASED ON OUTSTANDING ARREST WARRANTS 48
1. Outstanding Federal Warrant 48
2. Outstanding State Warrants 49
D. CROSSING THE LINE FROM A "STOP" TO AN "ARREST" 50
E. ARRESTS MADE WITHOUT PROBABLE CAUSE AND/OR WITHOUT AUTHORITY 50

IV. METHODS OF ARREST 51
A. OBTAINING ARREST WARRANTS 51
B. ALTERNATIVES TO ARREST 53
C. LIMITATIONS ON FEDERAL ARREST WARRANTS 54
D. ARREST WARRANTS 55
1. Arrest in Defendant's Home 55
2. Arrest in Third-Party Premises 55

3. Protective Sweeps (The Buie Doctrine) 56
E. EXIGENT CIRCUMSTANCES AND ARREST 58
F. WARRANTLESS ENTRY BY CONSENT 59
G. ARRESTS WITHOUT WARRANTS 60
1. Felonies 60
2. Misdemeanors 60
H. USE OF FORCE IN ARREST AND SEARCH WARRANTS 61

V. USE OF FORCE IN MAKING ARRESTS 65
A. NECESSARY FORCE 65
B. USE OF DEADLY FORCE 67
C. THE DOJ/TREASURY FIREARMS POLICY 68
D. FIREARMS GUIDELINES 69

VI. SEARCHES WITH A SEARCH WARRANT 69
A. AUTHORITY TO ISSUE SEARCH WARRANTS 70
B. ANTICIPATORY SEARCH WARRANT 71
C. PROPERTY AND PERSONS SUBJECT TO SEIZURE WITH A WARRANT 71
D. AFFIDAVIT FOR A SEARCH WARRANT 72
1. Descriptions 72
a. place to be searched 73
b. persons or things to be seized 74
2. Probable Cause 75
a. personal knowledge - reasonable officer standard 75
b. hearsay and the Aguilar test 76
c. corroboration and other facts 76
d. timeliness 77
e. place to be searched 77
f. containers to be searched 77
g. dog alerts 78
3. Affidavits - Miscellaneous 78
E. TELEPHONIC SEARCH WARRANTS 79
F. EXECUTION OF THE SEARCH WARRANT 80
1. Authority to Execute Federal Search Warrants 80
2. Time Limits 81
3. Searches, Seizures, and Scope of the Warrant 81

a. areas not covered by the warrant 82
b. seizure of items not particularly described in the warrant 82
c. remaining on the premises 83
4. Plain View 83
a. constitutionally present 84
b. lawful access 85
c. apparent incriminating nature 85
5. Search, Detention, and Arrest of Persons on the Premises 86
6. Service of the Copy of the Warrant 88
7. Inventory and Return of the Warrant 88
8. Civil Lawsuits 90

VII. SEARCHES WITHOUT WARRANTS (PC Required) 90
A. MOBILE CONVEYANCES - THE CARROLL DOCTRINE 91
B. DESTRUCTION OF EVIDENCE 93
C. HOT PURSUIT 94
D. EMERGENCY SCENE 96

VIII. SEARCHES REQUIRING NEITHER A WARRANT NOR PROBABLE CAUSE 97
A. SEARCHES INCIDENT TO ARREST 97
1. Searches of the Person Arrested 98
2. Searches of the Arrestee's Area and Possessions 98
3. Contemporaneousness Requirement 99
4. Body Cavity Searches 100
5. Protective Sweeps and Security Measures 101
B. CONSENT SEARCHES 102
1. Voluntary 102
2. Authority to Consent 103
C. INVENTORIES 105
D. INSPECTIONS 105

IX. RELATED SEARCH AND SEIZURE ISSUES 108
A. PRETEXTUAL STOPS AND SEARCHES AND SEIZURES 108
B. ENTRANCES IN UNDERCOVER CAPACITY 109
C. FORFEITURES 110

I. INTRODUCTION

> THE FOURTH AMENDMENT
>
> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Constitution serves as a contract between the American people and the federal government. The federal government has made a set of promises, most of which can be found in the Bill of Rights, in exchange for the ability to govern. This contract places a variety of restrictions on the federal government. For example, the federal government has promised not to establish a religion (First Amendment), compel persons to be witnesses against themselves in any criminal case (Fifth Amendment), nor to inflict cruel and unusual punishment (Eighth Amendment). The Fourth Amendment places another kind of restriction on the federal government. The Fourth Amendment prohibits the federal government from conducting unreasonable searches and seizures.

The Fourth Amendment is an important legal area for law enforcement officers for several reasons. First, important evidence in criminal investigations is often obtained by searching a suspect's body, house, office or vehicle. Second, conducting searches and seizures is one of the most dangerous activities an officer will perform. Third, many lawsuits against officers stem from their actions in conducting a search. Courts may hold officers personally liable for money damages to persons whose constitutional rights have been violated by unreasonable searches and seizures. A functional understanding of the Fourth Amendment is critical to the success and effectiveness of a federal law enforcement officer.

> The Constitution regulates **government** behavior.

A close inspection of the Fourth Amendment reveals that officers need not conduct all searches and seizures with a warrant. The Fourth

Amendment does not even require probable cause to support all searches and seizures. Some types of searches, such as consent searches or those performed incident to a lawful arrest, require neither a warrant nor probable cause. The rule of the Fourth Amendment is that every search and seizure be reasonable.

A. PERSONS COVERED

Officers are likely to confront Fourth Amendment issues because of the girth of the protections found within. The Constitution protects persons rather than places. Katz v. United States. No differentiation is made between citizens of the United States and non-citizens, or between innocent or guilty persons. The Fourth Amendment protects "the people," even those who may be in this country illegally, when they voluntarily engage in conduct with the United States. The Supreme Court stated that "'the people' protected by the Fourth Amendment, and by the First and Second Amendments, and to whom rights and powers are reserved in the Ninth and Tenth Amendments, refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community." United States v. Verdugo-Urquidez.

Persons in the military service of the United States also have the protection of the Fourth Amendment. However, under some circumstances, military personnel have a reduced expectation of privacy due to the specialized mission and needs of the armed forces in fighting wars and maintaining the national defense.

A corporation, although not a living person, is a "person" for the purpose of the protection of the Fourth Amendment. Dow Chemical Company v. United States. A corporation, as a legal entity, may own property, sue and be sued, and be prosecuted for criminal violations. The Fourth Amendment protects corporations from unreasonable searches and seizures to the same extent as others persons.

B. PERSONAL NON-TESTIMONIAL EVIDENCE

As discussed in the Self-Incrimination chapter, some forms of evidence are "non-testimonial" and, therefore, not subject to the protection of the Fifth Amendment's self-incrimination clause. Evidence in the form of fingerprints, handwriting exemplars, blood samples, etc., may be taken from persons without causing those persons to be witnesses against themselves. However, as individuals do manifest an expectation of privacy in their bodies, the Fourth Amendment protects these non-testimonial items of evidence. Schmerber v. California; Winston v. Lee. Courts will suppress evidence that officers unreasonably search for or seize. For example, fingerprints are non-testimonial evidence and the taking of them from suspects, even over their objection, does not compel those individuals to be witnesses against themselves. However, if officers illegally arrested the suspects to obtain their fingerprints, the court will consider this seizure unreasonable and will suppress the evidence. Taylor v. Alabama.

C. SEARCHES DEFINED

The Fourth Amendment provides that the people shall be " . . . secure in their persons, houses, papers and effects against unreasonable *searches* and *seizures* …." The Fourth Amendment regulates the government when it is searching and seizing persons and things. If the government is not "searching" or "seizing" within the meaning of the Fourth Amendment, the Fourth Amendment is not applicable. Therefore, it is important to understand whether a "search" or "seizure" is taking place.

Knowing that the Constitution serves as a regulator of only federal (and in some instances, state) actions, the first component of a definition of a search (or seizure) must include governmental action. If the behavior or activities are those of private parties or foreign governments, the events

are not controlled by the Fourth Amendment, provided the federal (or state) government did not encourage or solicit the activities.

1. Reasonable Expectation of Privacy

The Supreme Court provided a definition for the term "search" in Katz v. United States. The Court stated that the Constitution protects *people,* not places. Another way to understand this principle is that the Fourth Amendment changed its focus from protecting property rights to protecting privacy rights. The degree of protection provided by the Constitution to an individual depends on the reasonable expectation of privacy maintained by that individual.

The Court articulated a two-prong test in Katz to determine if a reasonable expectation of privacy exists:

(1) Does the individual exhibit an actual expectation of privacy?

and, if so

(2) Is the right to privacy demanded one that society is prepared to grant as reasonable?

SEARCH DEFINED
Government
+
Intrusion
+
Reasonable Expectation of Privacy

What one seeks to preserve as private, even though in an area accessible to the public, may be protected. For example, a person who uses a public telephone booth and closes the door manifests an expectation of privacy in the conversation. Law enforcement officers using a concealed microphone on that public telephone booth are engaged in a Fourth Amendment search.

On the other hand, what one exposes to the public, even though in the privacy of their home or office, is not protected. For instance,

criminally possessed items such as contraband located in a garage, but plainly visible from a public sidewalk, can be observed by law enforcement officers with no concern for the Fourth Amendment's limitations, because this is not a search. Suspects cannot reasonably expect privacy in information or items they have unknowingly exposed to other either. For instance, a conversation overheard in a public restaurant by a law enforcement officer is not a search even if those involved in the conversation believed their communications were private.

Mr. Katz manifested an expectation of privacy by entering a telephone booth and closing the door. He had an expectation of privacy that society was prepared to recognize. He met both elements of the test. The law enforcement officers who electronically eavesdropped on his conversation were conducting a search and, therefore, were bound by Fourth Amendment restrictions. Unfortunately, the officers had neither a warrant nor could they demonstrate sufficient conditions that would justify a warrantless search. Therefore, their search was unreasonable.

2. "Papers and Effects" (personal property)

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, . . ."

The protection of the Fourth Amendment extends to all personal property in which someone has a reasonable expectation of privacy. The specific mention of "papers" in the Fourth Amendment is recognition of the great expectation of privacy that individuals have in their personal papers.

Although the government may not compel witnesses to produce their personal papers to use against them because of the Fifth Amendment, there is no special sanctity in papers as distinguished from other kinds of property for the purposes of search and seizure. Officers

may obtain a search warrant to seize personal papers, diaries, bank and financial records, etc., and use these items as evidence in court.

The expectation of privacy in first-class mail is such that the government may not open it except under the authority of a search warrant. With lower classes of mail, the expectation of privacy is reduced and postal officials, pursuant to postal regulations, may open such mail. Since the expectation of privacy in mail only extends to the contents of the letter or parcel, the weight, description, external markings and writings are exposed to the public and may be noted by officers without obtaining a search warrant, subject to postal regulations. (This investigative technique is sometimes called a "mail cover.") The courts have also permitted a reasonable delay in the transmission of an item of mail to obtain a search warrant based on probable cause. United States v. Van Leeuwen.

In United States v. Chadwick, the Supreme Court recognized a privacy interest in personal containers, such as luggage, briefcases, purses, etc., since these are areas where persons normally keep their papers and effects. The Court has also held that some containers reveal their contents by being constructed of clear material, or by "clearly announcing" its contents (such as a tied-off balloon). These containers, the Court has held, do not constitute an area where one would reasonably expect privacy.

The Fourth Amendment protects many kinds of evidence from unreasonable searches and seizures by the government. This is true regardless of the nature of the item seized. Even contraband and other property illegally possessed by an individual will be suppressed if unreasonably seized. Most courts, however, do not find that those in possession of stolen property have standing to object to the unreasonable search and seizure of that property. James v. Borg, 24 F.3d 20 (9th Cir. 1994). Note that the government does not return contraband and other illegally possessed items that it has unreasonably taken from a defendant. Trupiano v. United States; Horton v. California.

3. "Houses"

Courts have interpreted the term "houses" in the Fourth Amendment very broadly and have extended the definition to cover practically all buildings and structures, whether used as residences, offices, or storage facilities. The concepts of traditional property law are not controlling since the measure of the Fourth Amendment's protection is established by the individual's reasonable expectation of privacy concerning a particular area. This will be discussed more fully below in the section on "curtilage."

The Fourth Amendment protects a dwelling in a greater manner than any other structure. This is due to the traditional expectation of privacy manifested in the home. A structure that is temporarily unoccupied, whether a dwelling or not, does not lose this protection. For example, a vacation cottage which is occupied for only a few weeks each year has the protection of the Fourth Amendment from unreasonable searches at all times.

The Fourth Amendment also protects multiple-unit dwellings, such as apartments, hotel rooms, etc., during the period that the resident has the right to occupancy and use of the premises. Each dwelling unit in a multiple-unit structure is treated as an independent premises entitled to Fourth Amendment protection. If officers want to search an entire apartment building containing four units, they must establish reason to justify the search of each unit to comply with the requirements of the Fourth Amendment.

The standard expectation of privacy may not accompany some types of dwelling units. For example, the occupancy of college dormitories may be subject to regulations authorizing college officials to enter rooms to inspect mechanical equipment or to provide maid service. The residents retain an expectation of privacy in their personal belongings and their rooms, subject to the limited specific purposes for which others

may have authority to enter. College officials could not abuse their limited inspection authority to enter a student's room, nor authorize law enforcement officers to enter the room to conduct a search for criminal evidence. If officials of a private college conduct the intrusion, any evidence discovered would be admissible since it would be the product of private actions, to which the Fourth Amendment has no applicability.

Some dwellings may be used to conduct illegal activities such as gambling or prostitution. Even though the activities offend the law, the resident's right to expect privacy is protected. The illegal activities involved do not place the premises beyond the protection of the Fourth Amendment. However, individuals located at the premises for the exclusive purpose of engaging in commercial activities (such as drug transactions) do not have an expectation of privacy in the dwelling. Minnesota v. Carter.

The amount of privacy that is reasonable to expect in offices and other business premises depends on the character of the premises itself and the degree of public access. Wherever the public has access, law enforcement officers have access. However, permission to enter a public office or premises does not create a right to search inaccessible areas. Officers may make observations of and seize evidence in plain or open view (see below), but have no authority to search desks, filing cabinets, closets or other closed or limited-access spaces. Areas that an individual seeks to preserve as private, even though in an area accessible to the public, may be protected by the Fourth Amendment.

Persons typically cannot establish a reasonable expectation of privacy in a jail or prison. The need for security and discipline outweigh the privacy protection normally afforded a person by the Fourth Amendment. In prison, surveillance and monitoring are routine. Note that a reasonable expectation of privacy is established in those rooms specifically provided for prisoners to confer with their attorneys.

4. Curtilage and Open Fields

Curtilage is a common law property concept that defined the area of the home and separated it from the surrounding "open fields." Curtilage is defined as *that area which protects the intimate activity associated with the sanctity of a person's house and the privacies of life.* Courts have extended the protection of the Fourth Amendment from the dwelling to the curtilage around the house. Just as law enforcement officers may not enter the house to search without a warrant or other legal justification, neither may they enter the curtilage.

Curtilage is a fluid concept. This fluidity presents a major difficulty in determining whether a specific area is curtilage or not. Courts have been unable to give a fixed definition of curtilage for every case. In a typical suburban neighborhood, the curtilage of a home probably extends to the entire front, side and back yards. In an urban area, the curtilage may be only a small private courtyard at the rear of the house. In a rural area, the curtilage of the farmhouse might extend to adjacent outbuildings such as barns and storage sheds, and may include private garden areas near the house. Each case is different depending on its own special facts and circumstances.

Curtilage- area which protects the intimate activity associated with the sanctity of a person's house and the privacies of life.

To determine if an area is within the curtilage, the courts have <u>considered</u>:

- the nearness or connection to the dwelling
- its inclusion within a general enclosure surrounding the dwelling
- whether the area is used in association with the intimate activities of the home

- the steps taken by the homeowner to protect the area from view by passers by. United States v. Dunn.

Individuals maintain their expectation of privacy in the interior of structures outside the curtilage. However, the expectation of privacy does not extend to any area beyond the walls of the structure itself. For example, if an officer enters the backyard of a private home in order to look into the window of a small workshop attached to the home and observes evidence of a crime, that observation is considered a search because the officer has intruded on the curtilage. On the other hand, if the defendants maintained an unfenced workshop on property outside the curtilage, the officer could approach the workshop and look through the window without having this action scrutinized by the Fourth Amendment. The officer still could not enter the workshop without complying with the Fourth Amendment.

The Katz case reduced property concepts as they relate to curtilage. The courts still occasionally use the terms curtilage and open fields, but they use them to define the areas of expectation of privacy around the dwelling house. Courts consider the traditional curtilage area as the area where an individual has a reasonable expectation of privacy. Open fields are areas where the landowner does not have an expectation of privacy.

Officers on official business may enter upon the open fields to make observations of evidence in "open view" without a warrant or any other legal justification. If the officer obtains evidence from the open fields, its use does not violate the Fourth Amendment. The law enforcement officers may be trespassers on private property, but this fact will not prevent the lawful use of evidence obtained in the performance of their law enforcement duties. If the officers are physically located off the curtilage, they may observe the curtilage. If there is any doubt whether a vantage point or a place to be intruded upon is within the curtilage, the officers should obtain a warrant.

5. Surveillance vs. Privacy

A primary function of the law enforcement officer is to make observations and obtain evidence. The use of surveillance by officers is an accepted and effective tool for obtaining evidence. However, limitations on the scope of surveillance exist. Generally, the use of an electronic listening device is an invasion of privacy. On the other hand, if officers can position themselves lawfully in an area where they may eavesdrop on a conversation with the naked ear, the officers may lawfully overhear these conversations. This is not a search as the officers have not intruded on a reasonable expectation of privacy. For example, the courts have held that defendants have no *reasonable* expectation of privacy in their motel room conversations that a law enforcement officer overheard by listening through the door to the adjoining motel room.

An area of concern for law enforcement officers conducting surveillance is the use of electronic tracking devices, or beepers, to surreptitiously monitor the movements of automobiles, aircraft, vessels or other moveable items. Courts determine the legality of beeper use with a two-step analysis: (1) does the Fourth Amendment apply to the *installation* of the beeper? and (2) does the Fourth Amendment apply to the *monitoring* of the beeper?

The government needs a warrant, or a well-established exception to the warrant requirement, to *install* a beeper if installation of the beeper requires entry into an area protected by a reasonable expectation of privacy. On the other hand, the Supreme Court held in United States v. Knotts that the monitoring of a beeper on public highways, waterways or airways for surveillance purposes is not a violation of one's reasonable expectation of privacy. Once the beeper enters into an area in which a reasonable expectation of privacy exists a warrant is required to monitor. United States v. Karo.

The courts have generally held that a person has no legitimate reason to believe that the government will not place a beeper in items exchanged for contraband (e.g., a television set exchanged by undercover officers for narcotics). Due to the divergence of opinions by various courts, officers should contact either the United States Attorney's office or their agency's legal advisor before using any tracking device to determine the position of the courts in their area on the legality of the use of these devices.

6. Abandonment

If persons voluntarily abandon their ownership, right to usage, possession or interest in property, they no longer have a reasonable expectation of privacy in that property. Abandoned property does not enjoy Fourth Amendment protection because: (1) the defendant has given up a reasonable expectation of privacy in that property; (2) the defendant no longer has standing (see below) to object to use of the evidence in court; or (3) both.

The intrusion into abandoned property is not a Fourth Amendment search because there is no expectation of privacy to intrude upon. If the court finds that the possessor abandoned the property before the intrusion by an officer, then the actions of the officer are not a search. This is true whether the officer knew that the property was abandoned at the time of the intrusion or not.

Abandonment is defined as the voluntary casting away or relinquishing of possession of property with no present intention of reclaiming it. The resolution of the question of whether abandonment of property has resulted is determined from all of the facts and circumstances surrounding the alleged abandonment, e.g., location, statement, conditions, actions.

The location of allegedly abandoned property is very important. If an individual discards personal property in an area where one normally

has a lesser expectation of privacy, i.e., a public place, then that property may be deemed to be abandoned without proving that the defendant intended to rid himself of it permanently. Generally, the act of discarding property alone is sufficient to determine abandonment. For example, if individuals walking through a public park notice that a police officer is following them, they may decide to discard their bag of narcotics behind a park bench. The officer can pick up the bag and look inside. The officer's actions constitute neither a search nor seizure. A court could allow the government to introduce the narcotics against the defendants because they were abandoned. It is immaterial that the individuals could claim their true intent was to hide the bag and return for it after the police officer had left. Individuals may abandon their house, automobile or any other property if the court finds that there was an apparent *intent* to abandon plus the *act* of abandonment.

Property discarded in a traditionally private area, e.g., an individual's home, or on the curtilage, is not generally considered to be abandoned. Some other action could be required to show not only the act of discarding, but the actual intent to relinquish the expectation of privacy. An example of this is where individuals discard items in their trashcan in their dwelling or on their curtilage. The item should not be considered abandoned until it is removed from the curtilage for garbage pickup or until the garbage collectors have taken possession of the property. California v. Greenwood.

One limitation that the courts have placed on searching or seizing property alleged to have been abandoned is that the police may not take advantage of abandonment induced by the *unlawful* acts of the law enforcement officers. For example, if officers illegally stop an automobile and notice an occupant throw a paper bag out onto the side of the road, a subsequent seizure and search of that bag would be illegal. Courts would not deem the bag abandoned because the officers caused the reaction by their *illegal* acts. The abandonment was not voluntary. The owner retains standing to object to the violation of his or her constitutional rights.

D. SEIZURE DEFINED

A person has been "seized" by an officer if a reasonable person under the circumstances would believe they were not free to leave or to decline the officer's requests. A seizure occurs whenever the officer 1) uses physical force on a person, however slight, or 2) makes a "show of authority," and the person submits to that authority. The two primary types of seizures are 'investigative detentions," also known as Terry stops, and "arrests." Brower v. County of Inyo; California v. Hodari D.; Florida v. Bostick; United States v. Mendenhall; Florida v. Royer.

SEIZURE occurs upon:

1) use of physical force, however slight,

OR

2) submission to a "show of authority"

1. Voluntary Contacts

Generally, there are two broad types of person-police encounters: voluntary and involuntary contacts. No legal justification is required for a voluntary contact with a person. Involuntary contacts must be justified by either reasonable suspicion (for an investigative detention) or probable cause (for an arrest). [Please Note: Throughout this course, the terms "investigative detention," "investigative stop," "temporary detention," "Terry stops," and "stop, question and frisk" are often used interchangeably, just as they are used in both legal and law enforcement circles.]

A "voluntary contact" is an encounter in which the citizen is free to disengage and continue about their business. It occurs when an officer voluntarily engages the citizen in conversation. In such a case, the officer has not seized the citizen, who is free to leave at any time. As a result, there are no Fourth Amendment issues involved and the government need not justify a voluntary contact. It requires no facts or degree of suspicion by the officer. The contact should be reasonable in nature and for a short duration.

For example, an officer has a hunch that a citizen is involved in criminal activity, but cannot articulate any objective facts to support his or her suspicion. At this point, the officer has a mere suspicion (see below) that criminal activity may be taking place. The officer is not justified in making an arrest (which requires probable cause) or even an investigative detention (which requires reasonable suspicion). However, the officer is justified in approaching the citizen and asking him or her: "How are you doing tonight? Is everything alright?" If the citizen is willing to speak with the officer, then the conversation may continue, and the officer might learn something that causes the officer to develop reasonable suspicion or even probable cause. Under these circumstances, the citizen is free to refuse to speak with the officer and to walk away.

The following actions, without more, should NOT convert a voluntary contact into a seizure:

- Approaching an individual in a public place.
- Identifying one's self as a law enforcement officer.
- Asking a person if they are willing to answer a few questions.
- Questioning a person, if they willingly agree to listen.
- Asking for, examining, and returning a form of identification.
- Giving assistance to an individual.
- Controlling the movements of a crowd, e.g. directing traffic.

In most circumstances, a person has the right to not talk to officers nor answer their questions. Should an individual exercise that right, their refusal is not enough, in and of itself, to create reasonable suspicion (permitting an investigative stop) or probable cause (permitting an arrest).

In order to avoid turning a voluntary contact into an investigative stop:

- Be polite - ask if assistance is needed.
- Identify self as soon as possible (i.e. "Hi, I'm Officer Smith").
- Make requests, NOT demands.
- Give a general, brief explanation of purpose.
- Do NOT give the person Miranda warnings.
- Do NOT use any force.
- Do NOT frisk.

A key factor the courts will look at to determine if the "contact" was voluntary or involuntary will be - - "Would a reasonable person believe he or she was free to refuse the officer's requests, and/or free to leave the scene and go on his or her way?"

2. Investigative Stop (or "Investigative Detention," or "Terry Stop")

An "investigative stop" is a brief, temporary seizure of a person as a part of an investigation to make a limited inquiry into possible criminal activity. Terry v. Ohio. Such seizures must be supported by reasonable suspicion (see below), legal authority, and a legitimate purpose. An officer may use that degree of force that is reasonably necessary to effect the stop. The length of the seizure must be as brief as possible. If, during this temporary seizure, information giving rise to

INVESTIGATIVE STOP:

Brief
Temporary
Seizure

… of a person to make a limited inquiry into possible criminal activity.

probable cause develops, then the officer may arrest the suspect. However, if the officer is unable to develop probable cause after conducting a lawful investigative detention - - then the officer must release the suspect.

3. Arrest

An "arrest" is the taking of a person into official custody in order to have that person answer to a criminal charge. Officers arrest persons to insure their presence before a court of law for judicial proceedings (i.e. to answer to the formal criminal charge(s) against them). Once arrested and brought before the court for an initial appearance, the court may set bail, which is designed to assure the person's reappearance at future court proceedings.

The requirement for the existence of probable cause before making an arrest, and reasonable suspicion before conducting an investigative detention creates a balance between the needs of society for law and order against the individual's right to be free from an unreasonable seizure.

4. The Two Different Seizures

Depriving a person of their freedom of movement in a significant way is a seizure. Whether this seizure is a stop or arrest depends on several factors. Ultimately, a court will determine this issue by examining several factors, such as the force used, the degree of inconvenience imposed, the reasonableness of the action under the circumstances, etc. Florida v. Royer. This is one of the most difficult determinations a court will make. Some of the factors courts will consider in determining whether a seizure is a stop or an arrest include:

- ➔ Duration of seizure
- ➔ Use of force during seizure
- ➔ Location of the seizure

- ➔ Removal of suspect from area
- ➔ Other factors

a. Duration

The courts have held that once an officer stops an individual for an investigation, that individual may only be detained for a "reasonable amount of time," which is determined by the facts and circumstances of each situation. By definition, a "stop" is limited to a short, temporary period of time. Once an individual has been stopped, he or she may be detained only for as long as is reasonably necessary to accomplish the investigative purpose of the stop. For example, if officers stop a vehicle for a suspected equipment violation, they may detain it only long enough to investigate that suspected violation and to issue a citation if necessary. At the end of the stop, the officer may ask for consent to continue further investigation, but if consent is refused, the person must be released. Ohio v. Robinette.

If the officer detains the vehicle any longer, in the absence of other evidence indicating the possible existence of other violations, evidence obtained during this period is subject to the exclusionary rule. Likewise, officers who stop an individual for a traffic violation and discover that they cannot verify the person's license, etc., due to the police computer being out of service, cannot hold that person some extended time until the computer is back on line.

If, on the other hand, further suspicious facts are brought to the officer's attention during the lawful detention, this will justify detaining the individual until those facts can also be investigated. For example, if a suspect gives an officer false information that causes the officer to waste time trying to verify the "phony story" - - a longer temporary detention may be justified.

A ten-minute temporary detention may be justifiable under one set of circumstances, but ruled as too long under different circumstances. The

determining factors will be - - was the length of the detention justifiable and reasonable under the circumstances? Several police agencies have adopted an informal twenty (20) minute rule, taking the position that, generally speaking, an investigatory stop should not last longer than twenty minutes unless clearly justified. This "twenty-minute rule" has never been formalized and should not be considered "policy," but is apparently used as a general guideline by some municipal police agencies nationwide.[1] This is not to be interpreted as a principle of law, but rather a guideline.

The key to the reasonableness of any detention's duration is whether the officer's intrusion into the detainee's rights was as brief and non-intrusive as possible, while still accomplishing the purpose of the stop. If the investigation could have been done in a less intrusive manner or in a shorter period of time, the detention may be unreasonable.

b. Use of Force

The courts allow an officer to use reasonable force to execute a valid investigative detention and a related frisk. However, the courts have given no general rule as guidance other than that the amount of force used must be reasonable under the facts and circumstances existing at the time of the incident. Graham v. Connor. To be reasonable, the amount of force used should be no more than that reasonably necessary to assure compliance with the officer's lawful commands. Factors to consider in determining reasonableness include:

- the seriousness of the crime being investigated and the strength of the facts supporting the officer's reasonable suspicion for the stop;

[1] The Supreme Court has become aware of the "twenty minute rule" but refused to sanction it by stating "We understand the desirability of providing law enforcement authority with a clear rule to guide their conduct. Nevertheless, we question the wisdom of a rigid time limitation. Such a limit would undermine the equally important need to allow authorities to graduate their responses to the demands of any particular situation. United States v. Place, 462 U.S. 693 (1983).

An officer who has reasonable suspicion that the suspect is the individual who just committed an armed robbery may use that force reasonably necessary to control the suspect during the investigation, to include display of weapons, handcuffs, placing the suspect in the back of a patrol car, etc.

- the number of suspects and the number of officers;

Two officers stopping six individuals may find that a greater degree of force or threat of force is necessary to maintain control due to the suspects' superior numbers.

- reasonable suspicion to believe that the suspect(s) are armed and dangerous;

Due to their reasonable suspicion, officers can take greater steps to assure their personal safety, such as frisking the suspects, their containers, and vehicles.

- the amount of resistance demonstrated by the suspect(s).

The greater the resistance by the suspect, the greater the amount of force an officer is entitled to use to overcome that resistance. The display of a drawn firearm or use of handcuffs by an officer may be deemed reasonable based on the circumstances confronting the officer at the time the weapon or handcuffs are employed. The use of handcuffs does not automatically mean a suspect is under arrest, particularly when an officer can articulate reasons for the temporary use of the restraints. In such cases, the use of handcuffs is merely an extension of the concept that a lawful Terry stop is, in fact, an involuntary contact during which time a suspect may not leave of his or her own free will.

E. LEVELS OF SUSPICION/STANDARDS OF PROOF

Different standards of proof are required to justify different levels of government action. Unless the government can establish a sufficient level of suspicion for its search and/or seizure, that action is considered unreasonable under the Fourth Amendment. The following are common standards of proof with which a law enforcement officer must be familiar:

1. Mere Suspicion

"Mere suspicion" is the lowest level of knowledge. It is nothing more than an unsupported hunch, or "gut feeling" many people experience, but cannot explain (or articulate). This level of knowledge does NOT allow an officer to take any forcible action against a person. Officers may not stop, detain, or arrest based on mere suspicion. Mere suspicion supports voluntary contacts only.[2] Mere suspicion is characterized by an inability to articulate (or explain) facts that give rise to one's suspicion.

2. Reasonable Suspicion

"Reasonable suspicion" is information that would lead an objectively reasonable officer to suspect that (1) a crime possibly has been committed (or is about to be committed) and that (2) a particular suspect might have committed the crime. It is more than mere suspicion (see above), but less than probable cause (see below). The officer must be able to identify and articulate the facts that have caused his or her suspicion. Reasonable suspicion supports an investigative detention (Terry stop). Based on reasonable suspicion, a law enforcement officer may

Some Suspicion Factors
- reputation of suspect
- recent criminal activity
- time/location
- unusual conduct
- prior information/tip
- flight upon sight of LEO

[2] No suspicion is required to conduct a voluntary contact.

temporarily stop and detain an individual for questioning.

In addition, with reasonable suspicion that a person is both armed and dangerous, the law permits the officer to conduct a "Terry frisk," that is, a pat down of the suspect's outer clothing to determine whether the suspect is armed. See Terry v. Ohio.

Over the years, the courts have provided the law enforcement profession with certain factors that officers may use to determine whether reasonable suspicion exists. It is unlikely that any of these factors, standing alone, gives rise to reasonable suspicion. However, when used as building blocks in concert with other factors, they may reach reasonable suspicion. For example, the fact that an individual is in a high crime area is not, by itself, sufficient for a stop. However, when coupled with other facts, the combined facts may result in reasonable suspicion and support a stop. The courts have held the following factors to be significant:

a. the suspect's reputation

If the officer has knowledge that the individual has a prior conviction for the suspected crime or has been known to engage in similar activities, the officer may use this knowledge in developing reasonable suspicion.

b. report of a recent crime in the area

Law enforcement officers are not required to operate in a vacuum. Information provided by members of the public can be used to develop reasonable suspicion. The kind of crime as well as how recently it occurred will both be relevant in this development.

c. time of day

Courts generally allow more flexibility in investigative stops that occur after dark or late at night than they do for daytime stops. Also, the

time of day may be a discerning factor in itself. Individuals milling about a closed warehouse fence line at 2:00 a.m. is generally more suspicious than the same activity at 2:00 p.m.

d. location

A suspect's presence in a known crime-related area can cause suspicion. If the area has a high crime rate (i.e., drug sales, car thefts, prostitution, etc.). If the area is one that is generally closed or "off limits" to the public, this is also a cause for consideration.

e. suspicious or unusual conduct

If the actions of the person are unusual and consistent with criminal behavior, they may lead to reasonable suspicion. Reasonable suspicion exists, for example, where an ATF agent working a moon shining case sees an individual driving down a backwoods road at night with no headlights on.

f. prior information

If police have received a tip that a certain type of crime is to occur and the individual's conduct is consistent with that type of crime, this may give rise to reasonable suspicion. The information's ability to predict future behavior is significant in determining whether it provides a reasonable suspicion.

g. behavior of the individual upon seeing a law enforcement officer

An individual's reaction upon realizing he or she is in the presence of a law enforcement officer is worthy of consideration in the development of reasonable suspicion. For example, law enforcement

officers may consider whether the person became nervous, attempted to hide, or slinked away from the area.

h. running from the sight of police

Law enforcement officers may consider the fact that a person runs from the sight of them as to whether or not reasonable suspicion exists to perform a stop. Running from the sight of police, by itself, does not justify a stop. There must be other factors that, taken along with the running from police, will support a finding of reasonable suspicion. Illinois v. Wardlow.

i. suspect fits a specific profile of a known criminal type

The fact that a suspect matches a particular profile does not generally create reasonable suspicion. Typically, there is nothing special about a profile. The facts constituting a profile might be enough, in and of themselves, to create reasonable suspicion, or they might simply be useful as factors in determining reasonable suspicion. United States v. Sokolow.

In addition, officers must be aware that "profiling" is susceptible to abuse and misapplication. Profiles based on race are unacceptable and will be challenged on the ground that the profile violated the constitutional requirement of equal protection of the laws. Officers must exercise extreme diligence to ensure they do not use their profiles in a discriminatory manner. In addition, officers must check their agency's current policy on profiling, and any relevant operational guidelines.

3. Probable Cause

"Probable Cause" is information that would lead an objectively reasonable officer to believe that (1) a crime probably has been committed (or is about to be committed) and that (2) a particular suspect probably committed the crime. Carroll v. United States. Probable cause is a higher

level of certainty than reasonable suspicion. It is the level of knowledge required by the Fourth Amendment where it states "...no warrant shall issue but upon probable cause..."

Officers must establish probable cause to search *before* a judge can issue a search warrant. Though this may appear uncomplicated, probable cause is not a simple term to define. Chief Justice Rehnquist stated that "[a]rticulating precisely what 'reasonable suspicion' and 'probable cause' mean is not possible. They are commonsense, nontechnical conceptions that deal with 'the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act' [quoting Illinois v. Gates]." Ornelas v. United States.

For this course's purpose, probable cause is defined as a set of apparent facts that are sufficiently strong in themselves to lead a reasonable, prudent law enforcement officer to believe that a crime probably has been, is about to be, or is being committed, or that evidence of a crime is probably located at the place to be searched. The test of probable cause is not a philosophical concept existing in a vacuum. As Chief Justice Rehnquist stated, it is a nontechnical standard to be applied with common sense. There is no set formula for probable cause. Courts must determine its existence on the facts and circumstances of each individual case.

a. Aguilar test

Often, law enforcement officers have no personal knowledge of criminal activities and must rely on information passed to them from informants, victims, witnesses and co-conspirators. Rule 1101(d)(3) of the Federal Rules of Evidence provides that the Rules of Evidence (other than with respect to privileges) are inapplicable in warrant application proceedings. Rule 41(c) of the Federal Rules of Criminal Procedure states "[t]he finding of probable cause may be based upon hearsay evidence in whole or in part."

When an officer uses hearsay information, the reviewing court must assure itself that sufficient facts are present to establish the trustworthiness of the information. In Aguilar v. Texas, the Supreme Court set forth a two-pronged "Aguilar test" for determining the trustworthiness of hearsay information. The magistrate judge must have specific *facts* upon which to make an independent finding of probable cause and not the bare conclusions of an officer or informant. First, the requesting officer should present sufficient facts that will show the magistrate judge that the particular source, whose identity the government need not disclose, is credible, or worthy of belief. This first part of the Aguilar test is the "veracity" prong. Second, the officer should inform the magistrate judge of the underlying facts and circumstances that led the source to believe that items subject to seizure are where the source claims they are. This is the "basis of knowledge" prong. The affidavit must satisfy both prongs of the test in order to support a valid search warrant based on the Aguilar test.

The *Aguilar* Test

(1) **CREDIBILITY OF SOURCE**

and

(2) **BASIS OF KNOWLEDGE OF THE SOURCE**

An officer cannot merely state that the informant is reliable, credible, or trustworthy. The magistrate judge must have *facts*, not conclusions, upon which to base an independent finding that the third party is reliable. The affidavit should set forth the character, reputation or history of the third party as a truthful person.

Some classes of persons are presumed to be credible by the very nature of their status. These persons include:

- other law enforcement officers
- victims
- eyewitnesses to a crime
- partners-in-crime

Courts do not presume paid informants to be credible. The best way to establish reliability of a paid informant is with a proven track record. The affidavit should establish the length of time the officer has known the informant, the number of times this informant has given previous information, the number of times the information has been correct, the types of criminal activities involved, etc.

It will not always be possible to establish a track record for every informant and, of course, there has to be a first time for every informant. If the reliability of the informant cannot be established through a track record, the affiant should set forth the circumstances surrounding the information that will assure the magistrate judge of its trustworthiness. For example, a magistrate judge can find information reliable if it comes from an informant who admits to being a participant in a crime or otherwise makes a statement against his or her penal interests. When it is desirable to maintain the confidentiality of an informant, the affiant should use as much detail as possible about the informant's past record without disclosing the informant's identity. The affiant may also establish the reliability of the information by showing independent verification or corroboration of as much of the informant's information as possible.

Independent observations by law enforcement officers can provide support to otherwise questionable hearsay to show that the informant has provided the truth, establishing the veracity prong. As the Supreme Court stated, "a direct showing that some of the story has been verified as true lends credence to the remaining unverified portions of the story and so may raise it above Aguilar's threshold." Illinois v. Gates.

The four basic practices a law enforcement officer may use to establish the reliability of a confidential informant (one whom the law enforcement officer has promised anonymity) are:

- established track record of the informant
- corroboration of the information informant has provided
- information was verified through independent sources
- information provided meets a description of the suspect's known reputation

Not only must the affiant establish that the source of information is reliable, the affiant must set forth facts that demonstrate that the information was attained through personal observations. A source may not make a bare assertion or conclusion that evidence of a crime will be found in a certain location. The affidavit must explain the facts upon which that conclusion is based. Did the source see the contraband or other evidence? What exactly did the source see, hear, smell, or touch?

If the information in the affidavit is deficient in stating specifically how the informant obtained the information, a few courts have considered an alternative. If the informant's information is presented in such minute detail that the magistrate judge can conclude that the source could have obtained the information only through first-hand observation, then this "self-verifying" detail may establish the basis of knowledge prong. The detailed information must be of such a nature, however, that the magistrate judge can be satisfied that the information was obtained first-hand and is not based on idle rumor or irresponsible conjecture. Reliance on detail to fully satisfy the basis of the knowledge prong, due to the lack of firm judicial support in this area, is not recommended. The officer should make every effort to satisfy this prong of Aguilar by disclosing the manner in which the source received the information. The details then provide added assurance of reliable information.

b. the Gates test

The Gates test is more general, requiring that one make "...a balanced assessment of the relative weights of the various indicia of reliability" in determining probable cause. It does not require an absolute adherence to the Aguilar two-prong test. Illinois v. Gates.

Instead, the existence of probable cause is to be judged on the "totality of the circumstances" which give rise to a practical, "common sense" determination, based upon all the circumstances and facts of the case. However, officers should use the Aguilar standard where possible, since it is a clear and simple test of probable cause. Consider using the Gates "totality of circumstances" test only when unable to demonstrate Aguilar's two prongs (for instance, in the case of an anonymous informant).

4. Reasonable Certainty

Law enforcement officers are required to ensure that any items they seize during the execution of a search warrant are subject to seizure through that search warrant. The officers must be reasonably certain that seized items are supposed to be seized. Reasonable certainty is a standard of proof greater than probable cause. As for the premises that is subject to a search warrant, "[i]t is enough if the description is such that the officer with a search warrant can with reasonable effort ascertain and identify the place intended [underline added]." Steele v. United States. Arrest warrants should also contain sufficient information to allow an arresting officer to be reasonably certain that the subject of the arrest is the individual identified in the warrant.

5. Proof Beyond a Reasonable Doubt

Proof beyond a reasonable doubt is the standard of proof needed to support a criminal conviction. While there is no concise definition of this

standard, it is essentially proof that precludes any "reasonable" doubts as to guilt. Some judges have instructed juries that beyond a reasonable doubt equates to a moral certainty of guilt, and that there can be no reasonable doubt as to guilt.

F. THE TERRY FRISK

A "frisk" is a "limited search for weapons, generally of the outer clothing, but also of those areas which may be within a suspect's immediate control." Terry v. Ohio. Frisks are often done by law enforcement officers in connection with stops. The objective of a frisk is to discover weapons that may be utilized by the detainee to assault the officer or others. The scope of the frisk should be the minimum necessary to discover weapons and should be initially confined to a pat down of the person's outer clothing and containers within their immediate control. A frisk, by definition, is limited to seeking hard objects that could be dangerous to the law enforcement officer and is NOT to be used for the purpose of discovering evidence, contraband, or means of escape. The scope of the frisk is limited due to its nature of being a type of "search" within the meaning of the Fourth Amendment. Just as a "stop" is a seizure, a "frisk" is a search for which there must be an articulable reason. The purpose of a frisk is to protect an officer from an unexpected assault. Officers may only conduct frisks when there is reason to suspect that a person is BOTH armed and dangerous. The "reasonable suspicion" standard means that the officer must have specific and articulable facts giving rise to a belief that a person is armed and dangerous. It must be more than a subjective belief on the part of the officer.

FRISK FEATURES

Based on reasonable suspicion that the suspect is **armed and dangerous.**

Focus is to locate **weapons** that could be used to harm the officer.

Search consists of **patting the hands over the suspect's person** and the area under their immediate control.

If, during a frisk, an officer feels a hard object that he or she reasonably believes to be a weapon, the officer may then reach into that area of the suspect's clothing to retrieve it. If the item turns out to be evidence of a crime, it is admissible against the defendant because the officer was lawfully present when the evidence was found, i.e., the officer was looking for weapons, not evidence. If, for example, during a legal frisk, an officer feels a flat hard object and reasonably believes it could be a plastic "credit card knife," the item may be removed and inspected. If during this inspection to determine if the object is a weapon, a tab of LSD falls out, then the LSD tab is now in "plain view" and may be legally seized as evidence against the suspect.

A "weapon" need not be illegal to be seized and inspected during a valid frisk. In addition to an illegally possessed handgun, a seized weapon could be a pen, a cellular telephone, etc. - - anything that could be used as a weapon against the officer (to stab, strike, strangle, etc.).

It is not necessary for an officer to be certain that an individual is armed in order to do a frisk. The officer must only have a reasonable suspicion based upon specific and articulable facts. Some of the factors that can indicate that a person is armed and dangerous are:

- The **reputation or record** of the individual being detained.

For example, the suspect has a general reputation in the community for being armed, or the suspect has been charged or convicted for an armed offense within a reasonable period before the officer's stop.

- A **bulge in the suspect's clothing** which suggests the presence of a weapon.

- A **quick or furtive movement** by the suspect, or a movement into an area where a weapon may be concealed.

- The **demeanor** of the suspect. The belligerent or threatening demeanor of suspect is a factor in whether the suspect is armed and dangerous.

- The **type of the offense** being investigated.

Officers can develop reasonable suspicion that an individual is armed and dangerous from the nature of the crime itself or from other factors. For example, certain crimes are, by their nature, considered to involve the use of weapons or items that could be used as weapons (armed robbery, murder, terrorist acts, firearms violations, burglary, large scale drug deals, etc.). Therefore, anyone suspected of being involved in those crimes can also be presumed armed and dangerous. On the other hand, some crimes do not by their very nature involve the use of weapons (fraud, bribery, mere drug possession, tax evasion, etc.) and therefore there must be additional facts giving rise to a belief that a person is armed and dangerous before a frisk may be done.

Reasonable suspicion that a person is armed and dangerous is not a difficult legal standard to sustain. As the Court said in the Terry case:

> *The officer need not be absolutely certain that the individual is armed; the issue is whether a reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger....And in determining whether the officer acted reasonably in such circumstances, due weight must be given, not to his inchoate and unparticularized suspicion or "hunch," but to the specific reasonable inferences which he is entitled to draw from the facts in light of his experience.*

Officers should be aware that whenever a "Terry frisk" exceeds a mere pat down of the outer clothing, the courts could consider this fact in determining that the seizure ceased being a Terry stop and became an arrest. If this is the case, the court will require the officer to demonstrate that he or she had the probable cause necessary to justify the

(unintentional) arrest and search incident to that arrest. The greater intrusion a seizure causes, the greater the likelihood a court will find that seizure to be an arrest.

1. Plain Touch Doctrine

If, during a frisk, an officer feels something that he or she does not believe to be a weapon, but the incriminating nature of the object (such as drugs wrapped in particular ways, hypodermic needles, etc.) is immediately apparent, the officer may retrieve the object. Minnesota v. Dickerson. In order for the evidence seized to be admissible in court, it is essential that the illegality of the object be immediately apparent to the officer, without continued manipulation of the suspect's clothing.

A lawful frisk allows an officer to be lawfully "present" to touch the object. The object's "immediately apparent" criminal nature gives the officer probable cause to believe it is evidence of a crime. Under the "plain touch,"[3] doctrine the officer may then lawfully seize the evidence. This doctrine recognizes that touch can produce probable cause, just as observations, sounds, and smells may.

2. Frisking Vehicles

Just as an officer may frisk an individual for weapons based upon reasonable suspicion, if that individual is in a vehicle, the officer may also frisk that vehicle. The frisk of a vehicle is limited to the passenger compartment (i.e., those areas which may be reached from inside the vehicle) and includes any closed but unlocked containers. Therefore, with reasonable suspicion to frisk

> You Lawfully Frisk ONLY when you can **articulate a reason** to suspect that the person is armed and dangerous.

[3] This is related to the concept of "plain view" in that the officer must be lawfully present (engaged in a lawful frisk) and discover something that is "immediately apparent" (establish probable cause) to be evidence of a crime.

an individual, an officer may also frisk the vehicle in which the suspect was driving or riding, including the unlocked glove box or console. The officer may also frisk other closed but unlocked containers such as briefcases, duffle bags, etc. The rationale for including the vehicle in the frisk is that if the officer releases the person, he or she may re-enter the vehicle and the officer should know whether it contains any dangerous weapons. Michigan v. Long.

3. Frisking Containers

To date, the Supreme Court has not decided whether an officer can frisk a container carried by a person reasonably suspected of being armed and dangerous. However, every circuit court that has examined this issue has decided that officers with reasonable suspicion that a suspect is armed and dangerous can frisk containers within control of those suspects. If the officer is uncertain about whether he or she can frisk a container, consider that separating the person and their container during the stop can adequately protect officer safety. If an officer does frisk a container, a "crush and feel" technique for a soft-sided container is acceptable. If the container is hard-sided and unlocked, then the officer may open the container and frisk the contents for weapons.

4. Frisking Companions

When an officer stops a suspect who is accompanied by an unknown person, and the officer has reasonable suspicion that the suspect is armed and dangerous, under certain circumstances the officer may also frisk the unknown person.

For example, if officers stop a suspect in a restaurant whom they believe may be armed and dangerous, they may frisk the suspect but not all the other patrons of that establishment. Before officers may frisk a companion, they must be able to articulate why they think the companion may be armed and dangerous as well. This is a limited right and does not

include those people who may just happen to be nearby. Ybarra v. Illinois.

5. Frisking the Opposite Sex

Reasonableness dictates that it is preferable to have a person of the same sex frisk the suspect. However, this may not always be possible. Should it be necessary to frisk a member of the opposite sex, the officer should do as thorough a frisk as if the person were of the same sex. However, the frisking officer should always be sensitive to the degree of discomfort such a search engenders and maintain a professional decorum throughout.

6. Related "Terry Stop" Points on Vehicle Stops

Law enforcement officers face increased risk of injury during vehicle stops. For this reason, the Supreme Court has extended the authority of an officer engaged in this activity to increase officer safety. The Supreme Court has ruled a law enforcement officer conducting a lawful vehicle stop may order the driver out of the car without any further legal justification. Pennsylvania v. Mimms. In Maryland v. Wilson, the Supreme Court extended this authority by ruling law enforcement officers, conducting a lawful vehicle stop, may order a passenger out of the car without any further legal justification.

II. THE EXCLUSIONARY RULE

Evidence recovered in an unconstitutional manner, i.e., an unreasonable manner, is subject to the exclusionary rule. The Supreme Court created the exclusionary rule to discourage government officials from abusing constitutional rights. Before 1914, the admissibility of evidence in United States courts was not affected by the illegality through which it was obtained. Evidence that was relevant and otherwise competent, regardless of how the government obtained it, was admissible

in a prosecution in both federal and state courts. Courts were not interested in the means employed by law enforcement officers to obtain the evidence.

In the 1914 case of Weeks v. United States, the Supreme Court ruled that evidence obtained through an unreasonable search or seizure by federal officers could not be used in a prosecution in federal court against the person whose constitutional right had been violated (the person with standing to object). The Supreme Court reasoned that this "exclusionary rule" would deter federal officers from violating the constitutional provisions they had sworn to uphold by removing the incentive for engaging in unreasonable activity.

A. DEVELOPMENT OF THE RULE SINCE 1914

After 1914, the federal courts continued to admit unconstitutionally seized evidence in federal courts so long as federal officers were not involved with the unconstitutional search or seizure. This practice was known as the "silver platter doctrine" because state and local officers could turn over the fruits of their illegal searches and seizures to federal authorities for prosecution if the federal government was not involved in a constitutional offense.

In 1961, in Mapp v. Ohio, the U.S. Supreme Court, by means of the Due Process Clause of the Fourteenth Amendment, imposed the exclusionary rule of the Fourth Amendment on the states. Consequently, in order to be admissible in any court in the United States, evidence must meet minimum Fourth Amendment standards for lawful searches and seizures.

B. FRUIT OF THE POISONOUS TREE

In Silverthorne Lumber Company v. United States the Supreme Court established the "fruit of the poisonous tree" doctrine. This doctrine prohibits the use of illegally seized evidence to obtain still more evidence.

In Silverthorne, the prosecuting attorney realized that the government had obtained documents in an unconstitutional manner. He directed their return to the defendant. The prosecuting attorney, knowing that the defendant was in possession of these documents, then issued a subpoena for their production in court. The Supreme Court stated that if the government learns of evidence through unconstitutional means (the illegal search), this evidence cannot be used to discover yet more evidence (through the subpoena used to produce the documents). Further, the government is precluded from using illegally seized evidence as a basis for establishing leads to develop other evidence. Nardone v. United States.

C. EXCEPTIONS TO THE EXCLUSIONARY RULE

Not all illegal searches and seizures trigger the application of the exclusionary rule. Factors such as the ultimate use of the evidence and the relationship of the defendant to the evidence play roles in determining whether the exclusionary rule is applicable. Nonetheless, officers must realize that most searches and seizures *are* covered by the rule, and an officer should not attempt to evade the effect of the rule by seeking, in advance of the search, to fit it into one of the "exceptions."

1. Standing

Constitutional rights are personal rights. The only person that has a right to object to the introduction of the evidence seized is the person whose right was violated. Person "A" cannot demand that evidence should be excluded against him because it was seized in violation of Person "B's" constitutional right. Standing, i.e., the right to object, belongs to the "victim" of the unreasonable search or seizure.

The U.S. Supreme Court held that a person must have a reasonable expectation of privacy in the place searched to have standing to object to government intrusion in that area. Minnesota v. Carter. In Rakas v.

Illinois, a passenger complained about the admissibility of illegally seized evidence from the car in which she was riding. She did not own either the car or the evidence that was unreasonably seized. The Court held that she did not have standing to object to the unreasonable seizure. In Rawlings v. Kentucky, the Court found that a defendant did not have standing to object to an illegal search of his girlfriend's purse.

2. Independent Source

Unreasonably seized evidence does not become "sacred and inaccessible" to lawful discovery by other officers. Silverthorne Lumber Company v. United States. If a second group of officers recovers the same evidence, while acting lawfully and independently of the first group, then that evidence will be admissible. In order to be considered truly independent, the second group of officers should not have any knowledge of the violation committed by the offending group, or any knowledge of the evidence the offending group recovered.

3. Inevitable Discovery

Another exception recognized by the Court is the "inevitable discovery" of evidence. The unreasonable search or seizure of evidence by one officer will not bar the use of that evidence when other officers, acting independently and without knowledge of the wrongful acts of the first officer, are searching lawfully for the evidence. If they would have inevitably discovered the evidence in question had others not already discovered it through unreasonable acts, the doctrine may apply. Nix v. Williams.[4]

[4] An essential difference between the inevitable discovery doctrine and the independent source doctrine seems to be that the inevitable discovery doctrine is available only when the officers that have engaged in the unreasonable search/seizure have removed the evidence from the scene, preventing its lawful (and inevitable) discovery. Officers that unreasonably search for but do not remove the evidence leave it for discovery by other lawful, independent means. This evidence is subject to the independent source doctrine.

4. Good Faith Exception

The Supreme Court provided a "good faith" exception to the exclusionary rule in United States v. Leon and Massachusetts v. Sheppard. The Leon case involved a "facially valid search warrant" issued by a judge. The police found large amounts of illegal drugs in the search that followed. State appellate courts suppressed the illegal drugs after determining that no probable cause existed to support the search warrant.

The U.S. Supreme Court pointed out that the purpose of the exclusionary rule was to deter police misconduct. The rule's intent is not to punish the errors of judges or magistrates. The Court said it had no basis for believing that exclusion of evidence seized would have a significant effect on the issuing judge. When the officer's conduct is objectively reasonable in conducting a search with a search warrant, there is no police illegality and therefore nothing to deter. In cases such as these, the exclusionary rule does not apply even if the warrant is invalid.

Generally, the "good faith exception" is available only if officers conducted their search with a warrant.[5] Even then, the exception will not always be available. The Supreme Court listed several circumstances in which the good faith exception is inappropriate. First, if the affiant knowingly included false information in the affidavit or acted in reckless disregard of the truth, the good faith exception does not apply. Second, if the magistrate did not perform his or her function in a neutral and detached manner or was serving as a "rubber stamp" for the government, the officers cannot serve the warrant in good faith. Third, if the affidavit is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable" the good faith exception is unavailable to the officers. The requirement that the officer's good faith be objectively reasonable creates a standard external to the officer. The officer's own

[5] The Supreme Court has recognized that officers can rely on statutes in good faith to secure evidence, even if those statutes are later declared unconstitutional. See Illinois v. Krull, 480 U.S. 340 (1987).

good faith is immaterial unless it is reasonable to believe he was acting in accordance with the law. United States v. Leon.

In Arizona v. Evans the Supreme Court held that evidence discovered during a search incident to an arrest based on an erroneous computer record need not be suppressed. A court clerk failed to remove an arrest warrant from a computer database and a police officer reasonably relied (acted in good faith) on the existence and validity of the warrant. The search incident to an arrest based on that warrant resulted in the discovery of evidence (in this case, marijuana) that the government could introduce against the defendant.

5. Impeachment of Testimony

Evidence that is inadmissible in the government's case-in-chief may be admitted for the limited purpose of impeaching defendants if they testify in their own defense. For instance, if a law enforcement officer unreasonably seized narcotics that were in the possession of the defendant, the exclusionary rule would prohibit the government from testifying about (or otherwise proving) the existence of the drugs. However, if the defendant voluntarily took the witness stand and stated that he has never possessed narcotics, the government may impeach the defendant by introducing the illegally obtained evidence. Walder v. United States; United States v. Havens.

6. Grand Jury

The Supreme Court refused to allow a defendant to avoid answering questions before a grand jury despite the defendant's argument that the subpoena was based on an investigation that originated from an unreasonable search and seizure. The Court held that the necessity for ensuring the efficacy of the grand jury's investigative powers outweighed any possible deterrent effect. United States v. Calandra.

7. Foreign Searches

The Fourth Amendment does not apply to searches by foreign officers in foreign countries, whether the search conducted was legal or illegal by American standards or even by the standards in the country of the search. The Constitution places limitations on the actions of federal officers (and some state actions through the Fourteenth Amendment) but has no bearing on the activities of foreign nations or private individuals.

Nor does the Fourth Amendment apply to searches or seizures by United States law enforcement officers of property owned by a nonresident alien and located in a foreign country. The Supreme Court stated that no U.S. Magistrate Judge or U.S. District Court Judge has jurisdiction to issue a warrant to search outside this country. There is no indication that the Framers' understood the Amendment was to apply to United States activities directed against aliens in foreign territory or in international waters. United States v. Verdugo-Urquidez.

8. Other Exceptions

The Court has recognized other exceptions to the rule in recent years that are beyond the scope of this course. For example, the Court has said that evidence otherwise subject to the exclusionary rule can be admitted in certain civil cases (though not all), cases involving the deportation of illegal aliens, and parole violation hearings.

III. ARREST

A. ARREST AUTHORITY GENERALLY

In the federal system, the authority to make arrests varies from agency to agency. The scope of a federal officer's authority is established by statute. Each officer must know the extent of the authority granted by these statutes. For some, authority and jurisdiction are limited to certain

geographical areas, while for others, authority is limited to certain subject matter. For example, a United States Park Police officer can enforce almost all federal laws, but only within specific physical boundaries. On the other hand, an Internal Revenue Service agent may generally enforce only internal revenue laws, but may do so anywhere within the jurisdiction of the United States.

Therefore, just because a crime, federal or otherwise, has been committed, does not signify that a federal officer can make a lawful arrest. Officers may do so only if they have the statutory authority and jurisdiction to arrest for that specific crime. There are three types of authority to take action in arrest-type situations:

1) **Federal Statutory Authority**: That authority granted to federal officers by acts of Congress.

2) **State Peace Officer Authority**: This is power granted by some states to some federal officers, authorizing them to enforce state law.

3) **Citizens' Arrest Authority**: This is a power, granted in some states, permitting citizens who witness a felony to arrest for that crime.

B. STATUS OF FEDERAL LAW ENFORCEMENT OFFICERS RESPONDING TO STATE CRIMES

In the absence of federal arrest authority, if a federal officer makes an arrest, the law of the state in which the arrest takes place is controlling. Where states do not confer peace officer status on federal officers, an arrest made by federal officers outside their statutory federal arrest authority will generally be treated as a citizen's arrest.

As an alternative to a citizen's arrest or an arrest under state peace officer status, the Terry doctrine allows a limited seizure for investigative matters. If an offense has been committed but the offense is not one

within an officer's authority and/or jurisdiction, the officer should arrange to immediately turn the person over to authorities with jurisdiction over the crime.

The Federal Good Samaritan statute may also allow federal criminal investigators to, without fear of civil liability:

take reasonable action, including the use of force, to:

1) protect an individual in the presence of the officer from a crime of violence;

2) provide immediate assistance to an individual who has suffered or who is threatened with bodily harm; or

3) prevent the escape of any individual whom the officer reasonably believes to have committed in the presence of the officer a crime of violence.

Omnibus Consolidation and Emergency Supplemental Appropriations Act, Pub. L. No. 105-277, 112 Stats. 2681 (1998), at Div. A, Sec. 101(h), Title VI, Sec. 627.

This protection is granted to federal officers whose duties primarily are:

(I) the investigation, apprehension, or detention of individuals suspected or convicted of offenses against the criminal laws of the United States, or

(II) the protection of officials of the United States against threats to personal safety; and

(III) are sufficiently rigorous that employment opportunities should be limited to young and physically vigorous individuals, as determined by the Director [of the Office of Personnel Management] *considering the recommendations of the employing agency.*

It also applies to the United States Park Police, United States Secret Service, the Bureau of Prisons, and military detention officers. Title 5 U.S.C. § 8401(17).

An officer should take action only in accordance with instructions issued by an agency. If an officer detains a person under the Federal Good Samaritan law, he or she should turn the person over to authorities with jurisdiction over the crime of violence. If the seizure of a person continues in an officer's custody, then the person must be charged with a valid federal violation, arrested under state peace officer status, arrested as a citizen, or released.

Arresting for a federal violation, or turning a dangerous individual over to local authorities for arrest, enables the federal officer to remain within the scope of federal authority, and affords the highest level of civil liability protection. When a federal officer arrests under color of state law, his or her legal exposure to liability increases. Making a citizen's arrest requires that the officer make no mistake about probable cause for the arrest, or the officer may be liable for false arrest.

C. ARRESTS BASED ON OUTSTANDING ARREST WARRANTS

In the course of an officer's duty, he or she may discover the existence of an arrest warrant for a person with whom they are in contact. Officers typically discover this through an identity check through the Treasury Enforcement Communications System (TECS) or National Crime Information Center (NCIC), and commonly refer to this as a "hit." How to handle such "hits" is discussed below:

1. Outstanding Federal Warrant

Authority to arrest is limited to an officer's statutory arrest authority. The arresting officer should verify that the warrant is still valid and that the arrested person is the person specified on the warrant. The

officer need not have the warrant in possession at the time of the arrest, but upon request, is required to show the warrant to the suspect as soon as possible. If the officer does not have the warrant at the time of the arrest, he or she should inform the suspect of the offense charged and of the fact that a warrant has been issued. Rule 4(d)(3), Federal Rules of Criminal Procedure. If a federal officer detains a person for an outstanding federal warrant concerning a crime outside the scope of the officer's statutory authority, he or she should continue to detain the individual until an officer with the proper authority can make the arrest.

2. Outstanding State Warrants

No federal statute authorizes federal law enforcement officers to arrest for outstanding state warrants. Such arrests are made either as a state peace officer or as a citizen, depending on the law of the state in which the arrest is made.

Discoveries of persons with pending state arrest warrants may result in federal offenses. Title 18 U.S.C. § 1073 prohibits persons from traveling in interstate or foreign commerce with the intent either (1) to avoid prosecution (or custody or confinement after conviction) for a felony under the laws of the place from which the fugitive flees, or (2) to avoid giving testimony in any felony criminal proceeding, or (3) to avoid service of (or contempt proceedings for alleged disobedience of) lawful process requiring attendance.

The preferred practice is to detain an individual for a reasonable period until state or local police officers can affect an arrest. United States v. Burkeen 350 F.2d 261 (6th Cir. 1965). Federal officers should contact local police officers to determine if the requesting state wants the suspect detained. Such a request may give the federal officer additional authority to comply with this request.

D. CROSSING THE LINE FROM A "STOP" TO AN "ARREST"

The question of when an investigative stop becomes an arrest has generated a great amount of judicial discussion. The determination of whether an arrest has occurred is not dependent on whether the officer has formally arrested the person or whether the seizure would be considered an arrest under state law. Dunaway v. New York. Rather, a stop may become an arrest (for which probable cause rather than reasonable suspicion is required) when a detention is "in important respects indistinguishable from a traditional arrest." Dunaway.

Although there is no precise test for determining when a detention has evolved into an arrest, removing a person a significant distance from the place of the original stop, or detaining a person longer than necessary to investigate suspicions, may turn an investigative detention into an arrest. Hayes v. Florida; Florida v. Royer; United States v. Sharpe. Also, the use of force can be a significant factor in determining whether a suspect was placed under arrest or just stopped by a law enforcement officer.

E. ARRESTS MADE WITHOUT PROBABLE CAUSE AND/OR WITHOUT AUTHORITY

When and if a person is arrested without probable cause, or without legal authority, a court may determine the arrest was illegal. Consequences of an illegal arrest include:

1) suppression of evidence obtained in or during search incident to the arrest;

2) suppression of statements made by the defendant during the arrest;

3) lawsuits against the arresting officer for a violation of the defendant's constitutional rights or for false arrest under state law.

Note further that the officer may be held personally liable for such actions.

Miranda warnings have no impact on the validity of an arrest. If an officer makes an arrest with probable cause, failure to give Miranda warnings will not invalidate the arrest. On the other hand, if the officer makes an arrest without probable cause, or without lawful authority, Miranda warnings will not make the arrest lawful. Dunaway v. New York.

IV. METHODS OF ARREST

A. OBTAINING ARREST WARRANTS

The validity of all arrests depends on the existence of probable cause to make an arrest. In general, if an officer has probable cause, the officer may make an arrest without a valid warrant even though (1) there was ample time to obtain an arrest warrant and the officer failed to do so, or (2) the officer obtained a warrant but it turned out to be defective. In other words, the propriety of an arrest is judged by whether or not there was probable cause, and not by the existence or nonexistence (or the validity or invalidity) of a warrant. Naturally, the arresting officer should always be mindful of whether such an arrest is within the scope of the officer's statutory authority.

Despite the fact that officers may arrest on probable cause without a warrant, courts prefer that officers obtain a warrant when possible. The Supreme Court reasoned that obtaining a warrant permits a "neutral and detached" magistrate judge to consider the issue of probable cause instead of leaving that issue to an officer in the field. Obtaining a warrant is also beneficial to the officer, in that it provides a degree of protection from possible civil suits, and it allows the "good faith exception" to the exclusionary rule to operate.

In the federal system an arrest warrant may be issued on the basis of:

1) A Criminal Complaint--see Rule 3, Federal Rules of Criminal Procedure.

Law enforcement officers may obtain arrest warrants by filing a sworn complaint before a magistrate judge. The probable cause statement may be based upon hearsay evidence, either in whole or in part. (Rule 4, Fed. R. Crim. P.). Principally, the federal criminal complaint consists of the following:

- ✓ a writing of the essential facts making up the offense being charged,
- ✓ clear language of facts sufficient to establish probable cause that an offense was committed, and who committed it,
- ✓ the signature of the accusing officer, under oath in front of the magistrate judge or other judicial official,
- ✓ allegations that the offense charged occurred, in whole or in part, within the judicial district where the warrant is being sought,
- ✓ a statement that the individual filing the complaint is an authorized law enforcement officer. Only sworn officers may file criminal complaints.

2) An Indictment by a Grand Jury.

3) An Information by the United States Attorney.

The rules governing the issuance of indictments by grand juries and informations by United States Attorneys are covered in the course

titled "Federal Court Procedures." Suffice it to say, there are many similarities with complaints, in that all must set forth facts sufficient to show probable cause to believe a named individual committed a specific crime within a certain judicial district.

4) An Order of the Court.

5) A Federal Violation Notice.

6) A Probation Violation Petition.

A good practice is to obtain an arrest warrant when practicable. However, a warrant by a court "commands" an officer to arrest the named individual should the officer come across that individual.[6] Thus, it could be premature to secure a warrant when further investigation (especially undercover work) is needed, and could possibly upset the case.

B. ALTERNATIVES TO ARREST

The authority and the probable cause to make an arrest do not have to result in an arrest. There are alternatives to arrest that may be more appropriate under some circumstances. In addition, some agencies, judicial districts, and prosecutor's offices place restrictions on arrests. Consider the following alternatives to arrest, especially when the offense is a minor one and/or there exists little reason to take the person into custody (e.g., the suspect cannot or will not flee):

☒ Release with a warning--advising the person that a law has been violated and that should he persist or do it again, legal

[6] This is not an absolute dictate. There can exist circumstances in which an officer can lawfully choose not to affect an arrest, despite the fact that an outstanding arrest warrant exists. For instance, if the officer discovers the subject of an outstanding arrest warrant, surrounded by several bodyguards, the officer may choose to affect the arrest at a different time. United States v. Wilson, 342 F.2d 782 (2nd Cir. 1965); Carlo v. United States, 286 F.2d 841 (2nd Cir. 1961); United States v. Watson, 423 U.S. 411 (1976)(cited in Justice Marshall's dissenting opinion).

action can be taken.

- ☒ Issuance of a citation or ticket—an appropriate action for a petty offense and those where no jail time will result. It commands the person to either pay a fine or appear before the court on a certain date. Failure to do either can result in the issuance of a summons or an arrest warrant.

- ☒ Issuance of a summons--this is a court order commanding a defendant to appear before the court and answer a charge. If the defendant ignores the summons, the Court will issue an arrest warrant. It is appropriate to use a summons in cases where there is little chance that the defendant will flee to avoid prosecution (e.g. misdemeanors, white collar crime cases, and cases involving well-known, public persons).

- ☒ Issuance of a subpoena--this is a court order commanding a witness to appear before the court and testify. Failure to appear is contempt of court and an arrest warrant may issue. A subpoena is most commonly and appropriately used to require a witness, not a defendant, to appear at a grand jury hearing or a trial.

C. LIMITATIONS ON FEDERAL ARREST WARRANTS

Any authorized officer may execute a federal arrest warrant at any time within the jurisdiction of the United States, its possessions, and its territories. It does not matter how much time has elapsed since the issuance of the warrant to the time the arrest occurred. Once the arrest is made, the arresting officer must comply with Rule 5(a), Federal Rules of Criminal Procedure, by bringing the arrested person before a magistrate judge.

D. ARREST WARRANTS

1. Arrest in Defendant's Home

Officers must first lawfully gain entry into a suspect's home to look for them before making the arrest. This is a search within the meaning of the Fourth Amendment. Therefore, unless exigent circumstances exist or officers make their entry with consent, an arrest warrant must have been issued.

The courts have held that the right to seize the body of the defendant (through the use of an arrest warrant) carries with it the right to enter into the defendant's property to specifically look for the defendant (a search). The rationale is that the entry into the property is a lesser intrusion of an individual's Fourth Amendment rights than is the arrest and, therefore, the greater permits the lesser. However, in order to enter into the defendant's home with an arrest warrant, officers must have a reasonable belief that the defendant is there. Payton v. New York. The arrest warrant itself may include the address of the defendant. No judicial determination of the defendant's dwelling is necessary at the time the warrant is secured. If the officers serving the arrest warrant reasonably believe that another location is the defendant's dwelling, the arrest warrant is still valid, i.e., the officers do not have to obtain another warrant with the amended address. United States v. Lauter, 57 F.3d 212 (2d Cir. 1995).

2. Arrest in Third-Party Premises

An arrest warrant alone will not authorize entry into the home or office of a third person for the purpose of looking for and arresting a suspect, unless exigent circumstances exist or consent of the third person is obtained. An arrest of a suspect in a third person's home generally does not violate any of the suspect's rights. It does violate, however, the constitutional rights of the third person to be secure from unreasonable

searches and seizures. Therefore, should an officer unlawfully enter a third person's premises to arrest a suspect and find evidence or contraband linking the third party with a crime, such evidence will be suppressed as to the third party. The best practice is to obtain a warrant to search for the suspect on the third party's premises. Steagald v. United States.

Officers should also be aware that obtaining a search warrant for a third party's premises also brings the time limitation of search warrants into play, limiting execution of the search warrant to the period between 6 a.m. and 10 p.m., unless other times are authorized by the issuing magistrate judge. Also, recognize that an unlawful warrantless entry (search) into a third person's home leaves an officer open to possible civil suit for violating that third person's constitutional rights.[7]

3. Protective Sweeps (The Buie Doctrine)

Officers do not need any particular suspicion to look into the areas immediately adjoining the room where the subject was arrested, as long as those areas are large enough to conceal a potential attacker. The Court in Maryland v. Buie held that this examination of adjacent areas is appropriate as a routine precautionary matter when performed incident to an arrest. The Court in Buie said "...as an incident to the arrest the officers could as a precautionary matter and without probable cause or reasonable suspicion, look in closets and other spaces immediately adjoining the place of arrest from which an attack could be immediately launched [underline added]."

In order to extend their examination beyond the area immediately adjoining the arrest scene, officers must establish reasonable suspicion

[7] It does not appear from the case law that the arrested person has standing to complain about the intrusion into a third party's home for the purpose of making the arrest, unless he or she is an "overnight guest" as described in Minnesota v. Olsen, 495 U.S. 91 (1990). United States v. Clifford, 664 F.2d 1090 (8th Cir. 1981); United States v. Underwood, 717 F.2d 482 (9th Cir. 1983) 465 U.S. 1036 cert. denied (1984).

that a potentially dangerous person is in that area. This is known as a "protective sweep."[8] The officers must be able to articulate the specific facts that gave rise to their suspicion. For instance, to "sweep" the upstairs portion of a premises, officers would have to justify their intrusion with facts such as information that the person arrested committed the crime with an unlocated accomplice, or hear the sound of someone attempting to flee or a shotgun being loaded. Maryland v. Buie.

The Supreme Court in Buie emphasized that:

> *...such a protective sweep, aimed at protecting the arresting officers, if justified by the circumstances, is nevertheless not a full search of the premises, but may extend only to a cursory inspection of those spaces where a person may be found. The sweep lasts no longer than is necessary to dispel the reasonable suspicion of danger and in any event no longer that it takes to complete the arrest and depart the premises.*

In any event, the search must be for *persons*, and can last *no longer than it would take* to remove the arrested person from the premises.

While courts are not overly concerned with the application of a "protective sweep" during most search warrants (the officers are there to search in the first instance), an arrest warrant gives officers both the authority to arrest the subject, and the limited authority to search for the subject within his or her home. Once the officers have lawfully entered the subject's home, located and arrested the subject, and performed a search incident to the arrest (see below), then they are no longer justified in remaining on the premises. However, concerns about officer safety could justify a "protective sweep."

"Protective sweeps" must be limited to a search of the premises for people who could pose a danger to the officers at an arrest scene. It is

[8] Sometimes known as a Buie sweep.

narrowly confined to a cursory visual examination of those places from which an attack reasonably could be launched. This means spaces large enough to hide a human being, e.g. a closet, but not a shoebox. The officer's level of suspicion determines how far away from the arrest scene he or she may lawfully sweep. Maryland v. Buie.

E. EXIGENT CIRCUMSTANCES AND ENTRY TO MAKE AN ARREST

If exigent circumstances exist, an officer needs neither an arrest warrant, nor a search warrant, to enter a private residence, business, etc. Exigent circumstances include public safety emergencies, the imminent destruction of evidence, and hot pursuit.

Under the "hot pursuit" doctrine, an officer without a warrant may lawfully enter a private premises in order to follow a suspect and effect an arrest when:

1) The officer first encounters the suspect in public, but the suspect flees into an area of expected privacy (a home, etc.);

2) There exists probable cause to arrest the suspect for a "serious" crime (which most likely means that the officer must be entering to execute an arrest for a felony; see footnotes 11 and 12, Welsh v. Wisconsin);

3) The officer has a continuous knowledge, within reason, of the suspect's whereabouts, (i.e. the officer must be in the suspect's presence, but does not have to have the suspect in view);

4) The officer needs to act with speed; and

5) The officer has probable cause to believe that the suspect is in the premises that he or she has entered under "hot pursuit." Welsh v. Wisconsin.

Note that "hot pursuit" need not just be on the public ways but can also occur as the result of the subject's moving just a few feet from public exposure into a protected premise. For example, a suspect standing on the threshold of the doorway of her home was "in public." An officer saw her there, had probable cause to arrest her for a felony, and then ran after her into her house and arrested her in the vestibule. The Court found that the officer lawfully entered the residence in "hot pursuit." Evidence seized as a result of the entry was admissible, since a warrant was not required for the entry. United States v. Santana.

F. WARRANTLESS ENTRY BY CONSENT

An officer may make a warrantless entry into a private premises if the officer has first obtained a valid consent from a person capable of giving that consent. This means that the person granting consent must reasonably appear to have the legal ability to consent, and must exercise dominion or control over the premises into which consent to search is being granted, and must voluntarily give such consent. Illinois v. Rodriguez; Bumper v. North Carolina.

The person must be of an adequate age to understand the implications of granting consent and must have a degree of control over the property. For example, a motel clerk may not consent to a police entry into a room currently leased by a motel guest, as the guest is the one who exercises the control. Stoner v. California. Likewise, a child may not consent to police entry into the parental home if the child is too young to understand the issues involved in granting consent.

G. ARRESTS WITHOUT WARRANTS

1. Felonies

At common law, a peace officer was authorized to arrest a person for a felony without first obtaining an arrest warrant whenever he or she had "reasonable grounds to believe" that a felony had been committed and that the person being arrested committed the crime. The terms, "reasonable grounds to believe" and "probable cause" are substantially the same standard. Draper v. United States.. This common law standard is applicable today.

There is no difference in the standard of probable cause whether an officer seeks an arrest warrant or decides to make a public arrest. In other words, the probable cause standard is the same for both warrantless arrests and arrests with a warrant. Also, the arresting officer does not need to have personal knowledge of all the facts giving rise to probable cause. The collective knowledge and information of all officers can be used. The arresting officer must know, however, that facts are in existence that establish probable cause before the officer can act.

2. Misdemeanors

The law with respect to warrantless arrests for misdemeanors is quite different. A warrant is required except when the misdemeanor occurs in the presence of the arresting officer. The arresting officer is entitled to use all senses in determining whether a misdemeanor occurred in his or her presence. Carroll v. United States. Thomas v. United States, 412 F.2d 1095 (D.C. Cir. 1969).

Officers may make arrests without arrest warrants in a public place:

- ✶ if the crime is a misdemeanor, and was committed in the presence of the arresting officer; or

✶ if the crime is a felony.

Note that suspects have no constitutional right to be arrested earlier than the law enforcement officer chooses. Officers may not be forced to halt an investigation before they have enough evidence to support a conviction simply because they have enough evidence to support probable cause.[9]

If an arrest is made without a warrant, it will be necessary to file a criminal complaint (assuming no indictment or information has been filed) at the time the defendant is taken to court for the initial appearance. The better practice is to obtain an arrest warrant in advance when possible. By doing so, the officer may then rely on the "good faith" rule supporting arrest warrants, and will have diminished any possible civil liability. Arizona v. Evans.

H. USE OF FORCE TO EXECUTE ARREST AND SEARCH WARRANTS

Deeply rooted in Anglo-American law is the requirement that, before forcing entry to execute a warrant, law enforcement officers must announce their identity and purpose and afford the occupant the opportunity to open the door voluntarily. This longstanding common law concept has been codified for federal law purposes in Section 3109 of Title 18 which provides:

> *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.*

[9] Not all courts follow this rationale. Some courts have held that once an arrest warrant has been issued, the warrant compels the officer to act on that warrant. Benjamin v. United States, 554 F. Supp. 82 (E.D.N.Y. 1982). See also 18 U.S.C. § 755 "Officer Permitting Escape."

The purposes of this so-called "knock and announce" rule are to reduce the potential for violence against both the officers and the occupants of the premises, to guard against needless destruction of private property, and to show respect for individual privacy. United States v. Bustamante-Gamez. This respect for privacy is part of the constitutional protection of the home. Wilson v. Arkansas.

This law applies to all entries under color of law, either to search or to arrest, with or without a warrant. The officer must announce both his or her *authority* and *purpose* before using force to enter a dwelling. Merely stating "Federal agents" is insufficient. The officers must also state their purpose, e.g., "Federal agents with a search warrant," and demand entry.

The courts have given a broad construction to this statute. For instance, courts interpret the word "break" to include opening an unlocked door or using a passkey. Law enforcement officers may use force once they have been refused admittance. The term "refused admittance" means that an officer must wait a reasonable length of time before forcing entry. There is no set minimum time. The occupant must be given reasonable time to open the door voluntarily. This length of time will depend on the facts of the case, taking into account such factors as the size of the dwelling, the destructible nature of the evidence, the time of day, and the physical condition of the occupant.[10]

Only after officers have been refused or denied admittance, may they make a "forced" entry into the premises. A refusal or denial of admittance may take several forms:

* a verbal refusal such as "go away;"

[10] Some courts have articulated a five-second standard. "However, when officers have waited more than 5 seconds, the courts have generally held that there was no violation of § 3109." United States v. Jones, 133 F.3d 358 (5th Cir.), cert. Denied, 523 U.S. 1144 (1998). This is not to be considered absolute law, but a guideline.

* the sounds of flight, i.e. the occupant attempting to escape; such sounds include footsteps running in the opposite direction, a window being opened, a fire escape ladder being lowered, etc.;

* gunfire, such as a shotgun blast through the door;

* the sounds of evidence being destroyed. In a drug case, for example, the officer hears a flushing toilet;

* silence after waiting a reasonable period of time, the officer hears nothing; in other words, no response at all to the demand for entry.

Under certain circumstances, officers can lawfully force entry without complying with the "knock and announce" requirement. The Supreme Court permits a "no-knock" entry when law enforcement officers can establish reasonable suspicion that compliance with § 3109 would be dangerous, futile, or would result in the loss of the evidence. Richards v. Wisconsin; United States v. Ramirez. Examples include:

➔ When to do so would increase the level of danger to the officers or to other innocent persons. Wilson v. Arkansas.

For example, officers had been warned that occupants were to be considered armed and dangerous, and the apartment manager informed the officers that she had advised the occupants that the police were looking for them. United States v. Ramirez.

➔ When the officer has reasonable suspicion that "knocking & announcing" will cause the occupants to destroy evidence or escape. Richards v. Wisconsin.

- ➔ When officers determine that the best course of action to follow in gaining admittance is to utilize a ruse or trickery. Entry by use of deception, wholly without application of force, is not governed by § 3109. United States v. Beale. For example, it would be lawful for an officer serving a warrant to gain entry by posing as a mail carrier in order to avoid the dangers of forcing an entry. Most circuits have approved entry by ruse or deception to execute a warrant. Such entries, however, must be effected without any force whatsoever. The danger of discovery before or during entry that may require the use of force could violate the statute. Officers should consider all their options before resorting to this type of entry, e.g., when confronted by a fortified door in a case involving easily destructible evidence.

- ➔ When officers are in "hot pursuit" of an individual who enters into a private premises, the officers do not have to comply with the "knock and announce" statute, because the person being chased knows who the law enforcement officers are and what they want. United States v. Flores, 540 F.2d 432 (9th Cir. 1976).

In interpreting the term "house," some circuits have limited the application of § 3109 to dwellings. Other circuits, however, have extended the meaning of "house" to cover such structures as offices, smokehouses, and barns. Officers therefore should be familiar with the rule in their area of operation when contemplating the entry of such buildings.

If it is necessary to physically force entry it is incumbent upon the officers to ensure that the premises are in a secure condition when they leave. Failure to do so could result in liability for loss of items from the premises and/or damage to the premises that results from leaving the property unsecured. It is legal to break down doors, etc., in order to gain entry, if that degree of force is necessary. United States v. Ramirez. However, if that force is used, officers must take measures to minimize damage to the property. The best practice is to use only the minimum

amount of force necessary to safely gain admittance under the circumstances.

V. USE OF FORCE IN MAKING ARRESTS

A. NECESSARY FORCE

"Force" is defined as the display of physical power as is reasonably calculated or likely to induce fear of physical harm to those opposing it. Deadly force is that force which, from the manner used, is calculated or likely to produce death or serious bodily injury. Law enforcement officers are entitled to use that force which an ordinary, prudent, and intelligent person, with the same knowledge of the situation as the law enforcement officer, would deem to be necessary and appropriate.

The generally accepted standard for police use of force is that an officer may use whatever degree of force is reasonably necessary to assure compliance with all lawful commands. The indiscriminate use of force is illegal and prohibited. The use of unreasonable force may result in an illegal arrest, and in the suppression of evidence obtained because of that arrest. It may also result in a civil suit being filed against the officer, as well as criminal charges.

Use of force by law enforcement officers in the performance of their duties has been traditionally limited to four categories:

1) Necessary to overcome resistance to the officer's lawful commands,

2) Necessary to detain a suspect and to effect an arrest,

3) Necessary to maintain custody and prevent escape,

4) Necessary to protect the officer or other person(s).

In every seizure situation, officers should use only that reasonable amount of force necessary to take control and overcome resistance in order to effect a lawful seizure. As the Court stated in Graham v. Conner, "[d]etermining whether the force used to effect a particular seizure is 'reasonable' under the Fourth Amendment requires a careful balancing of 'the nature and quality of the intrusion on the individual's Fourth Amendment interests' (quoting United States v. Place) against the countervailing governmental interests at stake. Our Fourth Amendment jurisprudence has long recognized that the right to make an arrest or investigatory stop necessarily carries with it the right to use some degree of physical coercion or threat thereof to effect it."

In determining how much force may be, or should be used, the officer should consider such factors as:

- The nature of the offense for which the suspect is being arrested, e.g., felony or misdemeanor.
- The number of participants involved.
- The size, age, and condition of the participants.
- The record and/or reputation of the suspect for violence.
- The use of alcohol or drugs by the suspect.
- The suspect's mental or psychiatric history.
- The presence of innocent bystanders.
- The availability of other, less violent or non-lethal weapons, such as tear gas, batons, nets, tasers, etc.

In Graham v. Connor, the Supreme Court discussed the standard reviewing courts should use to determine if the use of force was reasonable. In the decision, the Court stated:

> *Based on a totality of circumstances, ...the reasonableness of a particular use of force must be judged from the perspective of a reasonable officer on the scene, rather than the 20/20 vision of hindsight...As in other Fourth Amendment contexts, however, the reasonableness inquiry in an excessive force case is an objective one: the question is whether the officers' actions are objectively reasonable in light of the facts and circumstances confronting them, without regard to underlying intent or motivation.*

The FLETC has developed a USE OF FORCE MODEL to create a standardized training approach to the utilization of force by federal officers. The MODEL allows students to visualize various situational confrontations and select the appropriate and lawful amount of force called for under the circumstances. The MODEL will be presented by Physical Techniques Division, but will be referenced throughout your training at the FLETC.

B. USE OF DEADLY FORCE

In Tennessee v. Garner, the United States Supreme Court delineated the circumstances in which law enforcement officers are authorized to use deadly force. The Court held that an officer is justified in using such force when:

1) The officer is threatened with a weapon or the life of another is so endangered, or

2) The officer has probable cause to believe that the suspect has committed a crime which involved the infliction or threatened infliction of serious bodily harm, and deadly force is necessary to prevent the offender's escape, and

3) Where feasible, the officer gives a warning regarding the possible use of deadly force prior to its use. This does not include the firing of a warning shot.

C. THE DEPARTMENT OF JUSTICE/TREASURY FIREARMS POLICY

The Department of Treasury's policy is not as broad as this Supreme Court interpretation. Regarding the use of deadly force, it is the policy of the Department of the Treasury, and of the Federal Law Enforcement Training Center, that:

> *A firearm may be discharged only as a last resort when the agent or police officer reasonably believes that there is imminent danger of loss of life or serious bodily injury to himself/herself or to another person.*

Or, to put it in more simply, an officer should only use their weapon to protect their own life or the life of someone else. Imminent danger is the appearance of threatened and impending injury as would put a reasonable and prudent person to their instant defense. There are three elements in deciding whether jeopardy exists are:

Present Opportunity--current conditions exist which would allow injury.

Physical Capability--the subject has the apparent ability, i.e. the subject is armed.

Manifested Intent--by word or deed the subject has expressed the desire to injure.

As this policy is more restrictive than the legal guidelines established by the Supreme Court, it is possible that officers could use deadly force within constitutional principles and still violate agency

policy. All officers should be aware of the policy established by their agency for the use of deadly force. Most agencies have policies similar to the FLETC.

While in a training status at the FLETC, all students, regardless of their parent agency, are bound by the FLETC policy.

D. FIREARMS GUIDELINES

The intent when discharging a firearm should be to render the person at whom the shot is fired incapable of continuing the activity prompting the officer to shoot. Therefore, the use of warning shots is usually prohibited by policy.

Firing at a moving vehicle with the intent of rendering it incapable of operation poses a formidable danger to innocent parties. The possibility of a ricochet is greatly increased when the target is a car body or a spinning tire. Officers must use the utmost caution when considering such action, and such action may be governed by agency policy.

VI. SEARCHES WITH A SEARCH WARRANT

Officers should not routinely rely on the exceptions to the warrant requirement to make searches. Whenever possible, a valid, judicially approved search warrant should be obtained before officers intrude on an individual's expectation of privacy. The Fourth Amendment sets out the prerequisites for a valid search warrant ("...and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."). The procedures for obtaining a search warrant are set forth in Rule 41 of the Federal Rules of Criminal Procedure. See 28 CFR § 60.2 for a list of federal officers who are authorized to apply for and receive a search warrant.

A. AUTHORITY TO ISSUE SEARCH WARRANTS

Rule 41(a) states:

> *Upon the request of a federal law enforcement officer or an attorney for the government, a search warrant authorized by this rule may be issued (1) by a federal magistrate judge, or a state court of record within the federal district, for a search of property or for a person within the district and (2) by a federal magistrate judge for a search of property or for a person either within or outside the district if the property or person is within the district when the warrant is sought but might move outside the district before the warrant is executed and (3) in an investigation of domestic terrorism or international terrorism, by a Federal magistrate judge in any district in which activities related to the terrorism may have occurred, for a search of property or for a person within or outside the district.*

A "state court of record" is a court in which a record of judicial proceedings is made and one which has the power to fine or imprison for contempt. This can vary from state to state depending on state laws. Although it is legal, a federal officer should only seek a warrant from a state judge as a last resort.

A federal magistrate judge will usually require the affiant to appear personally with a written affidavit. Under certain circumstances, the magistrate judge may issue a warrant based upon sworn testimony communicated by telephone or other appropriate means, including facsimile transmission. Fed.R.Crim.P. 41 (c)(2)(A). This part of the rule states "[I]f the circumstances make it reasonable to dispense, in whole or in part, with a written affidavit, a federal magistrate judge may issue a warrant based upon sworn testimony communicated by telephone or other appropriate means, including facsimile transmission." This is often referred to as a telephonic search warrant, which is discussed below.

The term "Federal magistrate" as used in this rule includes United States magistrate judges and federal judges. The judicial officer who will commonly issue search warrants will be the United States magistrate judge. Federal law does not permit state court judges to issue federal telephonic search warrants.

The judicial officer must be neutral and detached and can issue a valid warrant only within their jurisdiction or district. A justice of the United States Supreme Court has the authority to issue a warrant for property anywhere in United States jurisdiction, but a district court judge can only issue a valid warrant within his or her district.

It is possible to secure a search warrant from any federal judge. Federal Rule of Criminal Procedure 54(c) provides that Federal District Court Judges, Court of Appeals Judges and Supreme Court Justices are authorized to issue search warrants, though their performance in this function would be extremely rare.

B. ANTICIPATORY SEARCH WARRANT

Anticipatory search warrants are warrants that become effective upon the happening of a future event (such as the delivery of contraband). While there is no rule permitting the issuance of this kind of warrant, every circuit but the Eleventh has specifically approved their use and the Eleventh Circuit has assented to their use. United States v. Loy, 191 F.3d 360 (3rd Cir. 1999); cert. denied 529 U.S. 1023 (2000). Probable cause must support a valid anticipatory warrant and must clearly identify the circumstances that activate the warrant.

C. PROPERTY AND PERSONS SUBJECT TO SEIZURE WITH A WARRANT

Search warrants may only be issued for certain types of evidence. Officers must know what kind of evidence they are seeking with a search

warrant. Rule 41(b) provides for the issuance of a warrant to seize: (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; (3) property designed or intended for use or which is or has been used as the means of committing a criminal offense; or (4) a person for whose arrest there is probable cause. Any person or property can be the subject of a valid search warrant if it falls into at least one of these categories.

D. AFFIDAVIT FOR A SEARCH WARRANT

The Fourth Amendment requires that "no Warrant shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The sworn affidavit is the vehicle for meeting this constitutional requirement. In order to obtain a search warrant, the officer must file, in accordance with Rule 41(c), an affidavit before the magistrate judge. The officer seeking the search warrant must complete the affidavit and ascertain that it meets the constitutional requirements of probable cause, that the affidavit is sworn to before a judge, and that the place to be searched and the persons or things to be seized are particularly described. Failure to meet these requirements will result in the magistrate judge either refusing to issue the warrant or issuing an invalid warrant. Though hearsay evidence may be considered and can be included in the affidavit, the issuing judge will require the presence of the affiant (unless a telephonic warrant is being sought).

1. Descriptions

The Fourth Amendment requires a particular description of the place (be it a house, building, automobile, suitcase, or person) to be searched and the persons or things to be seized. The purpose of the particularity requirement is to limit the scope of a search and insure that no greater invasion of privacy occurs than is necessary. If a warrant

describes the wrong place or things, or is vague or overly broad, then reviewing courts may suppress all evidence seized under that warrant.

a. place to be searched

Before officers enter a place subject to a search warrant, they must be reasonably certain that they are entering the proper location. Steele v. United States. The precise location and area to be searched must be described in sufficient detail so that any officer executing the warrant can, with reasonable effort, ascertain the place intended to be searched. Minor errors in a description should not affect the validity of the warrant if the description, on the whole, enables the officer to identify the proper place with reasonable certainty.

Officers conducting searches in rural areas should include directions showing how to locate the target premises, including a precise physical description of the premises. In addition, a map or photograph that would aid identification may be attached. Directions should begin from some fixed and identifiable point and end with the specific place to be searched. These factors help assure that the premises has been identified with reasonable certainty.

In an urban area, directions may not be necessary (but are always useful). The affiant should pay particular attention to obtaining the correct house or apartment number, the owner's name, and the street address. In any situation, a detailed physical description should be given which clearly distinguishes the place to be searched. For example, in situations where one unit in a multiple unit apartment building is to be searched, officers must exercise care to describe the particular unit to be searched to preclude unreasonable mistakes by officers executing the warrant.

In describing a dwelling house to be searched, officers should not overly restrict their search by describing just the "house." Officers can use

the term "premises" to extend their coverage to include the curtilage area of the home. Officers can also insure coverage of the entire premises by specifying "any outbuildings and appurtenances thereto."

b. persons or things to be seized

The persons or things to be seized under the warrant must be specifically described so that the searching officers should exercise as little discretion as possible as to what can be seized. Officers should describe persons by name, if known (including any aliases), and by physical description. The detail in which the sought items must be described will depend on the nature of the items themselves. If the items are traditional contraband, such as heroin or counterfeit currency, then a general description of the illegal items will usually suffice. This is because the likelihood that officers will seize lawfully possessed property with this general description is remote.

In the case of noncontraband property, the more ordinary an item is the greater the need for the warrant description to be particularized. For example, a stolen firearm should be described by make, model, serial number, barrel length, type of finish, etc., if possible. Also, such items as books and records need to be specifically described as much as possible by account, type, manner of keeping, relationship to the particular criminal activity, etc.

If a reviewing court finds that the description is overly broad, giving too much discretion to the searching officers, the court will declare the warrant invalid. The essence of "particularity" needed for a warrant is: the items subject to seizure must be described to the extent that they can be distinguished from similar items on the premises that are not subject to seizure. Failure to do so may result in a "general search," which is prohibited by the Constitution.

Officers may not always know exactly what evidence they might find during a search. After officers have described in as much detail as

possible all those items which they have probable cause to believe are located where they intend to search, the courts have authorized the inclusion of a general description such as "together with the means and instruments and all other property constituting evidence of the crime." This general description is intended to cover under the warrant those items not specifically listed which relate *only* to the crime for which the particular warrant is issued.

2. Probable Cause

A magistrate judge initially determines the existence of probable cause. The officer seeking the warrant must articulate facts so that the magistrate judge can make an independent determination that probable cause exists. Only those facts actually communicated to the magistrate judge under oath can be used to support a warrant. If a warrant is issued, but subsequently ruled to be invalid for a lack of probable cause, an officer may not save the warrant, or a search under its authority, by later bringing forward facts that the officer had known previously but failed to communicate to the magistrate judge. Whitley v. Warden.

a. personal knowledge - reasonable officer standard

The ideal situation for the establishment of probable cause is one in which the officer presents facts from personal knowledge. Courts will evaluate the facts in light of how they appear, not just to the ordinary person, but to the reasonable law enforcement officer. The court will consider the officer's specialized knowledge and experience.

The officer must be careful to recite only facts in the affidavit. Mere suspicion, hunches, or conclusions by the officer are not sufficient for the magistrate judge to determine the existence of probable cause. The magistrate judge must make the conclusions and reasonable inferences from the facts presented in the affidavit. Without the articulated facts

from which the magistrate judge can make an independent determination of probable cause, no valid warrant can be issued.

b. hearsay and the Aguilar test

See above discussion regarding the Aguilar test and the government's use of hearsay evidence in the development of probable cause for search warrants.

c. corroboration and other facts

Corroboration of facts by law enforcement officers in establishing probable cause can be a very important step in the process. The reviewing court still can consider defective information that does not meet the Aguilar test in determining probable cause if there is sufficient corroboration by officers. Officers need to independently corroborate defective hearsay information to establish probable cause. Therefore, the officer should include in the affidavit any information in the officer's possession that will help the magistrate judge find probable cause. For example, if the subject of the proposed search has a criminal record or a bad reputation, the officer should provide this information to the magistrate judge.

Probable cause is the result of a consideration of the "totality of the circumstances." A number of facts that may seem innocent when considered separately, but become suspicious when collectively considered can create probable cause. Former Chief Justice Warren Burger stated "[p]robable cause is the sum total of layers of information and the synthesis of what the police have heard, what they know, and what they observe as trained officers." The only limitation placed on probable cause is that evidence, information, or observations obtained by officers through violations of an individual's constitutional rights may not be used to establish probable cause for a warrant against that person.

d. timeliness

Probable cause must exist at the time the judge issues the warrant and at the time of the search. A warrant cannot be based on "stale information," or information that is no longer dependable because of its age. United States v. Lamorie, 100 F.3d 547 (8th Cir. 1996). In addition to the requirements for probable cause, there must be sufficient facts presented in the affidavit so that the magistrate judge can conclude that the items to be searched for are presently located or will be located in the place to be searched.

The issues regarding timeliness have nothing to do with when the officer received the information. Fresh information indicates the items to be searched for have recently been or will be in the place to be searched at the time of the proposed search. How fresh the information must be depends on the circumstances of each case considering the nature of the evidence sought, the volume and turnover rate, plans of the violators as established by the probable cause, etc. As with the other areas of probable cause, corroboration and surveillance by officers can aid in establishing timeliness and maintaining the life of the probable cause.

e. place to be searched

Probable cause to search must establish a link (or nexus) between the place to be searched and the items to be seized. For example, to search the residence of a suspect in a narcotics investigation, probable cause that a suspect is dealing in heroin is not sufficient to justify a premises warrant. The requesting officer must demonstrate probable cause that the heroin to be seized is located at that residence.

f. containers to be searched

Generally, containers that conceal their contents provide a reasonable expectation of privacy because of the fact that personal papers

and effects may be kept within. United States v. Chadwick. Without an exception to the warrant requirement of the Fourth Amendment, officers must obtain a search warrant to search a container that has a reasonable expectation of privacy.

g. dog alerts

Law enforcement officers have used specially trained dogs as valuable investigative tools in tracking fugitives and in the detection of explosives and narcotics. Most courts agree that the Fourth Amendment does not control the government's use of such dogs, as long as the dog and its handler are lawfully present during their activities. The dog merely smells the air surrounding a container. Typically, an individual has no reasonable expectation of privacy in the air surrounding containers. Therefore, no Fourth Amendment "search" is involved.

An alert by a trained dog provides probable cause for a warrant, provided the government laid the proper foundation in the affidavit for the warrant. To lay the proper foundation, the dog and its handler must be qualified as experts in detecting the particular odor of the substance to be seized.

3. Affidavits - Miscellaneous

There is no special language or form necessary to insure a good affidavit for a search warrant. The courts have held that they read affidavits for their substance and not for their grammar. However, officers should present their information professionally, in a logical and complete order. Officers should write their affidavits clearly, avoiding vagueness, unclear references, misused pronouns, and the passive voice. Officers should clearly reference attachments and additional affidavits or statements from others. The affidavit submitted to the magistrate judge must be sworn to and signed in the presence of the magistrate judge. Officers should not sign any document that requires such signature to be

witnessed by the magistrate judge until in the presence of the magistrate judge.

Sometimes, informants who provide information forming the basis of the probable cause give false information to the officers. In such a case, the officer-affiant is swearing to what was told to the officer, i.e., hearsay. If the officer does not lie or act in reckless disregard for the truth, i.e., commit perjury, and is acting in good faith on the information, then no adverse action will lie against the officer and the warrant will stand. If the officer-affiant falsely swears to an affidavit or acts in reckless disregard for the truth, a court may suppress the resulting evidence discovered unless enough independent (untainted) information remains so that the magistrate judge can still find probable cause.

E. WARRANTS ISSUED ON ORAL TESTIMONY (TELEPHONIC SEARCH WARRANTS)

Fed.R.Crim.P. 41(c)(2) provides that a federal search warrant may issue upon oral testimony or other appropriate means (e.g., electronic devices). This is allowed when circumstances make it reasonable to dispense with a written affidavit. Typically, the officer makes the application for a warrant based on oral testimony over the telephone (telephonic search warrants). The officer must prepare a document known as a "duplicate original warrant" and read it verbatim and under oath to the magistrate judge. The magistrate judge enters the officer's information verbatim on a document known as the "original warrant." In the process, the magistrate judge may modify the warrant. Once satisfied that the circumstances are reasonable to dispense with a written affidavit and that probable cause exists, the magistrate judge orders the issuance of a warrant by directing the officer to sign the magistrate judge's name on the duplicate original warrant.

Occasionally, situations confront law enforcement officers in which they do not have time to obtain a warrant in the traditional manner due to

the impending destruction or removal of evidence. However, if they have time to attempt to secure a telephonic search warrant before the removal or destruction becomes imminent, the officers should attempt to do so. Failure to attempt to secure a "telephonic search warrant," if the opportunity was available, may be considered in an unfavorable manner by a reviewing court.

F. EXECUTION OF THE SEARCH WARRANT

1. Authority to Execute Federal Search Warrants

Rule 41(c)(1) provides: "[T]he warrant shall be directed to a civil officer of the United States authorized to enforce or assist in enforcing any law thereof or to a person so authorized by the President of the United States."

Section 3105 of Title 18 further 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."

SEARCH WARRANT QUESTIONS

- proper authority to issue SW?
- premises described with particularity?
- proper authority to serve SW?
- items described w/particularity?
- probable cause stated in application?
- telephonic SW when necessary?
- 10 day limit for execution?
- 6:00 a.m. to 10:00 entry period?
- 18 U.S.C. § 3109 compliance?
- copy of SW provided?
- inventory/receipt?

The courts hold that other law enforcement officers may accompany an authorized officer named (individually or by a class) in the warrant even if the issuing magistrate has not designated them in the warrant. For example, a warrant specifying service by "any special agent of the U.S. Fish and Wildlife Service" must be executed by at least one special agent of Fish and Wildlife. However, other officers (e.g., Customs officers, local police officers, etc.) may accompany this special

agent. Anyone lawfully participating in the warrant execution may lawfully seize evidence.

Courts have permitted the use of phrases such as "to any special agent of the Bureau of Alcohol, Tobacco, and Firearms," or "to Special Agent John Jones of the U.S. Secret Service." Limiting the warrant to one officer, e.g., "to Special Agent Janet Jones, U.S. Secret Service" should be avoided as that officer must be present at the execution of the warrant and her absence may render the execution of the warrant invalid.

2. Time Limits

Officers should serve search warrants in the daytime, which Rule 41(h) defines as 6:00 a.m. to 10:00 p.m. according to local time. A search that begins during these hours may extend past 10:00 p.m., if such extension is reasonably necessary to complete the search. Rule 41(c)(1) provides that "[t]he warrant shall be served in the daytime, unless the issuing authority, by appropriate provision in the warrant, and for reasonable cause shown, authorizes its execution at times other than daytime."

Rule 41(c)(1) also states that officers should conduct the search within a specified period not to exceed 10 days. If, for some reason, the officers do not execute the warrant within the specified period, the warrant is no longer valid. If the officers desire another warrant, they must resubmit the factual basis for probable cause to the magistrate judge. The magistrate judge has no authority to extend the period beyond the original 10 days.

3. Searches, Seizures, and Scope of the Warrant

Once the officers have gained entry to the premises and secured the area to be searched, the search for the items specifically described in the warrant should commence. When officers exceed the limits of their

warrant by searching areas not covered by the warrant, searching for items not specified in the warrant, or remaining on the premises after having an opportunity to reasonably complete the search, their intrusion is considered unreasonable. Evidence obtained through these actions will be suppressed.

a. areas not covered by the warrant

The search warrant restricts the authority of the officers to search only those places wherein the items described in the warrant could be concealed. If a warrant authorizes the search for a stolen adult bicycle, officers may not search in dresser drawers, the kitchen breadbox, or the bathroom medicine cabinet.

If the warrant for the premises is properly drawn, it will authorize a search of all containers and personal property that could contain the item sought. Most circuits include the resident-suspect's vehicles found on the curtilage if they could conceal the items sought. These courts treat the automobile as if it were a container found at the premises. Officers cannot search the suspect's car parked off the premises under the premises warrant. However, other reasons may justify the search, e.g., consent or independent probable cause. Social visitors' property, to include their vehicle, are not subject to the authority of the search warrant. The best course of conduct to follow, if the officer has probable cause that an occupant's automobile contains evidence, is to include the automobile in the search warrant application.

b. seizure of items not particularly described in the warrant

Generally, officers may seize only those items particularly described in the warrant. Limited exceptions to this rule exist, however. Where the description section of the warrant contains language such as "and all property that constitutes evidence of the offense," those items found during the course of the search that constitute means and instruments, fruits, or evidence of the offense for which the warrant is

issued may be seized although not specifically described in the warrant. The items searched or seized must appear to have some logical relationship or "nexus" to the purpose of the search. For example, in conducting a search for marijuana in a suspected drug dealer's apartment, if officers find residue of marijuana, a quantity of plastic bags, and a set of scales, the officers may examine and seize all the items. The residue is subject to seizure because it is specifically listed in the warrant. The plastic bags and scales are subject to seizure because they are the means and instruments of the offense of dealing in marijuana.

c. remaining on the premises

When officers find the last item specified in the warrant or have exhausted all reasonable efforts to uncover specified items, then their authority to be on the premises under the search warrant is extinguished. Officers who remain on the premises for an unreasonable period become trespassers.

4. Plain View

The plain view doctrine is an acknowledgment by the courts that a law enforcement officer lawfully engaged in the ordinary course of duties is not required to wear blinders to that which is observed. When an officer has a legal right to be where he or she is and observes items that the officer immediately believes to be of an apparent incriminating nature, the courts allow those items to be seized without a warrant. Horton v. California. The three necessary elements for a lawful plain view seizure are:

(1) The officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed;

(2) the officer must have a lawful right to access the item; **and**

(3) It must be immediately apparent that the item is of an incriminating nature

a. constitutionally present

Officers must be justified in being where they are at the time they make their plain view observation. If the officers are not in a place where they have a constitutional right to be, a reviewing court will then suppress their observations or any evidence seized. Officers may gain lawful presence by executing a lawful arrest warrant, search incident to an arrest, service of a lawful search warrant, consent, etc.

Officers may legally walk up to an individual's front door to obtain directions, seek the whereabouts of an individual, conduct an interview, or even to request to use the bathroom. Nevertheless, in determining whether officers are legally on the premises, the courts place a heavy burden on the government to show that the entry was not a subterfuge to avoid the warrant requirement of the Fourth Amendment. If the court finds that the officer designed his or her actions to allow them to search without obtaining a warrant, then it may suppress any observations or seizures.

There is a difference between a seizure justified by plain view and an observation based on open view (which is not to be confused with "open fields" discussed above in section discussing curtilage). A plain view seizure of evidence is justified when an officer is constitutionally intruding on a person's reasonable expectation of privacy (through consent, a warrant, etc.). For example, when officers are lawfully in a suspect's home to execute a search warrant for counterfeit currency and discover cocaine, they are justified in seizing the cocaine under the plain view doctrine. The officers have violated no further expectation of privacy. An open view observation is simply one that an officer makes from a location he or she has a lawful right to be (without intruding on the suspect's privacy, i.e., a public street corner). However, this does not

imply that the officer can retrieve the evidence that he or she has lawfully observed. For instance, while standing on a public sidewalk, an officer looks in the direction of the suspect's home. If she observes an item that is obviously evidence of criminal activity, such as a marijuana plant, this observation creates probable cause but does not create a legal right to retrieve the plant on the spot.

b. lawful access

In order to lawfully retrieve the item the officer has observed, he or she must have lawful access to the thing. Consider the following: officers make a lawful observation from the neighboring property into the back yard of a suspect's home and observe marijuana plants. Absent other information, this observation alone will not authorize the officers to enter the suspect's property to seize the plants. This open view observation provides probable cause for an arrest of the suspect or the issuance of a search warrant but does not authorize a warrantless entry of premises to search without a warrant. Probable cause itself is never enough to justify a warrantless search. Some exception must also be present.

c. apparent incriminating nature

The officer making a seizure under the plain view doctrine must have probable cause to believe, without further investigation, that the item in plain view is evidence. Texas v. Brown. For example, if officers go to the home of a known convicted felon for an interview, are admitted to the premises, and see a pistol lying on a table during the interview, they may seize the pistol because it is evidence of the crime of possession of a weapon by a convicted felon that is immediately apparent to them. On the other hand, if they are conducting an interview of a witness to a crime and observe a purse they reasonably suspect is stolen, the officers may not pick it up for the purpose of determining ownership without consent. It is not immediately apparent that the purse is evidence of criminal activity.

5. Search, Detention, and Arrest of Persons on the Premises

The issuance of a search warrant for a premises does not give officers the authority to search or arrest those persons found on the premises. The person's body may be subject to search if the requesting officer made a proper request in the application for a search warrant. Officers may frisk (a limited search for weapons) a person they reasonably suspect is armed and dangerous. Ybarra v. Illinois. If the officers conduct a lawful arrest, they may search that person pursuant to that arrest.[11]

The degree of invasion by the government into an individual's expectation of privacy may not exceed the scope of the warrant (other than through the recognized exceptions). If officers want to search individuals found at the scene, they should obtain a warrant in advance. Of course, they will have to provide probable cause that the items they seek will be located on the person's body at the time of the search.

Personal articles carried by persons on the premises are not necessarily considered part of the premises. Therefore, they are not subject to the warrant. The most important aspect in determining if an item is covered by a premises warrant is the reason why the item is at the premises. Courts inquire into the degree of reasonable expectation of privacy that a certain person retains on the searched premises. People do not surrender their expectation of privacy in their person or possessions because they happen to be on the premises subject to a search warrant. The courts consider whether the person has a special relationship to the

[11]Probable cause to search a particular person for items listed in a premises warrant may arise due to that person's behavior, such as opening a desk drawer and quickly stuffing items into a pocket. If this occurs, it is unclear whether the law enforcement officers may search the person based on the premises search warrant. Some courts have held that the Ybarra decision authorizes a search of that person, based on probable cause. White v. United States, 512 A.2d 283 (D.C.App. 1986). Others have held that the officers must secure an additional search warrant (or a telephonic search warrant) for the items. Because this is an area that is unresolved by the law, seeking a telephonic search warrant would appear to be the most effective manner in dealing with this situation.

premises and whether probable cause for the issuance of the search warrant reasonably comprehended the personal property searched. For example, if officers arrive at a premises to search for illegal drugs and find a cosmetics salesperson on the premises with a sample case and a purse, the search warrant does not justify a search of these possessions. On the other hand, if a container on the premises belongs to a co-conspirator, several possibilities exist that may justify a search: consent; search incident to arrest; telephonic search warrant; or under the authority of the premises warrant. Officers are not expected to confirm ownership of items found unattended at the premises subject to a search warrant. They may search these items under the authority of the premises search warrant (provided these containers could contain the evidence sought under the warrant).

Officers conducting a lawful search under a warrant have authority to ensure that they can conduct the search without forcible interference. Officers may take reasonable and necessary measures to protect the safety of themselves and persons and property under their control during their search. If an officer can articulate a reasonable suspicion that a particular person may be armed and dangerous, the officer may conduct a Terry frisk of the individual. Search warrants, by themselves, do not authorize frisks. However, in deciding whether a person is armed and dangerous, the officer may consider the reasons authorizing the search warrant to justify a frisk. For instance, a search warrant issued to seize a large quantity of narcotics entails a degree of suspicion that persons found at the premises may be armed and dangerous.

Officers may detain a resident for a reasonable length of time without searching or arresting the person while they conduct a search of that residence in cases involving contraband. In Michigan v. Summers, the resident was leaving as the officers approached. They required him to stay, and later arrested him after finding contraband. However, the Summers doctrine only applies if the resident is on or about the premises. While the Supreme Court did not determine whether this rationale should apply to the service of any kind of search warrant, it appears likely that

the Summers doctrine is applicable to any kind of case.[12] Officers may not "pick up" the resident and bring him to the search scene if the resident is not at the premises.

In controlling the environment at the premises subject to a search warrant, officers have, then, various legal tools at their disposal. Officers may conduct a Terry frisks if they have reason to suspect that an individual is armed and dangerous. Officers may detain occupants of the premises searched under the Summers doctrine. If the officers discover evidence linking an occupant to the criminal activity, they may arrest the occupant and search them incident to that arrest. Officers may also choose to remove any visitors from the premises during the search.

6. Service of the Copy of the Warrant

The officers executing a search warrant must provide the residents of the premises with a copy of the search warrant (but not the affidavit) before leaving the premises. Officers are not required to present a copy to the residents immediately upon entry into the premises (except in the 9th Circuit, United States v. Gantt, 194 F.3d 987 (9th Cir. 1999)). If no one is present during the search, Rule 41(d) requires the officers to leave a copy of the search warrant in a conspicuous place so that the occupant of the premises may find it. If the officers do not seize any property, they are only required to leave a copy of the warrant with the person or at the premises searched.

7. Inventory and Return of the Warrant

Officers must account for all property taken from the premises during the execution of a search warrant. Property taken pursuant to the authority of the search warrant must be listed on the inventory found on the reverse side of the search warrant (please see example in "Additional

[12] At footnote 20 in its opinion, the Supreme Court stated "[w]e do not decide whether the same result would be justified if the search warrant merely authorized a search for evidence." Michigan v. Summers.

Resources" at the end of this book). Officers must also account for items seized under the plain view doctrine.

The officers must make the inventory in the presence of the applicant for the warrant and the person from whose premises the property was taken if the person is present and available. If the person from whose premises the property was taken is not available, the inventory must be made in the presence of at least one credible witness and verified by the officer. Rule 41(d) requires officers to leave a copy of the inventory with the residents (or in a conspicuous place).

> Rule 41(d)- The officer taking property under the warrant shall give to the person from whom or from whose premises the property was taken a copy of the warrant and a receipt for the property taken or shall leave the copy and receipt at the place from which the property was taken. The return shall be made promptly and shall be accompanied by a written inventory of any property taken. The inventory shall be made in the presence of the applicant for the warrant and the person from whose possession or premises the property was taken, if they are present, or in the presence of at least one credible person other than the applicant for the warrant or the person from whose possession or premises the property was taken, and shall be verified by the officer. The federal magistrate judge shall upon request deliver a copy of the inventory to the person from whom or from whose premises the property was taken and to the applicant for the warrant.

The search warrant designates a federal magistrate judge to whom the officers must make a prompt return. The federal magistrate judge shall deliver, upon request, a copy of the inventory to the person from whom the property was taken and to the applicant for the warrant. Although a prompt return is required by the rule, a failure to make a prompt return will not invalidate the search warrant or the items seized since this is held to be only an administrative procedure after the search.

8. Civil Lawsuits

An officer may be subject to a civil lawsuit because of his or her illegal actions. There is no specific statute under which a federal officer may be sued. However, case law established in Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics provides the aggrieved party a cause of action. The Legal Division covers this area of the law extensively in other courses such as Officer Liability.

VII. SEARCHES WITHOUT WARRANTS (PROBABLE CAUSE REQUIRED)

Courts have a strong preference that law enforcement officers secure search warrants before they conduct searches. However, this is not always possible or necessary. The Supreme Court has authorized various exceptions to the Fourth Amendment's warrant and probable cause requirements. Sometimes officers are confronted with a situation where an immediate search is necessary to prevent the loss or destruction of evidence but they have insufficient time to obtain a search warrant. Courts have approved the following searches as an exception to the warrant requirement where the officers can establish that the circumstances were exigent, i.e., so urgent that immediate action was required. Both the exigent circumstance and the probable cause must exist at the time of the search. Exigent circumstances by themselves, just as probable cause standing alone, will not justify a warrantless search.

While there remains a strong preference for search warrants supported by probable cause, the Supreme Court has never held that the Fourth Amendment always demands a warrant (or even probable cause—see below) for searches to be "reasonable" within the meaning of that amendment. Presented in this section are exceptions to the warrant requirement the Supreme Court originally granted because of the need for expediency. The plain view doctrine has already been presented. The other four warrant exceptions (probable cause still needed) follow.

A. SEARCHES OF VEHICLES, VESSELS, AND AIRCRAFT - THE CARROLL DOCTRINE

The "mobile conveyance" exception[13] to the Fourth Amendment's warrant requirement authorizes the search of a mobile conveyance if probable cause exists to believe it is carrying items subject to seizure (contraband, means and instruments of a crime, etc.). Conveyances typically include automobiles, trucks, airplanes, boats, and common carriers. In such situations, it is not practical to seek a search warrant before stopping and searching the conveyance. The original rationale for this warrantless search is that the conveyance and its cargo could be hidden, destroyed or removed from the court's jurisdiction before officers could secure a search warrant. Carroll v. United States. The Supreme Court now only requires that a law enforcement officer demonstrate that the conveyance is mobile, that probable cause exists to conduct a search, and that the mobile conveyance is located in an area that the officer has a right to access (a warrant or some other exception is needed to enter upon curtilage or into a garage to conduct a search of a mobile conveyance located there) to approve a warrantless search under the mobile conveyance exception. Mobile conveyance searches are justified even if law enforcement officers had time to secure a search warrant. United States v. Johns; Pennsylvania v. Labron; Maryland v. Dyson.

Courts often refer to this exception as the "Carroll Doctrine." In Carroll v. United States, the Supreme Court stated that a vehicle, for which probable cause exists to believe contains items subject to seizure, may be stopped and searched without a warrant if it is potentially mobile or in an exposed condition. The Supreme Court also noted that mobile conveyances have a reduced expectation privacy as they are subject to pervasive regulation. In such a case, there is a "fleeting opportunity on the open highway" to obtain the evidence and procuring a warrant is impractical.

[13] Also known as a Carroll search or the automobile exception.

Once the requirements for a Carroll search have been met, the warrantless search may be as thorough as one a magistrate judge could authorize with a warrant. A Carroll search may involve any area of the vehicle that is capable of containing the evidence sought, including all containers and packages (locked or unlocked). The object of the search defines the scope of the search. For example, probable cause to believe that illegal aliens are being transported in a car will not justify a warrantless search of the ashtray but would allow the officers to look in the trunk.

Mobile Conveyance Exception

Probable Cause to Search
+
Mobile Conveyance

However, if officers have probable cause to believe that evidence of a crime exists in a specific container, and have probable cause that the container is located in a mobile conveyance, that conveyance (if found in public) may be searched for the container. If the container is found, it may be opened and searched without a warrant. If the probable cause is limited to the container, then it may not support a general search of the vehicle but only a search for that container. California v. Acevedo.

The Supreme Court has extended the permissible period in which officers may search a vehicle under the mobility exception. If there is probable cause to search a vehicle at the moment the seizure occurs (e.g., at the scene of the stop or arrest of the driver), the officers can either conduct a search at that place or remove the vehicle to a better, more convenient, or safer location and search it there. This is true even though the officer could, after taking possession of the vehicle, hold it and obtain a valid search warrant. United States v. Johns. The probable cause to believe that the vehicle contains items subject to seizure is not lessened by being moved by the officers. Nor is the mobile conveyance exception limited by the fact that the officers chose to conduct their search of the vehicle at a later time.

The courts will view all the circumstances surrounding a warrantless search of a vehicle to determine whether there was mobility or potential mobility. Where a vehicle is immobile, for example, it is set upon concrete blocks without its wheels, a search cannot be based on the mobile conveyance exception.

B. DESTRUCTION OF EVIDENCE

An exigent circumstance that justifies a warrantless search is one where officers reasonably believe that a removal or destruction of evidence is *imminent* and there is not time to secure a search warrant. Cupp v. Murphy. Schmerber v. California. This exception has been applied where officers on surveillance overheard a conversation in the next room that led them to believe that heroin had been cut and packed there and was about to be removed. The court found the officers' subsequent entry and seizure of the heroin reasonable. The officers must provide probable cause that evidence is located in the area intruded upon and is about to be removed or destroyed. The courts have held that a warrantless search is not justified merely because there would be a delay or an inconvenience to the officers if they were required to obtain a search warrant.

Recall that Rule 41(c)(2) of the Federal Rules of Criminal Procedure provides for a search warrant based on oral testimony such as communicated by telephone or facsimile (fax) machine from officers in the field to a magistrate judge. This is commonly called a "telephonic search warrant" and is discussed above. This procedure may drastically reduce the time it takes to obtain a search warrant. The effect could be, therefore, that some situations formerly considered *exigent* due to the practical considerations of the time it would take to physically

> Rule 41(c)(2)(A) **General Rule**. If the circumstances make it reasonable to dispense, in whole or in part, with a written affidavit, a Federal magistrate judge may issue a warrant based upon sworn testimony communicated by telephone or other appropriate means, including facsimile transmission.

procure a search warrant are no longer considered urgent because a warrant can be obtained over the telephone in a relatively short period.

The destruction of evidence exception to the warrant requirement has been used successfully to justify a protective sweep-type search where officers *knew* that an accomplice was in the house, that the accomplice was likely to have witnessed the arrest, and that evidence could have easily been destroyed. Note that a search is not justified by the simple possibility that other persons or suspects could be in a residence nor is a search justified by the single fact that the evidence sought is of a type that can be easily destroyed. There must be specific, articulable facts that establish probable cause to believe that evidence is presently being destroyed or is in imminent peril of being destroyed.

The courts have also approved warrantless searches of persons where delay would make it impossible to obtain the evidence. For example, The Supreme Court permitted officers to obtain a blood sample from a drunk-driving suspect that was involved in an accident without a warrant because the delay to obtain a warrant would result in a loss of the evidence of the amount of alcohol in the suspect's blood. Schmerber v. California. In addition, courts have allowed officers to seize and search clothing or take scrapings from a suspect's fingernails where a delay would result in an opportunity for the suspect to remove or destroy the evidence before officers could obtain a search warrant. Cupp v. Murphy.

C. HOT PURSUIT

The "hot pursuit" exception was covered above. By way of reminder, a valid hot pursuit exception to the search warrant requirement exists when:

1) The officer first encounters the suspect in public, but the suspect flees into a private premises;

2) There exists probable cause to arrest the suspect for a "serious" crime (which most likely means that the officer must be entering to execute an arrest for a felony; see footnotes 11 and 12, Welsh v. Wisconsin)[14];

3) The officer has a continuous knowledge, within reason, of the suspect's whereabouts, (i.e. the officer must be in the suspect's presence, but does not have to have the suspect in view);

4) The officer needs to act with speed; and

5) The officer has probable cause to believe that the suspect is in the premises that he or she has entered under "hot pursuit." Welsh v. Wisconsin.

Recall that the officers do not have to obtain a search warrant before entering the protected area and searching for the suspect or weapons that may constitute a danger to the officers. Warden v. Hayden. Any evidence, whether contraband, fruits of the crime, etc., that are uncovered during a "hot pursuit" can be lawfully seized if the officers meet the requirements of the plain view doctrine (the officers are lawfully present by meeting the hot pursuit requirements, have a right to access the item, and the item seized is immediately apparent to be evidence of a crime).

---

[14] Those critical footnotes are: n11 "Our decision in Payton, allowing warrantless home arrests upon a showing of probable cause and exigent circumstances, was also expressly limited to felony arrests. See, e. g., 445 U.S., at 574, 602. Because we conclude that, in the circumstances presented by this case, there were no exigent circumstances sufficient to justify a warrantless home entry, we have no occasion to consider whether the Fourth Amendment may impose an absolute ban on warrantless home arrests for certain minor offenses.

n12 "Even the dissenters in Payton, although believing that warrantless home arrests are not prohibited by the Fourth Amendment, recognized the importance of the felony limitation on such arrests. See id., at 616-617 (WHITE, J., joined by BURGER, C. J., and REHNQUIST, J., dissenting) ('The felony requirement guards against abusive or arbitrary enforcement and ensures that invasions of the home occur only in case of the most serious crimes')."

D. EMERGENCY SCENE

There are many occasions when the police receive a call to a burglary, robbery, shooting, injury, fire or explosion that is occurring inside a premises. Police and firefighters do not have time to obtain a search warrant to justify an intrusion into a premises to respond to the emergency. However, their warrantless entry into these areas protected by a reasonable expectation of privacy is "reasonable" within the meaning of the Fourth Amendment.

During this period, evidence seized under the plain view doctrine is admissible. However, once the emergency is over, a continued search must be justified with a warrant or other exception. In Thompson v. Louisiana, a wife shot her husband and then attempted to kill herself with sleeping pills. Before she lost consciousness, the woman called her adult daughter and told her what had happened. The daughter called the police, who responded immediately but without a warrant. The husband and wife were rushed to a hospital where the husband was pronounced dead and the wife subsequently recovered. The Court held that the warrantless entry into the home was permissible to prevent further crime and to help injured persons. Evidence found during this phase was admissible under the plain view doctrine. However, the Court held that once the husband and wife were taken to the hospital the exigency (medical emergency) that allowed the officers to enter the premises no longer existed. Therefore, the officers' warrant exception no longer existed. They had to depart the premises.

"Crime Scene" or "Murder Scene" exceptions to the Fourth Amendment do not exist. The fact that a crime or even a murder occurred in an area does not authorize, on that fact alone, intrusion by the government. Law enforcement officers interested in intruding into that area must secure a warrant or be there under a Fourth Amendment exception (if there is an ongoing emergency—the emergency scene exception will do). If there is no ongoing emergency, the officers can

secure the premises to protect the evidence while awaiting the arrival of a warrant. Segura v. United States.

VIII. SEARCHES REQUIRING NEITHER A WARRANT NOR PROBABLE CAUSE

This category of searches has been defined by the limited circumstances that surround each exception. Frisks have been extensively covered above. The remaining four searches are reviewed here.

A. SEARCHES INCIDENT TO ARREST

One of the best known and often used exceptions to the probable cause and warrant requirements of the Constitution is the right of a law enforcement officer to conduct a search incident to a lawful arrest. The right to search under this exception is based solely on the legality of the arrest itself. If a court subsequently finds the arrest was unreasonable, then any search incident to that arrest will be invalid.

The general rule established by the Supreme Court is that incident to any lawful arrest an officer may contemporaneously search both the arrestee's person and the immediate area into which he might reach in order to obtain weapons, means of escape, and any evidence that might be concealed or destroyed.

The Supreme Court has drawn a sharp distinction between searches of the arrestee's person and searches of the area, including possessions, within the person's immediate control. In a search incident to arrest involving either area, the scope of the search is governed by that degree of privacy that individuals, even persons under arrest, can expect in their person and in their possessions.

1. Searches of the Person Arrested

An officer can make a complete and thorough search of the arrestee's person regardless of the type of offense for which the person is arrested or the circumstances in the particular case. The officer making the search does not have to articulate any expectation of finding evidence. If an individual is arrested on a warrant for failure to appear for a traffic citation hearing, the arresting officer may search the entire person and if counterfeit currency is found, it will be admissible as evidence.

The Supreme Court has held that the lawful search of the "person" includes a search of those items immediately associated with the person of the arrestee. Therefore, clothing and small containers carried on the person are also subject to examination under the authority of the search incident to arrest, e.g., a wallet, a purse, an eyeglass case, a cigarette package, a pill box, etc.

2. Searches of the Arrestee's Area and Possessions

The exact area around an arrestee that officers may search incident to an arrest depends on the facts and circumstances of each case, but generally has been limited to the "arms length" or "lunging distance" area into which the individual could reasonably reach. The arrest of an individual in a living room would not justify a search incident to arrest of other rooms of the house. However, in Maryland v. Buie the Supreme Court allowed officers to look into spaces or areas *adjacent* to the area where the defendant was arrested to determine if there are persons concealed there who might harm the officers or aid the defendant's escape.

In another case, the Supreme Court specifically held that when a law enforcement officer has made a lawful custodial arrest of the occupant of an automobile, the officer may, as a contemporaneous incident of that arrest, search the passenger compartment of that automobile. New York v. Belton. This includes the contents of ***all*** containers found within the

passenger compartment, whether they are open or closed. Courts consider these searches contemporaneous even though officers have removed the defendant from the vehicle (to be placed in the police car, for example). This has become known as the Belton bright line rule.

3. Contemporaneousness Requirement

A search incident to arrest must be made at the same time and place as the arrest, i.e., it must be contemporaneous. To be contemporaneous, the search must occur at the same time as the arrest or be so connected with the arrest as to form a part of the continuous, uninterrupted, lawful act. Officers may make a lawful search incident to arrest even though the search precedes the actual words of arrest. However, in this situation, the officers must have pre-existing probable cause to arrest and the actual intent to make the arrest.

The courts have recognized that there are potential dangers associated with all custodial arrests. Therefore, it is reasonable for officers to conduct a limited search of surrounding areas and containers for weapons and evidence during that brief and often hectic first few moments of the arrest. On the other hand, once the arrestee is removed from the arrest scene altogether, officers may not go back to the place where the arrest took place to search. In determining whether a search was "contemporaneous" with an arrest a court will consider the distance the arrestee was moved from the scene and the amount of that elapsed between the arrest and the search.

Other situations may arise that will authorize a valid search incident to arrest although slightly removed from the time and exact place of the arrest. It is permissible and reasonable to search any item that must necessarily be placed on the arrestee's person, such as warm clothing on a cold day, or placed within the arrestee's immediate control, such as a diabetic's insulin kit. This type of search is permissible as incident to the arrest because it is reasonable and still considered to be contemporaneous

with the arrest. Officers may not allow, however, an arrestee to roam around or lead the person around in an attempt to justify a search of every area into which he moves as incident to his arrest. Further, the requirement that a search of the arrestee be contemporaneous is somewhat relaxed as an arrested person can be searched again before being placed in holding facility, even though this occurs at a later time and place removed from the scene of the arrest.

4. Body Cavity Searches

Body cavity searches involve intrusions beyond the body surfaces and into the vagina, rectum, stomach, etc. Although people lose a degree of expectation of privacy in their persons upon being arrested, they retain their expectation of privacy in their body cavities. A warrantless search of a body cavity of an arrestee is not justified as incident to an arrest. However, a warrantless search of a body cavity may be reasonable where the defendant is going to be incarcerated.

Generally, the courts take a very restrictive approach in determining the validity of body cavity searches. *First,* there must be probable cause to believe that an item subject to seizure is concealed within the body cavity. *Second,* a physician or other appropriate medical professional must remove the item under proper medical conditions, or the defendant must voluntarily remove the item himself. *Third,* there must be no other means of obtaining the item. Although the courts have sanctioned the warrantless removal of evidence from a subject's body by a doctor under exigent circumstances, such as obtaining a blood sample for a blood-alcohol content test for intoxication, the preferable procedure for obtaining blood samples for other purposes is through a search warrant.

Officers may detain and observe the defendant, reducing the opportunity for the suspect to destroy the evidence while the officers obtain a search warrant. The courts will weigh the degree of intrusion into the defendant's body against the dangers that may exist to the defendant in deciding whether to authorize a search. While it may be

relatively simple to obtain a warrant to have a doctor search a vagina or rectum of a suspect for a concealed narcotics package, a court will be unlikely to grant a warrant authorizing major surgery on a defendant for an item of evidence, such as a bullet lodged near the person's spine. Winston v. Lee.

Officers may take reasonable steps and use reasonable force to prevent defendants from concealing an item in their body, such as stopping a defendant from swallowing a balloon filled with heroin. Conduct such as pressing the neck or Adam's apple or bending the head back to prevent swallowing is acceptable if the officers are careful not to choke or prevent the breathing of a defendant.

5. Protective Sweeps and Security Measures

When officers enter a premises to effect a lawful arrest, other individuals may be present in the premises who pose a danger to the officers' safety or the safety of others (see "Protective Sweeps" above). Recall that in Maryland v. Buie, the Supreme Court authorized arresting officers to check the areas adjacent to the arrest scene for persons that may pose a threat to security. This check does not have to be supported by any suspicion but is authorized because of the nature of the arrest and the inherent threats such scenes pose to law enforcement officers.

Where officers have a "reasonable belief based on specific and articulable facts which, taken together with the rational inferences from those facts, reasonably [warrant the officers] in believing that the area swept harbor[s] an individual posing a danger to the officer[s] or others," they may conduct a protective sweep of the entire premises. Maryland v. Buie. If the circumstances of the arrest suggest to a reasonable officer that someone inside the premises poses a potential danger to arresting officers, the officers may take steps to ensure that the premises is not harboring other persons who are dangerous.

B. CONSENT SEARCHES

A search conducted pursuant to a valid consent is an exception to the Fourth Amendment's requirements of a warrant and probable cause. The test of the validity of consent is whether it was ***voluntary granted by someone with the actual or apparent authority to do so.***

1. Voluntary

Courts determine whether persons grant consent freely and voluntarily by considering all of the surrounding circumstances. One of these circumstances is the consenter's knowledge of the right to withhold consent, though such knowledge is not required. An officer is not required to advise a person of their right to refuse consent nor, even if the person has been previously detained, that they have a right to depart. Ohio v. Robinette.

The government has the burden of proving that consent was voluntarily granted. This burden is especially heavy if the person is in custody. However, a person who is under arrest or in jail/prison has the capacity to grant voluntary consent. A valid consent need not be given in writing, though such is preferable to an oral consent for proof purposes.

Coercion applied by law enforcement officers will invalidate consent. Coercion may result from acts or words intended to induce an involuntary consent. The lower a person's intellectual or educational level or the less experience the person has had with the police, the more difficult will be the government's burden in proving that it did not coerce the consenter into granting consent. Some people (e.g., mental incompetents, adolescents) may lack the requisite capacity to consent. On the other hand, the government has a lighter burden to show consent is voluntarily obtained from well-educated, successful, or "street-wise" defendant.

Submission by the individual to the authority of the law enforcement officer does not constitute consent. Consent is not voluntarily given in response to an officer's statement that the officer has come to search with a warrant when, in fact, there is none (or the officer knows it is defective), or they will get a warrant if consent is withheld. On the other hand, it is permissible for officers truthfully to advise a person that they will *apply* for a warrant if consent is refused. Bumper v. North Carolina.

Actual force or threats by officers can invalidate consent just as in the case of confessions. Additionally, deception can also invalidate consent. Such practices as obtaining consent at gunpoint, telling the suspect that failure to consent will result in the loss of a job, or misrepresenting the purpose or scope of the search are discouraged.

The consenter may limit consent in time, scope, intensity, etc. Furthermore, consent may be revoked at any time, although what has already been discovered before the revocation may be introduced into evidence or used as probable cause to obtain a warrant.

Reasonable inferences determine the scope of the search authorized by consent. Consent to search a motor vehicle for an item such as narcotics implies a request to search those containers that could contain the item sought. For instance, a law enforcement officer was justified in looking in a brown paper bag found in the passenger's compartment after securing the owner's consent to search his car for drugs. Florida v. Jimeno. However, consent to search a car for drugs would not include the consent to destroy property found therein, such as cutting open the spare tire with a knife.

2. Authority to Consent

If two or more persons share a premises or a thing (e.g., a locker), each assumes the risk that the other will consent to a search. Where two

or more persons have common authority, access, and control over a place or thing, any of them can effectively consent to a search of it. Frazier v. Cupp. Property law is largely irrelevant. United States v. Matlock. It is the guest and not the motel manager, the tenant and not the landlord, who has the authority to consent.

Officers must be extremely careful when authority to consent is in doubt. If two persons are roommates, one of them can consent to a search of that person's own bedroom and such common areas as the kitchen and the living room. However, in all probability, they cannot give a valid consent to search the roommate's bedroom. Likewise, a wife will have the authority to consent to a search of a closet that she shares with her husband but not of a locked box in that closet to which he alone has the key and to which she does not have access.

The head of a household can normally consent to a search of their under aged child's bedroom even though the parents' access may be somewhat limited. The issue become more complicated as the child's age increases and they exert more control over the property in question. Two critical issues that may limit the parent's ability to consent is whether the child pays rent for the property and if the child has taken steps to limit the parent's access to the area.

A guest cannot ordinarily consent to a search of a host's premises if the guest's occupancy is limited in time and scope. Conversely, courts have held that a guest of indefinite duration with the "run of the house" has the authority to consent to a search of the host's premises. If a person implies by word or action that they have authority to consent to a search of a given area, and officers *reasonably* rely on such impression and search that area, the consent granted is acceptable as issued under the legal doctrine of "apparent" authority. Illinois v. Rodriguez.

The consent of any one party with authority is most likely valid even if the defendant is present and refuses consent. Although the Supreme Court has yet to rule directly on this issue, several Circuit Courts

of Appeal have done so (1st, 5th, 6th, 9th, 10th, D.C.). In cases involving residences and vehicles, each circuit has consistently ruled that consent of a third party with authority is valid even if the defendant is present and refuses. To date, there are no Federal Circuit Courts that have held differently.

C. INVENTORIES

Once law enforcement officials lawfully have obtained custody and control of an automobile or other personal property, officers may make an inventory of the automobile or personal property to record valuables. Officers must make their inventories in accordance with a standard agency policy. South Dakota v. Opperman. The purpose of an inventory is:

- ⇒ to protect the owner's property;
- ⇒ to protect the seizing officers from false claims; or
- ⇒ to protect the officers or the public from potential danger.

The scope of the inventory exception to the warrant requirement has been limited. Inventory searches may not extend any further than is reasonably necessary to discover valuables or other items for safekeeping. Officers are not justified in looking into the heater ducts or inside the door panels of an automobile because valuables normally are not kept in such places. In Colorado v. Bertine, the Supreme Court held that police could lawfully inventory a sealed envelope they found in a backpack in a vehicle. Based on this case, if standard agency policy allows, an inventory of any container is justified. In any case, if officers discover evidence of a crime during a lawful inventory, the plain view doctrine will apply.

D. INSPECTIONS

Inspection searches have been authorized in such various areas as courthouse inspections, restaurant inspections, coal mine inspections,

airport security inspections and others. While these searches are not conducted with probable cause, they do share some limitations. For instance, the inspecting authority must have regulatory responsibility over the behavior being inspected. In most cases, the behavior being regulated is voluntary. In most instances, the government's need to inspect is great and the intrusion suffered is minimal. Most inspections are conducted in the pursuit of public safety.

The authority to conduct a lawful inspection is based on the power to regulate and not the authority to seek out evidence of criminal activities. Therefore, for officers to justify their presence in a private area to "inspect," there must be specific statutory or regulatory authority for an inspection, and the scope of the inspection may not exceed that authority. If a reviewing court finds that the initial purpose of the entry was for a legitimate inspection, any criminal evidence subsequently discovered may be seized lawfully (under the plain view doctrine) and used as evidence in a criminal prosecution. However, officers may not attempt to use their inspection authority as a pretext to conduct a warrantless search for evidence.

Usually, officers seeking to conduct a lawful inspection must do so with the *consent* of the person whose property or premises is to be inspected. If entry is denied, they must obtain an *inspection warrant* before force may be used. For example, an officer, who is refused admission to conduct an inspection of the premises of a license holder must follow the procedures provided for by law or regulation. The officer may advise the individual of the penalties for the refusal of admission in order to seek consent to enter and/or the officer may leave the premises and seek administrative sanctions such as revocation of the license concerned, or imposition of a civil penalty; or the officer may seek issuance of a warrant to conduct the inspection.

The Fourth Amendment does not require that the government establish traditional "probable cause" or obtain a traditional search warrant to conduct a regulatory inspection. Marshall v. Barlow's, Inc.

The officers must obtain a court authorized inspection warrant similar in format to a search warrant. The only elements required are: (1) that there is authority to conduct the specific inspection and that the official to perform the inspection has that authority; and (2) that the person's facilities are subject to inspection pursuant to the agency's general regulatory scheme. Prior refusal of entry is not a prerequisite to obtaining an inspection warrant. Note that the mere existence of a sign, warning of a possible inspection of persons and/or containers, does not justify an inspection. Regulations or statutes must exist before inspections in such circumstances can be justified.

Routine health, safety, and fire inspections require an inspection warrant. Exigent circumstances will excuse a warrantless administrative or regulatory inspection. Some federally regulated industries are exempted by statute from inspection warrant requirements. The Supreme Court has validated warrantless administrative inspections of liquor and firearms dealers conducted pursuant to federal statutes.

An inspection warrant does not confer any additional search authority on officers. Therefore, once they enter the premises, the scope of their inspection is limited to those activities that they could have performed under their inspection authority if entry had been obtained by consent. If officers have probable cause and desire to conduct a search for criminal evidence, they are required to obtain a traditional Fourth Amendment search warrant.

Border searches are a well-recognized exception to both the probable cause and warrant requirements of the Fourth Amendment. The government has always exercised a right to control the movement of people and goods coming into the country. This right is based upon the inherent power of every country to protect its territory from the invasion of unauthorized persons and merchandise.

A warrantless border search is lawful if: (1) the officers conducting the search have border search authority; (2) the persons or property searched have crossed the border or have come in contact with the border (nexus with the border); and (3) the search is conducted at the border or its functional equivalent.

Generally, only Customs, Coast Guard, Border Patrol and Immigration Officers have authority to conduct border searches. Other law enforcement officers have this authority only if specifically and officially designated as one of these officers. For example, an IRS agent conducting an inspection at the border to locate stolen vehicles is not permitted to border search vehicles unless designated with that authority.

Luggage, vehicles and personal effects (merchandise) can be searched at the border by authorized officers without suspicion. However, personal searches at the border require suspicion. The degree of intrusiveness permitted depends on the amount of suspicion that exists.

Likewise, mail entering the United States from any foreign country is subject to routine search by Postal and Customs authorities without a warrant or probable cause. However, by statute, officers must have "reasonable cause to suspect" that the first-class mail contains material other than correspondence before they open it.

IX. RELATED SEARCH AND SEIZURE ISSUES

A. PRETEXTUAL STOPS AND SEARCHES AND SEIZURES

The motive or intent of the officer in conducting a search or seizure is inconsequential. In Whren v. United States, the Supreme Court held that an officer could stop a vehicle if the driver had committed a civil traffic infraction, even if a reasonable officer would not ordinarily have made the stop. This is known as a pretextual stop and is reasonable under the Fourth Amendment.

B. ENTRANCES IN UNDERCOVER CAPACITY

Where an officer gains entry into a premises by assuming a false identity and seeking to purchase contraband or seeking to become involved in illegal activities, the entry (and any subsequent observations made) is lawful. The suspect, by allowing the undercover officer to enter with full knowledge that the undercover officer desires to seek or discuss contraband or other illegal activities, has relinquished the expectation of privacy in those matters.

In some situations, officers may desire to utilize a ruse in order to gain entry into a premises for the purpose of making observations. The federal circuit courts of appeal are divided on the extent to which different ruses are acceptable in order to make lawful observations. Some circuit courts have held that using a ruse to induce an individual to admit officers so they can conduct a surreptitious search is a violation of the individual's expectation of privacy. Other circuits have upheld the use of such ruses on the theory that persons who voluntarily allow strangers into their premises run the risk that the visitors are law enforcement officers or agents of the government.

The question about the use of ruses for gaining entry into areas of privacy becomes more problematic where officers disguise themselves as persons with some kind of official authority allowing entry into those areas. For example, if officers pretend to work for the city gas inspector's office and ask for permission to enter a premises to inspect for gas leaks, an occupant may feel compelled in such circumstances to grant entry because of the "official" nature of the request to enter. While the Supreme Court has not dealt expressly with this situation, some circuit courts of appeal and legal scholars suggest that this is an impermissible means of gaining access to a premises in order to conduct a search.

Occasionally, officers may encounter situations in which traditional law enforcement techniques for determining what is inside a premises

would not be effective or are for many reasons impractical under the circumstances. In those cases, officers may want to consider the use of ruses for gaining entry into areas where a person has a reasonable expectation of privacy. Since the Supreme Court has not spoken clearly with respect to what ruses may be acceptable, and the circuit courts are divided over the extent to which ruses may be used, officers should consult with their local U.S. Attorneys Office for guidance when considering such investigative techniques.

C. FORFEITURES

There are various federal statutes that authorize law enforcement officers to seize vehicles, vessels, or aircraft that have been or are being used to transport or facilitate the transportation of contraband. Some statutes allow such forfeitures when the conveyance is intended to be used for such transportation. The general forfeiture statute (Title 49 U.S.C. §§ 80301-80306) applies to controlled substances, and to forged and counterfeit obligations of the United States. Different specific statutes enforced by various agencies cover many other items.

Such seizures are permitted because the conveyance's title has been forfeited in law to the United States since the conveyance itself, by its use, is considered to have offended the sovereign. Therefore, once there is probable cause to forfeit a conveyance, i.e., believe that the conveyance has been or is being used to transport contraband, the government has a superior right to take possession of it and federal courts have held that a warrantless seizure becomes "reasonable."

There will be a subsequent formal legal proceeding against the conveyance to determine whether the United States government should permanently retain title. The results of this proceeding will have no bearing on the legality of a previous seizure and search of the conveyance.

Under the general rule, the seizure of the conveyance does not have to be incident to an arrest and may be made at any place and any time that

officers find the conveyance. Florida v. White. However, if the vehicle is located on curtilage, a warrant is required to enter onto the premises to seize the vehicle. In any event, officers must follow the provisions of the forfeiture statutes. Forfeitures are not authorized because a conveyance merely has been used in a crime, transported evidence, etc. The conveyance must be used in connection with a specific class of contraband as established in the particular forfeiture statutes

GOVERNMENT WORKPLACE SEARCHES

I. DOES REASONABLE EXPECTATION OF PRIVACY EXIST? 113
A. PRIOR NOTICE (LEGITIMATE REGULATION) 114
B. COMMON PRACTICES AND PROCEDURES 115
C. OPENNESS AND ACCESSIBILITY 116
D. THE POSITION OF THE EMPLOYEE 117
E. WAIVER OF RIGHTS 118

II. IF REP EXISTS, HOW CAN IT BE DEFEATED? 119
A. WORK-RELATED, NON-INVESTIGATORY PURPOSES 120
B. EVIDENCE OF CRIMINAL VIOLATIONS 120
C. "MIXED MOTIVE" SEARCHES 121

CASE CITATIONS 123

Can government employees have a reasonable expectation of privacy in their offices, desks, computers, and filing cabinets? If such an expectation of privacy does exist, what standards must a supervisor follow to lawfully conduct a warrantless search of those areas? Must a supervisor have probable cause to search a government employee's workplace? Or is a search permitted on some lesser standard of suspicion? The Supreme Court addressed these questions in O'Connor v. Ortega. The purpose of this course is to provide a framework within which the principles outlined in O'Connor for "workplace" searches by government supervisors can be understood and applied. As used in this chapter, the term "workplace" "includes those areas and items that are related to work and are typically within the employer's control. This would generally include such areas as offices, desks, filing cabinets, and computers. However, not everything within a business location can be considered part of the "workplace" as that term has been defined. For example, a government employee would continue to have an expectation of privacy in his or her personal belongings that might have been brought into the workplace environment, such as a purse or briefcase. Thus, the standards for workplace searches delineated below would not apply to a search of that type of personal property.

When a government supervisor is considering the search of a government employee's workspace, a two-part analysis can be utilized to simplify the process. First, determine whether the employee has a reasonable expectation of privacy in the area to be searched. If a reasonable expectation of privacy does exist, then consider how that expectation can be defeated.

I. DOES A REASONABLE EXPECTATION OF PRIVACY EXIST?

A "reasonable expectation of privacy" exists when (1) an individual exhibits an actual expectation of privacy, and (2) that expectation is one that society is prepared to recognize as being reasonable. If either of these two prongs is not met, then no expectation of privacy exists, and the

Fourth Amendment is not implicated. Government employees can, and often do, establish expectations of privacy in their government offices, desks, computers, and filing cabinets. A cursory glance into any government office will show that individual government employees typically expect some form of privacy, based on the intermingling of their personal and professional lives (e.g., pictures of kids on desks and diplomas on walls). Many government agencies allow, if not encourage, individuals to perform some personal business while in a governmental workplace to promote efficiency, such as using a government telephone to make a personal phone call during a lunch hour. Nonetheless, a government employee's expectation of privacy is limited by the "operational realities of the workplace," and "whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." O'Connor. Although government ownership of the property to be searched (e.g., a government-owned computer assigned to a government employee) is an important consideration, it does not, standing alone, dictate a finding that no reasonable expectation of privacy exists. "Applicability of the Fourth Amendment does not turn on the nature of the property interest in the searched premises, but on the reasonableness of the person's privacy expectation." Gillard v. Schmidt. Courts have utilized a variety of factors to determine whether a government employee has a reasonable expectation of privacy in his or her workspace. Among the most important are the following:

A. PRIOR NOTICE TO THE EMPLOYEE (LEGITIMATE REGULATION)

In O'Connor, the Supreme Court held that an employee's expectation of privacy could be reduced through "legitimate regulation." For example, "government employees who are notified that their employer has retained rights to access or inspect information stored on the employer's computers can have no reasonable expectation of privacy in the information stored there." Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section, Criminal Division, Department of

Justice at 41 (March 2001). A recent Fourth Circuit Court of Appeals case, United States v. Simons, illustrates this point. In Simons, the Foreign Bureau of Information Services (FBIS), a division of the Central Intelligence Agency, employed the defendant. FBIS had an Internet usage policy that (1) specifically prohibited accessing unlawful material, and (2) prohibited use of the Internet for anything other than official business. Further, the policy noted that FBIS would "periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate." When a keyword search indicated that Simons had been visiting numerous illicit web sites from his government computer, multiple searches of his hard drive were conducted from a remote location, resulting in the discovery of several pornographic images of minors. Simons challenged the search of his computer, claiming his Fourth Amendment rights had been violated. In rejecting this challenge, the Fourth Circuit Court of Appeals held that Simons "did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of the FBIS Internet policy." Through its language, "this policy placed employees on notice that they could not reasonably expect that their Internet activity would be private."

B. COMMON PRACTICES AND PROCEDURES

In O'Connor, the Supreme Court also recognized that "[p]ublic employees' expectations of privacy in their offices, desks, and file cabinets … may be reduced by virtue of actual office practices and procedures." Alternatively, common office practices and procedures may permit a government employee to establish an expectation of privacy in an area where one would otherwise not exist. For example, in United States v. Speights, the defendant was a police officer who retained a locker at his police headquarters. Both a personal lock and a lock that had been issued by the department were used to secure the locker. There were no regulations that addressed the issue of personal locks on the police lockers, nor was there any regulation or notice that the lockers could be searched. There was also no regulation as to what a police officer might

keep in the locker. Upon receiving information that Speights had a sawed-off shotgun in his locker, the locker was opened with a master key (for the police-issued lock) and bolt cutters (for Speights' personal lock). A sawed-off shotgun was recovered in the search, and Speights was convicted of illegally possessing the weapon. On appeal, he claimed his Fourth Amendment rights had been violated by the search of his locker. The Third Circuit Court of Appeals agreed, finding that "no regulation and no police practice" existed to justify the search of Speights' locker. According to the court, "only if the police department had a practice of opening lockers with private locks without the consent of the user would [Speights'] privacy expectation be unreasonable." While there had been scattered instances of inspections of the lockers for cleanliness (3-4 in 12 years), "there [was] insufficient evidence to conclude that the police department practice negated Speights' otherwise reasonable expectation of privacy."

C. OPENNESS AND ACCESSIBILITY

Courts will often look to the openness or accessibility of a workspace to determine whether an expectation of privacy can be sustained. Among the factors that are considered are "the employee's relationship to the item seized; whether the item was in the immediate control of the employee when it was seized; and whether the employee took actions to maintain his privacy in the item." United States v. Angevine. The more accessible the item or area is to others, the less likely it is an individual employee's claim of privacy would be accepted. The more the item or area in question was given over to an employee's exclusive use, the more likely an expectation of privacy would be found. As a general rule, "where a public employee has his or her own office or desk which co-workers and superiors normally do not enter, and where no agency policy or regulation warns the employee that an expectation of privacy is unreasonable, an expectation of privacy may be reasonable." McGregor v. Greer. Offices that are "continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits … may be so open to fellow

employees or the public that no expectation of privacy is reasonable." O'Connor.

"Ordinarily, business premises invite lesser privacy expectations than do residences." Vega-Rodriguez v. Puerto Rico Telephone Company. Where areas are, by their very nature, "open" and "public," no reasonable expectation of privacy can exist in that area. For example, where an unlocked desk or credenza was located in an "open, accessible area," no reasonable expectation of privacy was found to exist. O'Bryan v. KTIV Television. Nonetheless, the existence of a master key will not defeat an employee's expectation of privacy in his or her office. Nor does an employee's failure to consistently shut and lock the office door automatically sacrifice any expectation of privacy in that area. Just because others may be permitted access to an employee's office does not automatically destroy the employee's privacy expectation. As one court has noted, "[p]rivacy does not require solitude." United States v. Taketa.

D. THE POSITION OF THE EMPLOYEE

Courts will consider the position occupied by the employee who was the subject of the workplace search. This is especially true where the subject of the search is a law enforcement officer. While law enforcement officers do not lose their Constitutional rights by virtue of accepting their position, there is a "substantial public interest in ensuring the appearance and actuality of police integrity," in that "a trustworthy police force is a precondition of minimal social stability in our imperfect society." Biehunik v. Felicetta. This "interest in police integrity … may justify some intrusions on the privacy of police officers which the Fourth Amendment would not otherwise tolerate." Kirkpatrick v. The City of Los Angeles. A case on point is Biehunik, involving allegations of police brutality. After several citizens were severely beaten by a large group of police officers, the police commissioner ordered 62 police officers to participate in a lineup for investigative purposes. The officers moved to prevent the

lineup, claiming that it violated their Constitutional rights. In rejecting the officers' argument, the court noted, "policemen, who voluntarily accept the unique status of watchman of the social order, may not reasonably expect the same freedom from governmental restraints which are designed to ensure his fitness for office as from similar governmental actions not so designed."

A similar result was reached by the same court, albeit it in a different context, in Sheppard v. Beerman. Sheppard, a law clerk, brought a civil action against the judge for whom he clerked, alleging that the judge impermissibly searched his desk in violation of the Fourth Amendment. In holding that Sheppard had no reasonable expectation of privacy in the desk, the court relied upon the unique "working relationship between a judge and her clerk."

> *Unlike a typical employment relationship …, in order for a judicial chambers to function efficiently, an absolute free flow of information between the clerk and the judge is usually necessary. Accordingly, the clerk has access to all the documents pertaining to a case. In turn, the judge necessarily has access to the files and papers kept by the clerk, which will often include the clerk's notes from discussions with the judge. Because of this distinctive open access to documents characteristic of judicial chambers, we agree with the district court's determination that Sheppard had 'no reasonable expectation of privacy in chambers' appurtenances, embracing desks, file cabinets or other work areas.'*

E. WAIVER OF RIGHTS

Occasionally, a government employee may actually waive his or her expectation of privacy as a precondition of receiving a certain benefit from their employer. In American Postal Workers Union v. United States Postal Service, postal employees were eligible to receive personal lockers at their postal facility. Before being allowed to do so, however, each employee had to sign a waiver that noted the locker was "subject to

inspection at any time by authorized personnel." Further, the administrative manual of the Postal Services noted that all property provided by the Postal Service was "at all times subject to examination and inspection by duly authorized postal officials in the discharge of their official duties." Finally, the collective bargaining agreement for these employees "provided for random inspection of lockers under specified circumstances." As noted by the court: "In light of the clearly expressed provisions permitting random and unannounced locker inspections under the conditions described above, the collective class of plaintiffs had no reasonable expectation of privacy in their respective lockers that was protected by the Fourth Amendment."

II. IF A REASONABLE EXPECTATION OF PRIVACY DOES EXIST, HOW CAN THAT EXPECTATION BE DEFEATED?

"The Fourth Amendment protects individuals from unreasonable searches conducted by the Government, even when the Government acts as an employer." Nat'l Treasury Employees Union v. Von Raab. If a reasonable expectation of privacy does exist in the workplace, the courts will scrutinize the motivations behind the supervisor's search to determine if the warrantless search is valid. "The 'special needs' of public employers may … allow them to dispense with probable cause and warrant requirements when conducting workplace searches related to investigations of work-related misconduct." Leventhal v. Knapek. As noted by the Supreme Court in O'Connor:

> *In our view, requiring an employer to obtain a warrant whenever the employer wished to enter an employee's office, desk, or file cabinets for a work-related purpose would seriously disrupt the routine conduct of business and would be unduly burdensome. Imposing unwieldy warrant procedures in such cases upon supervisors, who would otherwise have no reason to be familiar with such procedures, is simply unreasonable.*

Thus, the motivation behind the search of the employee's workspace is key to determining the standard required. In *O'Connor*, the Supreme Court outlined two basic categories of workplace searches: (1) Searches for work-related, non-investigatory purposes, and (2) searches for evidence of criminal violations.

A. SEARCHES FOR WORK-RELATED, NON-INVESTIGATORY PURPOSES

When a search of a government employee's workspace is conducted for a work-related, non-investigatory purpose, such as retrieving a needed file or investigating work-related misconduct, the search must be reasonable based on the totality of the circumstances. As noted by the Supreme Court:

> *Ordinarily, a search of an employee's office by a supervisor will be 'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a non-investigatory, work-related purpose, such as to retrieve a needed file.* O'Connor.

Additionally, a search will be "permissible in scope" when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of … the nature of the [misconduct]." O'Connor.

B. SEARCHES FOR EVIDENCE OF CRIMINAL VIOLATIONS

In O'Connor, the Supreme Court "specifically declined to 'address the appropriate standard when an employee is being investigated for criminal misconduct or breaches of other nonwork-related or regulatory standards.'" Nonetheless, "the distinction between searches and seizures for purpose of criminal prosecution and those undertaken for work-related or administrative purposes is critical and many courts upholding a

standard lower than probable cause have recognized the lower standard is not appropriate in the criminal arena." Cerrone v. Cahill. "Accordingly, in the criminal context, the appropriate standard for searches and seizures involving work-related misconduct is probable cause." Id. Where the sole motivation behind the search is to uncover evidence of criminal wrongdoing, "the traditional requirements of probable cause and warrant are applicable." Id.

C. "MIXED MOTIVE" SEARCHES

While the standards set out above appear relatively clear, there are often situations in which a government employee's misconduct might well fit into both of the above categories. In other words, the employee is engaged in administrative misconduct that is also criminal in nature. "The courts have adopted fairly generous interpretations of O'Connor when confronted with mixed-motive searches." Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section, Criminal Division, Department of Justice at 45 (March 2001). For example, in United States v. Reilly, the defendant was accessing child pornography from his government computer, a clear violation of the Department of Labor's computer use policy. Two diskettes were seized from the defendant, both of which were later found to contain child pornography. His motion to suppress the two diskettes was denied. The court found the search of these diskettes fell within O'Connor's "work-related misconduct" exception: "Agent Wager's dual role as an investigator of workplace misfeasance and criminal activity does not invalidate the otherwise legitimate workplace search."

Similarly, in United States v. Simons, the court upheld a search of a government employee's office even "assum[ing] that the dominant purpose of the warrantless search of Simons' office was to acquire evidence of criminal activity."

Nevertheless, the search remains within the O'Connor exception to the warrant requirement; FBIS did not lose its special need for 'the efficient and proper operation of the workplace,' merely because the evidence obtained was evidence of a crime. Simons' violation of FBIS' Internet policy happened also to be a violation of criminal law; this does not mean that FBIS lost the capacity and interests of an employer.

CASE CITATIONS

American Postal Workers Union v. United States Postal Service, 871 F.2d 556 (6th Cir. 1989)

Biehunik v. Felicetta, 441 F.2d 228 (2d Cir. 1971)

Cerrone v. Cahill, 84 F. Supp. 2d 330 (N.D.N.Y. 2000)

Gillard v. Schmidt, 579 F.2d 825 (3rd Cir. 1978)

Kirkpatrick v. The City of Los Angeles, 803 F.2d 485 (9th Cir. 1986)

Leventhal v. Knapek, 266 F.3d 64 (2d Cir. 2001)

McGregor v. Greer, 748 F. Supp. 881 (D.D.C. 1990)

Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989)

O'Bryan v. KTIV Television, 868 F. Supp. 1146 (N.D. Iowa 1994)

O'Connor v. Ortega, 480 U.S. 709 (1987)(plurality opinion)

Sheppard v. Beerman, 18 F.3d 147 (2d Cir. 1994)

United States v. Angevine, 2002 U.S. App. LEXIS 2746 (10th Cir. 2002)

United States v. Reilly, 2002 U.S. Dist. LEXIS 9865 (S.D.N.Y. 2002)

United States v. Simons, 206 F.3d 392 (4th Cir. 2000)

United States v. Speights, 557 F.2d 362 (3rd Cir. 1977)

United States v. Taketa, 923 F.2d 665 (9th Cir. 1991)

Vega-Rodriguez v. Puerto Rico Telephone Company, 110 F.3d. 174 (1st Cir. 1997)

ELECTRONIC LAW AND EVIDENCE

I. INTRODUCTION 127

II. HISTORY OF ELECTRONIC SURVEILLANCE 128
A. OLMSTEAD V. UNITED STATES 128
B. FEDERAL COMMUNICATIONS ACT OF 1934 128
C. KATZ V. UNITED STATES 129
D. TITLE III 129
E. ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986 130

III. THE REQUIREMENTS OF TITLE III 130
A. WHO CAN APPLY FOR A TITLE III COURT ORDER 130
B. ENUMERATED CRIMES ONLY 131
1. Wire or Oral Communications 131
2. Electronic Communications 131
C. AUTHORIZATION FOR A TITLE III COURT ORDER 131
1. Wire or Oral Communications 132
2. Electronic Communications 132
D. CONTENTS OF THE APPLICATION 133
1. Identity 133
2. Statement of Facts and Circumstances 133
3. Necessity Statement 134
4. Time Period 134
5. Statement Regarding Previous Applications 135
6. Minimization Statement 135
7. Request for Covert Entry 136
E. WHO MAY APPROVE A TITLE III APPLICATION? 136

IV. SURVEILLANCE EXEMPTED FROM TITLE III 137
A. NO REASONABLE EXPECTATION OF PRIVACY 137
B. CONSENSUAL MONITORING 139
1. Written Approval Required 139
2. Oral Authorization 140
C. SPECIAL LIMITATIONS ON THE USE OF CONSENSUAL MONITORING 140
1. Device Located on the Person 141

2. Device in a Fixed Location 141
D. COMMUNICATIONS EXEMPTED FROM TITLE III..... 141
E. DISCLOSURE OF TECHNICAL DATA 142

V. ELECTRONIC TRACKING DEVICES..... 143
A. INSTALLATION OF AN ELECTRONIC TRACKING DEVICE 143
B. MONITORING OF AN ELECTRONIC TRACKING DEVICE..... 145

VI. PEN REGISTERS AND TRAP AND TRACE DEVICES 147
A. DEFINITIONS..... 147
1. Pen Registers 147
2. Trap and Trace Devices..... 147
B. REGULATION OF PEN REGISTERS AND TRAP AND TRACE DEVICES..... 148
C. OBTAINING A COURT ORDER TO USE A PEN REGISTER OR TRAP AND TRACE DEVICE 148

VII. VIDEO-ONLY SURVEILLANCE IN AN AREA WHERE A REASONABLE EXPECTATION OF PRIVACY EXISTS 149

VIII. STORED ELECTRONIC COMMUNICATIONS 151
A. CLASSIFYING THE INFORMATION SOUGHT..... 151
1. Basic Subscriber Information..... 151
2. Transactional Records 152
3. Contents..... 152
B. METHODS FOR OBTAINING THE INFORMATION SOUGHT 152
1. Obtaining Basic Subscriber Information..... 153
2. Obtaining Transactional Records 154
3. Obtaining Contents..... 154
a. In Storage – 180 Days or Less 154
b. In Storage – More Than 180 Days..... 155
C. PRESERVATION OF EVIDENCE 157

I. INTRODUCTION

In recent years, the use of electronic surveillance has taken on a new sense of importance based upon the increased use and availability of technology by criminals. The purpose of this course is to give federal law enforcement officers a basic overview of the federal laws regarding the use of electronic devices to (1) intercept wire, oral and electronic communications; (2) track the movements of suspects; and (3) trace telephone calls and electronic communications. Additionally, this chapter will cover the use of video-only surveillance in locations where an individual has a reasonable expectation of privacy, and the federal requirements governing access to stored electronic communications held by a network service provider, such as America Online or Prodigy.

This course will not cover in detail the policies of any individual agency regarding the proper method for wiretapping or eavesdropping. Officers must familiarize themselves with the particular requirements of their agency. Further, this course does not cover state law regarding electronic surveillance. While state and local law must follow, at a minimum, the federal laws regarding electronic surveillance, each state is free to make its laws more restrictive than that required by federal law. This text will cover only the requirements pertaining to federal law enforcement officers. Additionally, in 1978, Congress passed the Foreign Intelligence Surveillance Act, which allows certain warrantless surveillance when a foreign power solely is involved. This statute is beyond the scope of this course.

The statutes pertaining to the laws of electronic surveillance are codified at Title 18 U.S.C. § 2510, *et seq*. In 1968, Congress passed the "Omnibus Crime Control and Safe Streets Act" (OCCSSA). Title III of the OCCSSA dealt specifically with the acquisition and use of wiretap evidence. As a result, federal law enforcement officers have come to refer to this area of the law simply as "Title III." However, in 1986, Congress amended Title III with the passage of the Electronic Communications Privacy Act (ECPA). Title I of the ECPA deals with the law of "electronic communications." Because of the ECPA's passage, this area is now

referred to alternately by various federal departments and agencies as either "Title III" or "Title I." For purposes of this course, the term "Title III" will be used throughout to discuss the law of electronic communications.

II. HISTORY OF ELECTRONIC SURVEILLANCE

Title III 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. To fully understand the stringent requirements of Title III, it is vital to understand the history of the legislation.

A. OLMSTEAD V. UNITED STATES

Before 1934, no federal statute regulated wiretapping. However, in 1928, a Supreme Court ruling laid the foundation for what would ultimately become Title III. In Olmstead v. United States, the Supreme Court held that 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 did not violate the Fourth Amendment. According to the Court, 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 telephone line, no Fourth Amendment "search" occurred. In their decision, however, the Court noted that Congress could regulate wiretapping if it so desired.

B. 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, and read, in pertinent part:

> *"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 communications to anyone."*

However, the statute did not cover the interception of oral communications (e.g., eavesdropping or bugging).

C. KATZ V. UNITED STATES

It was not until almost 40 years after the Olmstead decision that the Supreme Court reversed itself, and changed the basis of Fourth Amendment analysis from focusing strictly on an individual's property rights to focusing on an individual's privacy rights. In Katz v. United States, 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 top of the telephone booth. Because they had not intruded on the defendant's property in installing and utilizing this device, the officers had complied with the mandate of Olmstead. However, the Supreme Court reversed its previous ruling in Olmstead, holding, instead, that whenever the government intrudes upon an individual's reasonable expectation of privacy, the Fourth Amendment applies.

D. 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. As noted by one court, "Congress codified the requirements ... of Katz in Title III." United States v. Petti. The purpose of Title III was twofold: First, to protect the privacy of wire and oral communications; and second, to delineate, on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized. 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.

E. ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

When Congress enacted Title III in 1968, it did not consider many of the technologies that are now commonplace. In an effort to update Title III and extend the privacy protections of that legislation to modern, more advanced technologies, Congress passed the Electronic Communications Privacy Act of 1986 (ECPA). With passage of the ECPA, Congress added a third category of communications, "electronic communications," whose interception would now be regulated by Title III. "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 facsimiles machines." United States Attorney's Manual, Chapter 9-7.100.

III. THE REQUIREMENTS OF TITLE III

Officers must meet stringent requirements to obtain a Title III court order to conduct non-consensual intercepts of wire, oral, and electronic communications.

A. WHO CAN APPLY FOR A TITLE III COURT ORDER

Any "investigative or law enforcement officer" may apply for a Title III court order. The phrase "investigative or law enforcement officer" is defined as "any officer of the United States ... 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." Title 18 U.S.C. § 2510(7).

B. ENUMERATED CRIMES ONLY

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 Title 18 U.S.C. § 2516. The type of interception being requested (e.g., wire or electronic) will play a role in this analysis.

1. Wire or Oral Communications

To intercept a wire or oral communication, an investigative or law enforcement officer must have probable cause to believe that one of the predicate offenses specifically listed in Title 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 § 2516(1) may be investigated through the interception of wire or oral communications.

2. Electronic Communications

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. Title 18 U.S.C. § 2516(2).

C. AUTHORIZATION TO APPLY FOR A TITLE III COURT ORDER

Before an investigative or law enforcement officer may submit an application for a Title III court order, the application must be reviewed and approved by an appropriate Department of Justice official. Who must authorize the application depends, again, on the type of communication being intercepted.

1. Wire or Oral Communications

Pursuant to Title 18 U.S.C. § 2516(1), a high-ranking member of the Department of Justice must authorize any application requesting permission to non-consensually intercept wire or oral communications. This requirement "evinced 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. The individuals who may authorize an application to intercept wire or oral communications include, but are not limited to, the Attorney General; Deputy Attorney General; Associate Attorney General; any Assistant Attorney General; and any Acting Assistant Attorney General.

2. Electronic Communications

Pursuant to Title 18 U.S.C. § 2516(3), any government attorney may authorize a Title III application to intercept electronic communications in the investigation of a federal felony. However, the Department of Justice has imposed limitations on this authority.

> *The Department of Justice and Congress agreed informally at the time of the ECPA's enactment that, for a three-year period, Department of Justice approval would nonetheless be required before applications could be submitted to a court to conduct interceptions of electronic communications. After that three-year period, the Department of Justice rescinded the prior approval requirements for the interception of electronic communications over digital-display paging devices, but continued the need for Department of Justice approval prior to application to the court for the interception of electronic communications over any other device, such as computers and facsimile machines. Applications to the court for authorization to intercept electronic communications over digital-display pagers – which are the most commonly targeted type of electronic communications – may be based solely upon the authorization of a United States Attorney.* United States Attorney's Manual, Chapter 9.7-100.

D. CONTENTS OF THE APPLICATION

Pursuant to Title 18 U.S.C. § 2518, each application for a Title III court order must contain specific information before a court can authorize the interception. In addition to being in writing, under oath, and signed by either the United States Attorney or an Assistant United States Attorney, the application must contain the following:

1. Identity

The application must contain the identity of the investigative or law enforcement officer making the application, as well as the officer who authorized the application. Title 18 U.S.C. § 2518(1)(a).

2. Statement of Facts and Circumstances

Title 18 U.S.C. § 2518(1)(b) requires a full and complete statement of the facts and circumstances relied upon by the applicant to justify his belief that a Title III court order should be issued. This statement must include the following information:

- Details as to the particular offense that has been, is being, or is about to be committed;
- A particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted;
- A particular description of the type of communications sought to be intercepted; and
- The identity of the individuals, if known, committing the offense and whose communications are to be intercepted. The Supreme Court requires that a Title III application name all individuals whom the government has probable cause to believe are

engaged in the criminal activity under investigation and whose conversations the government expects to intercept. United States v. Donovan. It is the policy of the Department of Justice to "name as potential subjects all persons whose involvement in the alleged offenses is indicated." United States Attorney's Manual, Chapter 9, Criminal Resources Manual at 28.

3. Necessity Statement

Pursuant to Title 18 U.S.C. § 2518(1)(c), a Title III application must contain 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 would 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. As noted by the Supreme Court, this section was "designed to assure wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the crime." United States v. Kahn.

4. Time Period

The application must contain a statement of the period of time for which the interception is to be maintained. Title 18 U.S.C. § 2518(1)(d). Pursuant to Title 18 U.S.C. § 2518(5), no Title III court order may authorize or approve the interception of wire, oral, or electronic communications for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days. This 30-day period begins on the earlier of either (1) 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. This 10-day period is intended primarily for the installation of whatever device will be used to conduct the interceptions. Extensions of the 30-day period are permissible, but

only after again meeting the requirements of the initial Title III application. Further, 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." Title 18 U.S.C. § 2518(1)(f).

5. Statement Regarding Previous Applications

Pursuant to Title 18 U.S.C. § 2518(1)(e), a Title III application must also contain a full and complete statement of the facts surrounding all previous Title III applications known to the individual authorizing and making the application that involved any of the same persons, facilities, or places specified in the application, and the action taken by the judge on each of these previous applications. In other words, an individual applying for a Title III court order must detail in the application any previous requests for a Title III court order, if that previous request involved the same persons, facilities, or places that are now being considered.

6. Minimization Statement

A Title III application should also contain a statement that the surveillance, if approved, will be "conducted in such a way as to minimize the interception of communications not otherwise subject to interception." Title 18 U.S.C. § 2518(5). In determining whether law enforcement officers have complied with this "minimization" requirement, courts look to the "totality of the circumstances" to see if the minimization effort was reasonable. United States v. Charles. Among the factors the courts have considered in making this judgement are (1) the nature and complexity of the suspected crimes; (2) the number of target individuals; (3) the ambiguity of the intercepted conversations; (4) the thoroughness of the government precautions to bring about minimization; and (5) the degree of judicial supervision over the surveillance practices. United States v. London. 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 portion of an interception do not automatically result in the suppression of all the evidence obtained through the use of electronic surveillance. 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.

7. Request for Covert Entry

The Supreme Court does not require that a Title III application contain a specific request for permission to covertly enter a location to install, maintain, and remove surveillance devices. Dalia v. United States. According to the Court: "Those considering the surveillance legislation (i.e., Congress) understood that, by authorizing electronic interception of oral communications in addition to wire communications, they were necessarily authorizing surreptitious entries." While not required by the Supreme Court, the Department of Justice requires that Title III applications specifically contain a request for permission to surreptitiously enter to install, maintain, and remove electronic surveillance devices.

> *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.* United States Attorney's Manual, Chapter 9, Criminal Resources Manual at 28.

E. WHO MAY APPROVE A TITLE III APPLICATION?

A Title III application must be submitted for approval to "a judge of competent jurisdiction," and must be accompanied by the Department

of Justice's authorization memorandum signed by an appropriate official. In the federal system, "a judge of competent jurisdiction" includes a United States District Court Judge or a United States Circuit Court of Appeals Judge. Title 18 U.S.C. § 2510(9). A United States Magistrate Judge may not approve a Title III application. In re United States of America.

IV. SURVEILLANCE EXEMPTED FROM TITLE III

Not all interceptions of wire, oral, or electronic communications require a Title III court order. For example, as will be discussed below, the use of tracking devices ("beepers" or "transponders") do not require a Title III court order. However, two of the most important exemptions to the requirements of Title III involve situations where (1) no reasonable expectation of privacy exists in an oral communication, and (2) one of the parties to the conversation has given consent to intercept the communications (sometimes referred to as "consensual monitoring"). Each of these exemptions will be discussed in turn.

A. NO REASONABLE EXPECTATION OF PRIVACY

In Katz v. United States, the Supreme Court established the standard for determining whether a reasonable expectation of privacy exists. The test is two-pronged: First, the individual must have exhibited an actual (subjective) expectation of privacy. Second, that expectation must be one that society is prepared to recognize as objectively reasonable. If either prong of this test is not met, then no reasonable expectation of privacy exists. Title 18 U.S.C. § 2510(2) 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 justify such expectation...." The legislative history of Title III indicates that Congress intended this definition to parallel the Katz "reasonable expectation of privacy" test. United States v. Longoria. Notably, however, the definition of "wire communication" does not contain such an exception. "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." United States Attorney's Manual, Chapter 9-7.301.

As a general rule, there is no expectation of privacy in any conversation that can be overheard from a location where the interceptor has a legal right to be and where the interceptor uses only the unaided ear. As stated by the Supreme Court in Katz: "[C]onversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable." Thus, if two individuals had a conversation in a public restaurant, and spoke loudly enough for others in the restaurant to overhear their conversation, no reasonable expectation of privacy would exist. The Supreme Court has repeatedly stressed that what an individual knowingly exposes to the public is not constitutionally protected from observation. And, as one court noted:

> *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.

Finally, even though a speaker may subjectively intend for his or her conversations to remain private, a speaker has no reasonable expectation of privacy that the person to whom he is speaking will not later reveal the contents of the conversation. There is only a legitimate expectation of privacy as long as both parties expect it. If, however, one party to the conversation decides to reveal the contents of the conversation, the other party cannot claim any "right to privacy" that would prevent this revelation. In sum, if an individual engages in conversation with another, the individual does so at his own peril. 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. 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." Hoffa v. United States.

B. CONSENSUAL MONITORING

Title 18 U.S.C. § 2511(2)(c) "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." United States Attorney's Manual, Chapter 9-7.301. The consent of a single party to the conversation is required, and this consent must be given voluntarily, without physical coercion or duress. The Attorney General established 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. The following is a general summary of those guidelines. However, each agent must become familiar with the particular requirements of their agency regarding this issue.

1. Written Approval Required

In certain sensitive 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. Examples of when this requirement would apply are when the monitoring relates to the investigation of a Congressman, Federal judge, Governor or Lieutenant Governor of a State or Territory, etc.

2. Oral Authorization

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, 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.

C. SPECIAL LIMITATIONS ON THE USE OF CONSENSUAL MONITORING

When conducting a consensual monitoring, questions often arise regarding where the monitoring device may be located, as well as when the device may be monitored. Some general comments are outlined in the United States Attorney's Manual:

> *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.* United States Attorney's Manual, Chapter 9-7.302.

1. Device Located on the Person

The monitoring device may be placed on the consenting person, provided the consent was voluntarily given. If the monitoring device is so placed, the party (be it an undercover agent or confidential informant) may record any conversations he has with the suspect. Hoffa v. United States.

2. Device in a Fixed Location

The monitoring device does not have to be on the consenting person. Instead, in many instances, it is necessary to place the device in a specified location (e.g., a hotel room where a 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. First, it may be necessary to obtain a 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. Second, the device may not be monitored when the consenting party is absent, even temporarily. United States v. Yonn.

D. ELECTRONIC COMMUNICATIONS EXEMPTED FROM TITLE III

As was previously noted, the ECPA extended Title III protections to "electronic communications." However, certain 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:

- Tone-Only Pagers. The term "electronic communication" does not include "any communication made through a tone-only paging device." Title 18 U.S.C. § 2510(12)(B).

- Beepers or Transponders. The term "electronic communication" does not include "any communication from

a tracking device (as defined in section 3117 of this title)." Title 18 U.S.C. § 2510(12)(C).

- Video-Only Surveillance. The use of video-only surveillance is not regulated by Title III, but is regulated by the Fourth Amendment. United States v. Koyomejian.

- General Public Communications. The ECPA also excludes general public communications that are easily received by the public, such as AM/FM radio station broadcasts, citizen band radio transmissions, etc.

E. 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. The majority of cases that have addressed this issue have recognized a qualified privilege that prohibits disclosure of the location, equipment, and techniques used by law enforcement officers during cases involving electronic surveillance. In recognizing this "police surveillance privilege," one court analogized it to the "government-informant" privilege established by the Supreme Court in Roviaro v. United States. This 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.* United States v. Van Horn.

The courts that have recognized this privilege have been clear that the privilege is a qualified one that will give way if the defendant can show a need for the information. This requires a case-by-case approach, balancing the interests of the government in protecting the information against the defendant's right to a fair trial.

V. ELECTRONIC TRACKING DEVICES

Title 18 U.S.C. § 3117 discusses the use of "electronic or mechanical device[s] which permit the tracking of the movement of a person or object." Electronic tracking devices serve an important law enforcement function by allowing law enforcement officers to track and monitor the movements of suspects or objects from a distance, thereby reducing the possibility of detection. Two of the most commonly used tracking devices are "beepers" and "transponders." A "beeper" is a radio transmitter, usually battery-operated, which emits periodic signals that can be picked up by radio receiver. United States v. Knotts. Similar to a beeper in many respects, a "transponder" is usually used to track the location of airplanes.

Title III does not regulate the installation or monitoring of electronic tracking devices. Title 18 U.S.C. § 2510(12)(C). Instead, the Fourth Amendment governs the use of electronic tracking devices. United States v. Karo. In determining whether the use of an electronic tracking device has met the requirements of the Fourth Amendment, it is easiest to break the issue down into two separate questions: First, did the installation of the electronic tracking device comply with the Fourth Amendment? Second, did the monitoring of the electronic tracking device comply with the Fourth Amendment?

A. INSTALLATION OF AN ELECTRONIC TRACKING DEVICE

In deciding whether an electronic tracking device was legally installed, the courts utilize the traditional Fourth Amendment standard, focusing on whether installation of the device required intrusion into an area where an individual has a reasonable expectation of privacy. If so,

then the Fourth Amendment has been implicated because a "search" was conducted. If not, then no "search" occurred, and the Fourth Amendment is inapplicable. Most commonly, questions regarding the legality of installing electronic tracking devices concern installation of the device into or on vehicles and into or on government property.

- **Vehicles.** In discussing the installation of an electronic tracking device into or on a vehicle, courts have traditionally focused on whether the installation required some physical entry into the vehicle. When installation of the tracking device requires some form of physical intrusion into the vehicle (i.e., under the hood or in the interior), courts have uniformly found that this action constitutes a "search," requiring either a search warrant or an exception to the warrant requirement to satisfy the Fourth Amendment. United States v. Butts. Similarly, if installation requires physically trespassing onto the curtilage of a residence or into an attached garage, it would appear that the Fourth Amendment requires a search warrant or an exception to the warrant requirement. United States v. Hufford. However, when an electronic tracking device is installed onto the **outside** of a vehicle, the courts that have addressed the issue have reached inconsistent results. Although the Supreme Court has specifically found that there is no reasonable expectation of privacy in the outside of a vehicle, Cardwell v. Lewis, this fact has not prevented the lower courts from framing their own rules on this issue. For example, one court, seizing on the lack of privacy in the exterior of a vehicle, has found that installing a tracking device to the exterior does not constitute a Fourth Amendment "search," as long as the vehicle is located on public property. United States v. McIver. Still, at least one court that addressed the issue held that, while the installation of a tracking device is not a "search," reasonable suspicion is still required for the installation. United States v. Webster. Finally, a third court has found the installation of a tracking device to the exterior of a vehicle to be a "search," yet

viewed the warrantless installation to be lawful, so long as the officers installing the device had probable cause. United States v. Moore.

- **Government Property.** An issue that often arises in beeper or transponder cases involves the installation of the device into or on government property that is later transferred to an unsuspecting target. This issue was addressed by the Supreme Court in United States v. Karo. In sum, the Court held that the installation of a tracking device into or on government property that is later transferred to an unknowing suspect does not violate the Fourth Amendment. First, when the device is placed into or on the government property, the suspect does not have any legitimate expectation of privacy in the property. Second, the transfer to the defendant does not amount to a "seizure" of the defendant's property. As stated in the Court's opinion:

> *A 'seizure' of property occurs when 'there is some meaningful interference with an individual's possessory interests in that property.' Although the [property] may have contained an unknown and unwanted foreign object, it cannot be said that anyone's possessory interest was interfered with in a meaningful way. At most, there was a technical trespass on the space occupied by the [device.]*

B. MONITORING OF AN ELECTRONIC TRACKING DEVICE

As with the installation of an electronic tracking device, the legality of monitoring the device depends on whether the object to which the device is attached is located in an area where a reasonable expectation of privacy exists.

- Monitoring in Areas With No REP. When an electronic tracking device is located in an area where no reasonable expectation of privacy exists, the Fourth Amendment is not implicated in the monitoring. For example, if a device is lawfully installed onto the

exterior of a vehicle, the device may be monitored while the vehicle is traveling on public streets and highways. In these cases, a defendant's movements are open to visual surveillance by anyone who wishes to look, including the police. For this reason, a defendant has no reasonable expectation of privacy that his movements on a public thoroughfare would not be observed. United States v. Knotts.

- Monitoring in Areas With REP. However, when an electronic tracking device is located in an area not open to visual surveillance and where a reasonable expectation of privacy exists, such as inside a home, the Fourth Amendment is implicated in the monitoring of the device. As noted by the Supreme Court in United States v. Karo, the Fourth Amendment is violated:

  "[w]here, 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."

In these types of cases, the monitoring of the device reveals aspects of the home that could not be observed through traditional visual surveillance. For example, while officers may observe the object to which the beeper is attached enter a home, the later monitoring of the device not only verifies the officers' observations, but also establishes that the object remains on the premises, a fact not verifiable by visual surveillance. Because it is often difficult to determine where an object containing an electronic tracking device will ultimately come to rest, the Supreme Court has stated that warrants for the installation and monitoring of an electronic tracking device are desirable, since it may be critical to monitor the device to determine that it is actually located in a place not open to visual surveillance. United States v. Karo. In obtaining a warrant for the installation and monitoring of an electronic tracking device, the Supreme Court has held that a warrant will meet the requirements of the Fourth

Amendment if it provides (1) a description of the object into which the device is placed; (2) the circumstances that led the officers to install the device; and (3) the length of time for which surveillance is requested.

VI. PEN REGISTERS AND TRAP AND TRACE DEVICES

Title 18 U.S.C. §§ 3121 – 3127 deal with "pen registers" and "trap and trace" devices. While these statutes deal with real-time electronic surveillance, the use of pen registers and trap and trace devices is not specifically regulated by Title III. Instead, these devices are governed by a host of different statutory requirements.

A. DEFINITIONS

To understand the regulations pertaining to "pen registers" and "trap and trace" devices, it is first necessary to understand what purpose these devices serve.

1. Pen Registers

A "pen register" is a "device 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 communication shall not include the contents of any communication...." Title 18 U.S.C. § 3127(3). In other words, a "pen register" captures all numbers that are being dialed out from a specific telephone line, and allows law enforcement officers to learn what numbers a suspect is calling from his telephone.

2. Trap and Trace Devices

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). In other words, a "trap and trace" device captures all numbers that are coming into a specified telephone line, and allows a law enforcement officer to learn where telephone calls to the targeted phone are originating from.

B. REGULATION OF PEN REGISTERS AND TRAP AND TRACE DEVICES

As noted above, the regulations governing pen registers and trap and trace devices are contained at Title 18 U.S.C. §§ 3121 – 3127. These devices are not regulated by Title III. Title 18 U.S.C. § 2511 (2)(h). Further, the Supreme Court has held that the use of pen registers and trap and trace devices does not implicate the Fourth Amendment, because there is no actual expectation of privacy in phone numbers dialed. Smith v. Maryland. Instead, the general rule regarding the use of pen registers and trap and trace devices is contained at Title 18 U.S.C. § 3121(a), which provides that "no person may install or use a pen register or trap and trace device without first obtaining a court order under section 3123."

C. OBTAINING A COURT ORDER TO USE A PEN REGISTER OR TRAP AND TRACE DEVICE

There are a number of procedural steps to obtain a court order for the use of a pen register or trap and trace device. First, an "attorney for the government" must make the application for the court order, not the individual law enforcement officer. Second, the application must be in writing, under oath, and directed to a court of competent jurisdiction, which includes a United States Magistrate Court, United States District Court, or United States Circuit Court of Appeals. Title 18 U.S.C. § 3122(a)(1). Third, the application must include the following three pieces of information:

- The identity of the attorney for the government who is

making the application;

- The identity of the law enforcement agency conducting the investigation; and

- A certification by the attorney for the government 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).

If these procedural steps are followed, Title 18 U.S.C. § 3123(a)(1) provides that 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 determines that an attorney for the government has certified that the information likely to be obtained by the installation and use of a pen register or trap and trace device is relevant to an ongoing criminal investigation." This court order cannot exceed sixty days, although extensions of 60 days may be granted, if the initial requirements for issuance of the court order are again met.

A violation of the statute regulating the installation and use of pen registers and trap and trace devices will not result in suppression of the evidence obtained through the use of the device. United States v. Thompson. Instead, the statute makes the violation a criminal offense, punishable by a fine and/or imprisonment for not more than one year.

VII. VIDEO-ONLY SURVEILLANCE IN AN AREA WHERE A REASONABLE EXPECTATION OF PRIVACY EXISTS

The use of video-only surveillance in an area where a reasonable expectation of privacy exists is not addressed in Title III. Instead, the use of video-only surveillance in protected areas is governed by the Fourth Amendment. Under the Supreme Court's decision in Katz v. United States, when a reasonable expectation of privacy exists, a search warrant issued under Federal Rule of Criminal Procedure 41(b) and the "All Writs Act" (Title 28 U.S.C. § 1651) should be obtained for the installation and

use of the device, unless consent has been obtained. If the device is being installed and monitored in a location where no reasonable expectation of privacy exists, no search warrant is required.

While recognizing that Title III does not govern the use of video-only surveillance in unprotected areas, there is a movement among the circuit courts to require that search warrants for video-only surveillance meet certain higher, constitutional standards required by Title III. United States Attorney's Manual, Chapter 9.7-200. Specifically, in addition to showing that probable cause exists to believe that evidence of a crime will be obtained, six federal circuit courts require that the following information be included in a search warrant for video-only surveillance:

- 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;

- 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;

- A particularized description of the premises to be surveilled;

- 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 (with 30 day extension periods possible); and

- The names of the persons to be surveilled, if known.

Further, the Department of Justice requires that the investigative agency seeking to use court-ordered video surveillance obtain prior approval from the appropriate Department of Justice official. Certain officials within the department have been delegated authority to review

requests to use video-only surveillance in areas where a constitutionally protected expectation of privacy exists. Specifically, this authority has been delegated to the Assistant Attorney General, any Deputy Assistant Attorney General, and the Director and Associate Directors of the Office of Enforcement Operations. United States Attorney's Manual, Chapter 9.7-200.

VIII. STORED ELECTRONIC COMMUNICATIONS

When the ECPA was enacted in 1986, it contained two separate titles. The second of these, referred to as the Stored Access Communications Act, outlines the requirements for obtaining wire or electronic communications that are being stored by network service providers, such as America Online. Electronic mail (e-mail) stored on a network server is the primary example of this type of communication. While this portion of the statute is unusually complicated, two general rules can be formulated to simplify understanding the statute. First, a law enforcement officer must determine what type of information is being sought from the network service provider. Second, a law enforcement officer must determine what type of legal document can be used to require the network service provider to disclose the information.

A. CLASSIFYING THE INFORMATION SOUGHT

There are essentially three types of information that a law enforcement officer may wish to obtain from a network service provider: (1) Basic subscriber information; (2) transactional records; and (3) the contents of stored communications.

1. Basic Subscriber Information

Title 18 U.S.C. § 2703(c)(2) provides that "basic subscriber information" includes the following: "Name; address; local and long distance telephone connection records, or records of session times and durations; length of service (including start date) and types of services utilized; telephone or instrument number or other subscriber number or

identity, including any temporarily assigned network address; and means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service."

2. Transactional Records

Title 18 U.S.C. § 2703(c)(1)(A) defines "transactional records" as "record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications....)." Described by many as a "catch-all" category, transactional records include "only historical data involving past activity on the account." Cyber Crime Fighting: The Law Enforcement Officer's Guide to Online Crime. Examples of "transactional records" include:

- Web sites visited by the customer or subscriber;
- Cell-site data for cellular telephone calls; and
- E-mail addresses of other individuals with whom the account holder has corresponded (e.g., those who have sent e-mail to, or received e-mail from, the customer or subscriber).

3. Contents

The "contents" of a network account includes the actual files stored in the account (e.g., the actual text contained with an e-mail). Title 18 U.S.C. § 2510(8) provides that "contents" includes "any information concerning the substance, purport, or meaning of that communication."

B. METHODS FOR OBTAINING THE INFORMATION SOUGHT

Generally, a law enforcement officer may use three basic types of

documents to compel disclosure of the information listed above: (1) Search warrants; (2) Title 18 U.S.C. § 2703(d) court orders; and (3) subpoenas. The legal method that must be utilized in any given case depends on the type of information the law enforcement officer is seeking. While the consent of the customer or subscriber may always be obtained, often consent is not sought for tactical reasons. Listed below are the minimum legal methods that can be used to require a network service provider to disclose information. However, it should be noted that:

> *"one 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) court order or [subpoena] can compel...."* Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.

1. Obtaining Basic Subscriber Information

A law enforcement officer may use a subpoena to obtain "basic subscriber information" from a network service provider. Title 18 U.S.C. § 2703(c)(2). When using a subpoena to obtain this information, the government is not required to provide notice to the subscriber or customer. Title 18 U.S.C. § 2703(c)(3). The following types of Federal subpoenas can be used to obtain "basic subscriber information:"

- Federal Grand Jury subpoenas;
- Federal trial subpoenas; and
- Administrative subpoenas authorized by a Federal statute (e.g., subpoenas authorized by 6(a)(4) of the Inspector General Act).

2. Obtaining Transactional Records

To obtain "transactional records," a law enforcement officer must, at a minimum, use a court order issued pursuant to Title 18 U.S.C. § 2703(d). Either a United States Magistrate Judge, United States District Court Judge, or United States Circuit Court of Appeals Judge may issue a § 2703(d) court order. To obtain this type of court order, a 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 information, or the records or other information sought, are 'relevant and material' to an ongoing criminal investigation." As with a subpoena, there is no requirement to provide prior notice to the customer or subscriber before requiring the network service provider to disclose the records sought.

3. Obtaining Contents

A network service provider may be compelled to provide the actual contents of wire or electronic communications held in storage, such as the contents of an e-mail. The legal method that must be used to compel disclosure of this information varies, depending on how long the communication has been held in storage.

a. In Storage – 180 Days or Less

To require a network service provider to disclose the contents of a wire or electronic communication that has been in storage for 180 days or less, the government must obtain a search warrant. Title 18 U.S.C. § 2703(a). When using a search warrant to compel disclosure, no prior notice by the government to the customer or subscriber is required. Further, the government may apply for a court order to prohibit the network service provider from notifying the customer or subscriber of the existence of the warrant. Title 18 U.S.C. § 2705(b). If the court determines that notification would result in an "adverse result" (e.g., flight from

prosecution by the target, the destruction of evidence, the intimidation of potential witnesses, etc.), a request for delayed notice will be approved. There is no specified period established in the statute for how long a network service provider may be required to delay notice to the customer. Instead, the statute provides that such an order may be issued "for such period as the court deems appropriate."

b. In Storage – More Than 180 Days

To compel disclosure of the contents of a wire or electronic communication that has been in storage for more than 180 days, a law enforcement officer has three options.

- **Search Warrant**. Again, a search warrant will allow a law enforcement officer to compel the production of wire or electronic communications that have been held in storage for more than 180 days. When a search warrant is utilized, the notice provisions outlined above apply.

- Title 18 U.S.C. **§ 2703(d) Court Order**. A law enforcement officer may use a § 2703(d) court order to require a network service provider to disclose the contents of wire or electronic communications that have been held in storage for more than 180 days. However, when a § 2703(d) court order is used to obtain this information, the government must provide prior notice to the customer or subscriber. Title 18 U.S.C. § 2703(b)(1)(B)(ii). This prior notice may be delayed for a period not to exceed 90 days, if the government requests a delay and the court determines that notifying the customer of the existence of the court order may have an "adverse result." Title 18 U.S.C. § 2705(a)(1)(A). Extensions of the delay period are possible, but must be justified each time using the "adverse result" standard. Title 18 U.S.C. § 2705(a)(4). Once the delayed notice period expires, the government must notify the customer of the court order and explain the procedures surrounding the delay in notification. Finally, as with a search warrant, the government may, in certain circumstances, 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." Title 18 U.S.C. § 2705(b).

- **Subpoena**. A law enforcement officer may also obtain the contents of wire or electronic communications that have been in storage for more than 180 days with a subpoena. Title 18 U.S.C. § 2703(b)(1)(B)(i). As with "basic subscriber information," the subpoena may be a Federal Grand Jury subpoena, a Federal trial subpoena, or an administrative subpoena authorized by a Federal statute. Prior notice to the customer is required when using a subpoena to obtain this type of information. Title 18 U.S.C. § 2703(b)(1)(B). However, the court may delay notification to the customer for a period not to exceed 90 days if a "supervisory official" certifies in writing that there is reason to believe that prior notice may have an "adverse result." A "supervisory official" is defined by statute 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). 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. 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). Again, in certain circumstances, the government may ask the court for an order precluding the network service provider, for a period determined by the court to be appropriate, from notifying any other person of the existence of the subpoena.

C. PRESERVATION OF EVIDENCE

When seeking information from a network service provider, law enforcement officers must always be concerned with the inadvertent or intentional loss or destruction of the information sought. Title 18 U.S.C. § 2703(f) provides a mechanism through which a law enforcement officer can take steps to ensure that information is preserved by the network service provider. This section provides, in pertinent part, that a network service provider must, upon request by the government, "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." By statute, the records must be retained for a period of ninety days, with a ninety-day extension possible upon a renewed request by the government.

CASE CITATIONS

Cardwell v. Lewis, 417 U.S. 583 (1974)

Dalia v. United States, 441 U.S. 238 (1979)

Hoffa v. United States, 385 U.S. 293 (1966)

In re United States of America, 10 F.3d 931 (2d Cir. 1993), cert. denied, 513 U.S. 812 (1994)

Katz v. United States, 389 U.S. 347 (1967)

Olmstead v. United States, 277 U.S. 438 (1928)

Roviaro v. United States, 353 U.S. 53 (1957)

Smith v. Maryland, 442 U.S. 735 (1979)

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. Charles, 213 F.3d 10 (1st Cir.), cert. denied, 121 S. Ct. 272 (2000)

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

United States v. Giordano, 416 U.S. 505 (1974)

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

United States v. Hufford, 539 F.2d 32 (9th Cir.), cert. denied, 429 U.S. 1002 (1976)

United States v. Kahn, 415 U.S. 143 (1974)

United States v. Karo, 468 U.S. 705 (1984)

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. London, 66 F.3d 1227 (1st Cir. 1995), cert. denied, 517 U.S. 1155 (1996)
United States v. Longoria, 177 F.3d 1179 (10th Cir.), cert. denied, 528 U.S. 892 (1999)

United States v. McIver, 186 F.3d 1119 (9th Cir. 1999), cert. denied, 528 U.S. 1177 (2000)

United States v. Moore, 562 F.2d 106 (1st Cir. 1977)

United States v. Petti, 973 F.2d 1441 (9th Cir. 1992), cert. denied, 507 U.S. 1035 (1993)

United States v. Thompson, 936 F.2d 1249 (11th Cir. 1991), cert. denied, 502 U.S. 1075 (1992)

United States v. Van Horn, 789 F.2d 1492 (11th Cir.), cert. denied, 479 U.S. 854 (1986)

United States v. Webster, 750 F.2d 307 (5th Cir. 1984), cert. denied, 471 U.S. 1106 (1985)

United States v. Yonn, 702 F.2d 1341 (11th Cir.), cert. denied, 464 U.S. 917 (1983)

SEARCHING AND SEIZING COMPUTERS

The Legal Division of the Federal Law Enforcement Training Center would like to express its gratitude to the United States Department of Justice Computer Crime and Intellectual Property Section of the Criminal Division for granting permission to liberally use and quote their publication *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. That publication was invaluable in preparing this student text, and many portions of this text were taken directly from that publication without change.

I. INTRODUCTION 163

II. PRIVATE SEARCHES 163

III. REASONABLE EXPECTATION OF PRIVACY 164
A. GENERALLY 164
B. LOSING REP IN A COMPUTER 165
1. Exposed to the Public 165
2. Stolen Computers 165
3. Third Party Possession 165

IV. EXCEPTIONS TO THE WARRANT REQUIREMENT 166
A. CONSENT 166
1. Requirements 166
2. Consent and Computers 167
a. the scope of a consent search 167
b. third party consent 168
c. implied consent 169
B. EXIGENT CIRCUMSTANCES 169
C. PLAIN VIEW 170
D. SEARCH INCIDENT TO ARREST 171
E. INVENTORY SEARCHES 173

V. PREPARING A SEARCH WARRANT 175
A. PLANNING AND EXECUTING THE SEARCH WARRANT 176
B. THE STEPS TO CONDUCT A COMPUTER SEARCH WITH A WARRANT 177
1. Step 1: Assemble a Team 177
2. Step 2: Special Information Needed 178
3. Step 3: Exactly What to Search for and Where 179
4. Step 4: The "Legal Role" of the Computer 180
a. the offense under investigation. 180
b. the independent component doctrine. 181
5. Step 5: Multiple Warrants (Network Searches) 183
6. Step 6: The Search Strategy 184
a. commingled file 186
b. hardware-only seizures 187
c. when seizure would bring down a network 188
d. data only searches 189
e. justifying off-site searches 189
f. justifying the seizure of hardware 190
g. conclusion 191
7. Step 7: Draft the Search Warrant and the Affidavit 191

VI. SPECIAL CONSIDERATIONS IN EXECUTING A SEARCH WARRANT TO SEARCH AND/OR SEIZE COMPUTERS 193
A. KNOCK AND ANNOUNCE 193
B. RETENTION OF SEIZED COMPUTERS 195

VII. AUTHENTICATION OF INFORMATION 196

VIII. SEEKING OR ENCOUNTERING PRIVILEGED INFORMATION 196
A. PRIVILEGED MATTERS 196
B. SEARCHING COMPUTERS OF DISINTERESTED PARTIES 197
C. PRIVILEGED FILES OF DISINTERESTED PERSONS 199
D. TARGETS 201

IX. PRIVACY PROTECTION ACT (PPA) MATERIALS. 201
A. PURPOSE AND STRUCTURE 201
B. WHAT THE PPA PROTECTS 202
C. EXCEPTIONS TO THE PPA 203

D. REMEDIES FOR VIOLATING THE PPA 204
E. APPLICATION OF THE PPA 204

Attachment A 206

Attachment B 208

Sample language for search warrants 208

I. DESCRIBING THE PROPERTY TO BE SEIZED 208

II. COMPUTER SEARCH AND SEIZURE AFFIDAVITS 212

CASE CITATIONS 224

I. INTRODUCTION

As with any search or seizure issue, the starting point when dealing with computer searches is the Fourth Amendment, which states:

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized.*

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. To summarize, the search of a computer without a warrant is acceptable in one of three potential situations. First, if the search is a private one, the Fourth Amendment is not violated. 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. 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.

II. PRIVATE SEARCHES

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.'" United States v. Jacobsen. 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. 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.

III. REASONABLE EXPECTATION OF PRIVACY IN COMPUTERS

A. GENERALLY

In Katz v. United States, 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. 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. 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.

B. LOSING 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.

1. Exposed to the Public

In Katz, 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.

2. Stolen Computers

Generally, an individual will not have a reasonable expectation of privacy in the contents of computers they have stolen. As one court has noted, "because expectations of privacy derive in part from 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…." United States v. Lyons.

3. Third Party Possession

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.

IV. EXCEPTIONS TO THE WARRANT REQUIREMENT

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

"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." Schneckloth v. Bustamonte.

1. Requirements

In order for a consent search to be valid, two requirements must be met. First, the consent must be given voluntarily (i.e., not coerced). In making this determination, courts will look at the "totality of the circumstances" surrounding the giving of the consent. 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 or proving that consent was voluntary. 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. 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.

2. 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?

a. the scope of a consent search

The scope of a search is generally defined by the consent given. An individual may limit the scope of any consent. In such a case, the scope of a consent search cannot exceed, either in duration of physical scope, the limits of the consent given. 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.

Computer cases often raise the question of whether consent to search a location or item implicitly includes consent to access computer memory or 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. 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. 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.

b. third party consent

It is common for several people to use or own the same computer equipment. If any of those people give 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. 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. Because the joint access test does not require a unity of interests between the suspect and the third party, however, Matlock permits third party consent, even when the target of the search is present and refuses to consent to the search. 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. Conversely, if the suspect has given the co-user the password or encryption key, then she probably has the requisite common authority to consent to a search of the files under Matlock. 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, regarding "apparent authority" to consent to a search.

c. implied consent

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. 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. Despite one federal circuit's broad construction (the Fifth Circuit Court of Appeals), 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. Absent such evidence, these courts have preferred to examine general waivers of Fourth Amendment rights solely under the reasonable-expectation-of-privacy test.

B. 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." United States v. Alfonso. In determining whether exigent circumstances exist, agents

should consider: (1) the degree of urgency involved, (2) the amount of time necessary to obtain a warrant, (3) whether the evidence is about to be removed or destroyed, (4) the possibility of danger at the site, (5) information indicating the possessors of the contraband know the police are on their trail, and (6) the ready destructibility of the contraband. 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. Of course, in computer cases, as in all others, the existence of exigent circumstances is absolutely tied to the facts. Importantly, 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. Accordingly, 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.

C. 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. Horton v. California. 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. Importantly, the plain view exception cannot justify violations of an individual's reasonable expectation of privacy. 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."

D. 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. In Robinson, the Supreme Court noted "two historical rationales for the search incident to arrest exception: (1) the need to disarm the suspect in order to take him into custody, and (2) the need to preserve evidence for later use at trial. Id. The permissible scope of a search incident to arrest was outlined by the Supreme Court in the 1969 case of Chimel v. California, where they held:

> *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.*

A search incident to arrest may only be conducted when two requirements have been met. First, there must have been a lawful custodial arrest. A search incident to arrest may not be conducted in a

situation where an actual arrest does not take place. The second requirement for a lawful search incident to arrest is that the search must be "substantially contemporaneous" with the arrest. Stoner v. California. Unfortunately, what exactly is meant by this phrase is open to interpretation. In United States v. Turner, the Ninth Circuit Court of Appeals stated that a search incident to arrest must be conducted "at about the same time as the arrest." 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 v. United States. 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. Among the factors to be considered in determining whether a search was "contemporaneous" with the arrest are where the search was conducted; when the search was conducted in relation to the arrest; and whether the defendant was present at the scene of the arrest during the search.

With regards to electronic storage devices, the issue of the proper scope of a search incident to arrest is not entirely clear. Due to the increasing use of handheld and portable computers and other electronic storage devices, agents often encounter these devices when conducting searches incident to lawful arrests. Turning first to electronic pagers, courts have analogized these devices to closed containers, recognizing that an individual has a reasonable expectation of privacy in an electronic pager. Nonetheless, as with other closed containers, that expectation of privacy can be intruded upon, either with a search warrant or with an exception to the warrant requirement. For this reason, courts have been consistent in allowing electronic pagers to be searched incident to a lawful arrest, relying primarily on two factors to justify their decisions: First, because of the finite nature of a pager's electronic memory, incoming pages may destroy currently stored telephone numbers in a pager's memory. Second, because merely turning off the power or touching a button can destroy the contents of some pagers, there is a potential

destruction of evidence issue. For both of these reasons, "it is imperative that law enforcement officers have the authority to immediately 'search' or retrieve, incident to a valid arrest, information from a pager in order to prevent its destruction as evidence." United States v. Ortiz.

However, courts have not yet addressed whether Robinson will permit warrantless searches of electronic storage devices that contain more information than pagers. Various court decisions have granted law enforcement officers the authority to search wallets, briefcases, and address books during a valid search incident to arrest. Thus, it could be argued that law enforcement officers should be able to search their electronic counterparts (such as electronic organizers, floppy disks, and Palm Pilots) as well. However, it seems unlikely that courts would permit such an extension for computers. The limit on this argument is that any search incident to an arrest must be reasonable. While a search of physical items found on the arrestee's person may always be reasonable, more invasive searches in different circumstances may violate the Fourth Amendment. For example, the increasing storage capacity of handheld and laptop computers suggests that Robinson's bright-line rule may not always apply in the case of electronic searches. Courts may conclude that a quick search through a pager that stores a few phone numbers is reasonable incident to an arrest, but that a very time-consuming search through a computer that contains an entire warehouse of information presents a different case. When in doubt, agents should obtain a search warrant before examining the contents of electronic storage devices that might contain large amounts of information.

E. INVENTORY SEARCHES

Inventory searches are a "well-defined exception to the warrant requirement of the Fourth Amendment." Colorado v. Bertine. Where evidence is found during a lawfully conducted inventory search, it may be used against the defendant in a later trial. In South Dakota v. Opperman, the Supreme Court outlined three justifications for allowing law enforcement officers to inventory lawfully impounded property without first obtaining a warrant. First, there is a need for law enforcement to

protect the owner's property while it remains in police custody. Second, an inventory protects the police against claims or disputes over lost or stolen property. And third, an inventory is necessary for the protection of the police from potential dangers that may be located in the property. There are two requirements for conducting a valid inventory search. First, because inventory searches are routine, non-criminal procedures whose justification does not hinge on the existence of probable cause, "the absence of a warrant is immaterial to the reasonableness of the search." Illinois v. Lafayette. Instead, to be reasonable under the Fourth Amendment, "an inventory must not be a ruse for a general rummaging in order to discover incriminating evidence. The policy or practice governing inventory searches should be designed to produce an inventory." Florida v. Wells.

In addition to being conducted for a non-investigatory purpose, a valid inventory search must also be conducted in accordance with a standardized inventory policy aimed at accomplishing the justifications for inventory searches. As stated 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.*

While the law enforcement agency involved must have a "standardized" inventory policy, several courts have upheld unwritten standardized policies. Nonetheless, as a practical matter, the best way for a law enforcement agency to avoid difficulty with this particular requirement would be to reduce their standardized inventory policy to writing. 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.

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. 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 intangible realm. Information does not generally 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.

V. SEARCHING WITH A WARRANT - SPECIAL CONSIDERATIONS IN PREPARING A SEARCH WARRANT TO SEARCH AND OR SEIZE COMPUTERS

Traditional searches differ from searches that target computers and data. In most searches, agents are looking for a particular physical item in a particular location. The search for electronic evidence is different. Because computer files 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.

The most significant difference between traditional and computer searches are that in computer searches, agents need to describe where and how the search is to be conducted. In addition, seizing an entire computer or a computer network can effectively close down a business, and judges will consider this factor in deciding whether to issue a search warrant.

A. SPECIAL CONSIDERATIONS IN PLANNING AND EXECUTING A COMPUTER SEARCH WARRANT

While it is always essential to plan prior to obtaining and executing a search warrant, planning computer searches is critical. Here are some special factors in computer searches.

* Special assistance from computer experts is often required to execute the search. (Title 18 U.S.C. § 3105).

* It is often difficult to identify what is to be searched for with particularity. Are agents looking for images, e-mails, spreadsheets, letters, documents, databases or just the computer hardware? Is the data on the hard drive, or some other storage media such as a Jazz or Zip drive, removable hard drive, CD, floppy diskette, or even remotely stored on the Internet or a network?

* Whether the hardware or data is the fruit, instrumentality, or evidence of crime, or contraband, can dictate how agents can execute a search and where the search may be executed.

* Agents may be required to search a computer on-site without removing it to another location. In other situations, agents may be able to remove the computer to another location to search it.

* Agents may not know upon which of many computers - or even which network server located outside the judicial district - the data is located.

* Just as in traditional searches, agents may be allowed to conduct a no-knock search.

* Even with the data in hand, agents will have to develop evidence that connects the target to the data.

* Certain data is given special statutory protection if it is privileged or because of 1st Amendment concerns. If agents are looking for, or encounter, that data, special precautions are required.

B. THE STEPS TO CONDUCT A COMPUTER SEARCH WITH A WARRANT

This section describes the steps agents need to take to effectively conduct a computer search. The reader may wish to consult Attachment A to this chapter that outlines the steps and what the steps accomplish.

1. Step 1: Assemble a Team to Plan and Execute the Search

Computer searches require a team with three important players: the agent, the prosecutor, and a technical specialist with expertise in computers and computer forensics. Each member of the team must work with the others to ensure an effective and lawful search.

The case agent organizes and directs the search, learns as much as possible about the computers to be searched, and drafts the affidavit establishing probable cause.

The technical specialist explains the technical limitations that govern the search to the case agent and prosecutor, creates the plan for executing the search, and, in many cases, takes the lead role in executing the search itself.

The prosecutor reviews the affidavit and warrant and ensures that the entire process complies with the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure.

A computer forensics expert is essential to planning the warrant. The technical expert should also accompany the search team or, at a minimum, be available on immediate call.

During execution of the search, agents must comply with Title 18 U.S.C. Section 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.*

Violating this statute can subject agents to civil liability.

If a computer forensics expert will participate in the search, name the person in the warrant or state that one will be needed to aid in the search. Except in all but the simplest case, a forensics expert should be consulted in planning the search, obtaining the warrant, and be present or on call during the execution of the search. The expert law enforcement uses does not himself or herself need to be a law enforcement officer.

2. Step 2: Collect Special Information Needed in Most Computer Searches

Computer searches require having certain technical information so agents know where to search. At a minimum, agents must know:

a. What types of computers and operating systems are involved?

b. What types of software does the suspect use?

c. Is the computer connected to a network? Where is the computer network server located?

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

e. Does the computer contain information that might be privileged or protected by the Privacy Protection Act?

Gathering this information may involve an interview of the system administrator of the targeted network and those familiar with the network. This might be done in an undercover capacity. On-site visits (often undercover) may also reveal important information about the hardware involved. A useful source of information about networks connected to the Internet is the Internet itself.

3. Step 3: Determine Exactly What to Search for and Where the Evidence is Located

The 4th 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***." The 4th Amendment's particularity requirement applies to the searches of computers and the data contained on them.

In some, but not many computer searches, what agents want to seize are the actual computer and other hardware and components. That would be the case where the computer is stolen property or purchased with illegally obtained funds. Searching for computers and other hardware and components might also be the objective of the search where the computer was the means of committing a crime, such as where a computer was used to prepare a letter, spreadsheet, or send an e-mail.

In most computer searches, the objective of the search is not to search *for* computers or hardware, but to search *in and on computers for data*. 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.

The difference between a data search and a search for only the computers is significant. For example, if agents want to seize only the computer, it is generally enough to describe the items that the agents have probable cause to seize. If, however, the agents want to seize the computer and search for data, then the agents will have to describe what ***in or on*** the computer they have probable cause to search for and seize, and where they want to look for that data.

4. Step 4: Determine the "Legal Role" of the Computer

To satisfy the particularity requirement, agents must know two concepts: the "legal role" of the computer and the independent component doctrine.

a. The "legal role" of the computer in the offense under investigation.

F.R.C.P. 41(b) provides categories of evidence that law enforcement may seize. Knowing the proper category or categories is important in crafting the warrant and executing it. Those categories are:

* Contraband, the fruits of crime, or things otherwise criminally possessed.

* Property designed or intended for use of or which is or has been used as the means of committing a criminal offense (generally referred to as "instrumentalities.").

* Property that constitutes evidence of the commission of a criminal offense.

To know which of the FRCP 41(b) categories apply, agents should determine the role of the computer in a crime. Practically speaking, the computer can fall into two general categories:

* The computer itself is contraband, evidence, an instrumentality, or a fruit of crime, or

* The computer is an electronic filing cabinet that stores evidence (data) of a crime. For example, if a suspect keeps evidence of his fraud schemes stored in his personal computer, the hardware itself is merely a container for evidence, just as a filing cabinet is to paper documents.

b. the independent component doctrine.

Understanding the independent component doctrine is essential so agents can: describe with particularity what agents are looking for; comply with the requirements of F.R.C.P. 41(b) as to the types of evidence agents may search for; determine the scope of the search; and otherwise draft and execute a proper warrant.

To say that agents want to search or seize a “computer” can be both too broad and too narrow. It rarely meets the 4th Amendment particularity requirement. Instead, agents must view each component of a computer independently and develop probable cause for each.

To illustrate the dangers of not looking at each component independently, suppose an agent has a warrant to search the suspect's "computer" (not further identified.) Does this warrant authorize a search or seizure of the monitor, keyboard, mouse, printers, and peripheral storage devices, such as hard and Zip drives, CD drives, scanners and the like? More importantly, does this warrant authorize seizing floppy diskettes, data CDs, software, or other items not connected or considered

a part of a computer?

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. Some examples are helpful.

* ***Peripheral devices***. If searching for data and the computer must be removed off-site to conduct the search, is there probable cause to seize the monitor and the keyboard? Often such seizure is justified if the particular monitor or keyboard is necessary to make the computer operate properly. In the case of peripheral devices (those connected to the computer, but not inside the computer's case), the computer forensics expert may not be able to read the peripheral storage disk or CD unless the peripheral device itself is available.

* ***Printers***. If looking for data, it may not be necessary to seize the printer. On the other hand, if agents wish to determine if a specific printer printed a document, the agents would need to seize the printer.

* ***Passwords, notes, and log ins***. In a search for data, agents may need to search for and seize computer files or papers that might contain passwords, logins and other information that might assist in finding, accessing, or interpreting data. The same may be true about computer files or papers that contain the names, e-mail addresses, or other identifying data of confederates.

* ***Software instructions and original copies of software***. In searching for data, it may be necessary to search for and seize original software and software manuals so agents conducting the search of the computer can know how the software works. Knowing about any encryption and software keys may be required to use the computer or software. Computer software often requires the original software to

perform some functions.

At the conclusion of this step, the search team should be able to articulate, with particularity:

- Exactly what the agents have probable cause to seize. Describe the hardware, the hardware components, and/or the data to be seized. (From Step 3)

- In the case of data, where in or on the computer - or upon which component - the evidence is located.

- The F.R.C.P. 41(b) category (fruits, contraband, instrumentalities, or evidence) into which the evidence falls.

- Agents may discover that in the case of a search for data, the data might not be all in the same judicial District. This issue will be addressed next.

5. Step 5: Determine if There is a Need for Multiple Warrants (Network Searches.)

Under Federal Rule of Criminal Procedure 41(a), a Federal judge or a judge of a state court of record may issue a search warrant for property located within the District. A Federal judge may also issue a search warrant for property located within or outside the District if the property is within the District when the warrant is sought but might move outside the District when the warrant is executed.

In the electronic evidence world, this rule would require agents to obtain warrants or court orders in each District where electronic evidence was stored. This would be the case if a person was storing electronic evidence on computers in another District or the email computer (server) was located outside the District.

The USA Patriot Act amended 18 U.S.C. Section 2703 to eliminate the need to obtain multiple warrants for stored wire or electronic communications. Now such a warrant can be issued "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant."

Under this change, if a suspect in the Eastern District of Virginia was stealing credit card numbers from the Internet in Virginia, used an email computer (server) in California to handle his email, and backed up his incriminating files on a computer server in Texas, a Federal judge in the Eastern District of VA could issue a search warrant for wire or electronic communications in Virginia, California, and Texas. Depending on the nature of the crime, Federal judges in other Districts where there is venue could issue the same warrant.

If there is doubt whether the court to which the law enforcement officer presents a warrant is one "with jurisdiction over the offense under investigation," agents should seek warrants in each District where there is probable cause evidence is located.

This provision expires on December 31, 2005.

6. Step 6: Determine the Search Strategy

Perhaps the most unique aspect of a computer search warrant is the need, in most cases, to describe how the search will be executed. Ordinarily, agents would only provide the issuing Magistrate Judge with what they want to look for, where they want to look, and the probable cause to look for it. In a computer search warrant, agents will often need to explain why an off-site search is required and the method used to search for data. Specifically, agents may need to explain:

- Will the search be conducted at the location where the computers are, or will the computers be moved off-site to be searched?

- Why is an off-site search necessary? If a data only search, what are the reasons why the computers may have to be searched off-site? Why cannot the computers be searched on-site, and left in place, so the owner can continue to use them? If an on-site search for data is planned, under what circumstances would the agents need to remove the computer off-site to do or complete the search?

- What will be done to minimize the disruption of an on going business while searching the computer?

- What will be done to minimize searching through those files that are not within the scope of the search warrant?

If agents expect that they may need to seize a personal computer and search it off-site to recover the data, the affidavit should explain this expectation and its basis to the magistrate judge informing the court of the practical limitations of conducting an on-site search and articulating the plan to remove the entire computer from the site if it becomes necessary. The affidavit should also explain what techniques the agents expect to use to search the computer for the specific files that represent evidence of crime and may be intermingled with entirely innocuous documents. If the search strategy has been influenced by legal considerations, such as potential Privacy Protection Act liability, the affidavit should explain how and why in the affidavit.

Although no particular language is required, Appendix F of the DOJ CCIPS Handbook, January 2001, offers sample language that agents may find useful in many situations. (See Attachment B)

The reasons for articulating the search strategy in the affidavit are both practical and legal. On a practical level, explaining the search

strategy creates a document that both the court and the agents can read and refer to as a guide to the execution of the search. Nat'l City Trading Corp. v. United States ("[W]e note with approval the care taken by the Government in the search involved here. . . . Such self-regulatory care [in executing a warrant] is conduct highly becoming to the Government."). Similarly, if the explanation of the search strategy is made an attachment to the warrant and given to the subject of the search pursuant to Rule 41(d), the explanation permits the owner of the searched property to satisfy himself during the search that the agents' conduct is within the scope of the warrant. Michigan v. Tyler (noting that "a major function of the warrant is to provide the property owner with sufficient information to reassure him of the entry's legality").

As a legal matter, explaining the search strategy in the affidavit helps to counter defense counsel motions to suppress based on the agents' alleged "flagrant disregard" of the warrant during the execution of the search. If agents execute a warrant and seize additional property not described in the warrant, defense counsel can file a motion to suppress the additional evidence. If the motion is successful, only the property not named in the warrant is suppressed. On the other hand, defense counsel will often attempt to use the seizure of additional property as the basis for a motion to suppress all of the evidence obtained in a search. To be entitled to the extreme remedy of blanket suppression, the defendant must establish that the seizure of additional materials proves that the agents executed the warrant in "flagrant disregard" of its terms. United States v. Le and United States v. Matias. Defense lawyers often argue that by seizing more than the specific computer files named in the warrant, the agents "flagrantly disregarded" the seizure authority granted by the warrant, and everything seized should be suppressed.

a. commingled file issues

Evidence that is to be searched for as indicated in the warrant may be commingled with data and files that have no relation to the crime

under investigation. When agents expect that the files described in the warrant will be commingled with innocent files outside of the warrant's scope, it is a good practice, if technically possible, to explain in the affidavit how the agents plan to search the computer for the targeted files.

When agents have a factual basis to believe that they can locate the evidence using a specific set of techniques, the affidavit should explain the techniques that the agents plan to use to distinguish incriminating documents from commingled ones. Consult with experts in computer forensics to determine what kind of search can be conducted to locate the particular files described in the warrant.

In many cases, a narrow approach will be technically impossible. The targeted files may be mislabeled, hidden, oddly configured, written using code words to escape detection, encrypted, or otherwise impossible to find using a simple technique, such as a "key word" search. Because some judges may fail to appreciate such technical difficulties, it is a good practice for agents to discuss these issues in the affidavit if it appears that a narrow search will not be effective. In such cases, a more extensive search through innocent files will be necessary to determine which files fall within the scope of the warrant. Explaining these practical needs in the affidavit can make clear at the outset why an extensive search will not be in "flagrant disregard" of the warrant, and why the extensive search complies fully with traditional Fourth Amendment principles.

b. hardware-only seizures

If the hardware is itself evidence, an instrumentality, contraband, or a fruit of the crime, agents will usually plan to seize the hardware and search its contents off-site.

Under Fed. R. Crim. P. 41(b), agents may obtain search warrants to seize computer hardware if the hardware itself is contraband, evidence, or an instrumentality or fruit of the crime. When the hardware itself may be seized according to Rule 41, agents will usually conduct the search by seizing the computer and searching it off-site. For example, a home

personal computer used to store and transmit contraband images is itself an instrumentality of the crime. Davis v. Gracey and United States v. Lamb. Accordingly, Rule 41 permits agents to obtain a warrant authorizing the seizure of the computer hardware. When agents have probable cause to seize hardware because it is evidence, contraband, or an instrumentality of crime, the warrant will ordinarily describe the property to be seized as the hardware itself. In many of these cases, however, the agents will plan to search the hardware after it is seized for electronic data stored inside the hardware that also constitute evidence or contraband. It is a good practice for agents to inform the magistrate of this plan in the supporting affidavit.

In some cases, agents may be allowed be seize the hardware under circumstances that would not automatically allow a search of the entire computer without also a search warrant. For example, the computer may be stolen (making it either fruits of a crime, contraband, or evidence of crime) but the person from whom it was seized may have innocently obtained the computer. To search the computer in those circumstances may require a separate warrant. The analogy to a non-computer case would be if a person stole a filing cabinet, a search warrant to seize the cabinet would probably not include the files the thief has stored in it unless there was probable cause to examine those files.

c. when seizure would bring down a network

When the "computer" involved is not a stand-alone PC, but rather part of a complicated network, seizing the entire network may not be feasible or legally possible. For example, if a system administrator of a computer network stores stolen proprietary information somewhere in the network, the network becomes an instrumentality of the system administrator's crime. Technically, agents could obtain a warrant to seize the entire network. However, bringing down the entire network might cripple a functioning business and disrupt the lives of many employees. In such circumstances, agents will want to take a more practical and less

intrusive approach to obtain the evidence they need.

d. data only searches

If the hardware is merely a storage device for evidence, agents generally will only seize the hardware if less disruptive alternatives are not feasible.

The strategy for conducting a computer search is significantly different if the computer hardware is merely a storage device for evidence of a crime. In such cases, Rule 41(b) authorizes agents to obtain a warrant to seize the electronic evidence, but arguably does not authorize the agents to seize the hardware that happens to contain that evidence because the hardware is merely a storage container for evidence, not evidence itself.

The general strategy is to pursue the quickest, least intrusive, and most direct search strategy that is consistent with securing the evidence described in the warrant. This strategy will permit agents to search on-site in some cases, and will permit them to seize the computers for off-site review in others. Flexibility is the key.

e. justifying off-site searches

Justifying off-site searches when searching for data only; when off-site searches are permitted when the computer is only a container for evidence.

When the computer is just a storage device, it doesn't always mean the government is prevented from seizing the equipment. It only means that the government generally should only seize the equipment if a less intrusive alternative that permits the effective recovery of the evidence is infeasible in the particular circumstances of the case. United States v. Tamura. Circumstances will often require investigators to seize equipment and search its contents off-site. It is essential that if the computer is just a storage device, but agents intend to search it off-site, this be made clear in

the warrant application and justified. In other cases, the plan may be to search on-site but the situation dictates it is safer or wiser to bring the computer to a lab. For example, agents seeking to obtain information stored on the computer network of a functioning business will in most circumstances want to make every effort to obtain the information without seizing the business's computers, if possible.

f. justifying the seizure of hardware

Notwithstanding the agent's efforts, a search for data alone may still allow an off-site search for the following reasons:

- 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

- Lack of on-site technical expertise. Attempting to search files on-site may even risk damaging the evidence itself. 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.

- 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.

- 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.

In light of these uncertainties, agents often plan to try to search on-site, with the understanding that they will seize the equipment if circumstances discovered on-site make an on-site search infeasible. Once on-site to execute the search, the agents will assess the hardware, software, and resources available to determine whether an on-site search is possible. In many cases, the search strategy will depend on the sensitivity of the environment in which the search occurs.

g. conclusion

Whatever search strategy is chosen, it should be explained fully in the affidavit supporting the warrant application. Sometimes, conducting a search on-site will be possible. A friendly employee or system administrator may agree to pinpoint a file or record or may have a recent backup, permitting the agents to obtain a hard copy of the files they seek while on-site. Alternatively, agents may be able to locate the targeted files and make electronic copies, or may be able to mirror a segment of the storage drive based on knowledge that the information exists somewhere within that segment of the drive. In other cases, of course, such strategies will fail. If the agents cannot learn where the information is stored or cannot create a working mirror image for technical reasons, they may have no choice but to seize the computer and remove it.

7. Step 7: Draft the Search Warrant and the Affidavit

With the information developed on the previous six steps, the team will have determined the facts and the search strategy. With the exception of including the search strategy in the affidavit itself, assembling the warrant application and affidavit is essentially the same as a traditional warrant. Below is a list of some considerations as a reminder of those differences between a computer and a traditional search warrant.

1) If the computer is contraband, evidence, fruits, or instrumentalities of crime, describe the hardware itself. Remember the independent component doctrine - describe each component and state the probable cause for each.

2) If probable cause relates only to the data, the warrant should describe the data to be seized and that search and seizure of the computer is necessary to get to the data. Indicating that agents want to only seize the computer does not necessarily get them to the data. The warrant should describe the information based on its content (e.g., gambling records, evidence of a fraud scheme), and then request the authority to seize the information in whatever form the information may be stored.

3) If there is probable cause to seize passwords, manuals, software, ID numbers, customer lists, lists of confederates and the like, describe what is to be seized and the probable cause to seize it.

4) When conducting a search for data, agents need to consider exactly what information they need. The information may be very narrow (e.g., a specific record or report), or quite broad (e.g., thousands of records relating to an elaborate fraud scheme). The warrant should describe the information to be seized, and then request the authority to seize the information in whatever form it may be stored (whether electronic or not).

5) 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.

6) Compare the probable cause in the warrant with the list of things to be seized. For example, in a data warrant, ensure you haven't included probable cause for just the hardware. In a warrant for hardware, ensure you haven't included probable cause that goes only to the data.

7) If there is probable cause to find the data in either electronic or paper form, indicate you wish to search for both.

8) Remember to explain both the search strategy and the practical considerations underlying the strategy in the affidavit to include:

- Why an off-site search is required.
- What techniques the agents expect to use to search the computer for the specific files that represent evidence of crime that may be intermingled with entirely innocuous documents.
- Explain how the agents plan to search the computer for the targeted files without unnecessarily accessing innocent files.
- If an on-site search is planned, but there is the possibility that an off-site search may be required depending on the facts as they develop on the scene, indicate the factors that might convert an on-site search to an off-site one.

VI. SPECIAL CONSIDERATIONS IN EXECUTING A SEARCH WARRANT TO SEARCH AND/OR SEIZE COMPUTERS

A. KNOCK AND ANNOUNCE

Federal officers are required to comply with the "knock and announce" statute set out in Title 18 U.S.C. Section 3109 which states:

> *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.*

This statute requires agents to announce their presence and authority prior to executing a search warrant. Complying with the statute reduces the risk of violence and destruction of property when agents execute a search.

The rule is not absolute. In Richards v. Wisconsin, 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.*

The time between when an agent announces his presence until that reasonable period the target opens the door may leave sufficient time to destroy a lot of evidence. Technically adept suspects may "hot wire" their computers in an effort to destroy evidence using "hot keys" that destroy evidence with a keystroke combination. In many cases, turning off the computer can destroy some evidence especially the file the user was working on at the time of the shut down.

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. 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.

For example, if while approaching a residence with a warrant to search for data officers develop reasonable suspicion their presence has been detected and that persons inside will destroy (delete) the data, such facts may excuse compliance with the knock and announce statute.

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." Richards.

B. TIME FRAMES GOVERNING RETENTION OF SEIZED COMPUTERS

The forensic examination of seized computers can take months to complete because computers can 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.

Unfortunately, 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 - in one case, as short as seven days. 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. 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.

VII. SPECIAL ISSUES INVOLVING AUTHENTICATION OF INFORMATION CONTAINED ON COMPUTERS

Refer to the Courtroom Evidence chapter that has a section specifically addressing this issue.

VIII. SEEKING OR ENCOUNTERING PRIVILEGED INFORMATION

A. PRIVILEGED MATTERS

Certain communications between an attorney and client, and between a member of the clergy and their communicants, are privileged. In addition, under DOJ policy, the communications between physicians and their patients (and not just between psychotherapists and their patients) are given a privileged status.

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.

Agents must ensure that the search will not violate the Attorney General's regulations relating to obtaining confidential information from

disinterested third parties, and they should devise a strategy for reviewing the seized computer files following the search so that no breach of a privilege occurs.

B. SEARCHING COMPUTERS OF DISINTERESTED PARTIES

The law permits 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.

1) 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. Title 42 U.S.C. § 2000aa-11(a); 28 C.F.R. § 59.4(b).

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. The regulation does contain a narrow exception. A search warrant can be used if:

- ⇨ Using less intrusive means would substantially jeopardize the availability or usefulness of the materials sought (subpoenas are less intrusive);

- ⇨ Access to the documentary materials appears to be of substantial importance to the investigation; and

- ⇨ The application for the warrant has been recommended by the U.S. Attorney and approved by the appropriate Deputy Assistant Attorney General.

28 C.F.R. 59.4 lists many factors to decide whether a subpoena or other means must be used before obtaining a search warrant is attempted. Those factors revolve around the following concepts:

1) Whether using a subpoena or other alternative that gives advance notice would be likely to result in the destruction, alteration, concealment, or transfer of the materials sought. In this regard, agents may consider:

- ⇨ Whether a suspect has access to the materials to include the relationship between the suspect and those possessing the materials sought;

- ⇨ 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; or

- ⇨ 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.

2) The immediacy of the government's need to obtain the materials considering:

- ⇨ Whether immediate seizure is necessary to prevent injury to persons or property or to preserve their evidentiary value;
- ⇨ Whether delay would significantly jeopardize an ongoing investigation or prosecution; or
- ⇨ Whether a legally enforceable form of process, other than a search warrant, is reasonably available as a means of obtaining the materials.

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.

C. 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.

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 will comb through the files vary widely among different courts. There are three options.

1) 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.

2) 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 long time to accomplish, and prosecutors try to avoid this process.

3) 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 quickly. 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.

Although no single standard has emerged, the 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.

D. TARGETS

If the person who holds the documents sought is not "disinterested" but 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. 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 methods to locate only the material described in the warrant.

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.

IX. SEEKING OR ENCOUNTERING PRIVACY PROTECTION ACT MATERIALS - TITLE 42 U.S.C. SEC. 2000AA.

A. THE PURPOSE AND STRUCTURE OF THE PRIVACY PROTECTION ACT (PPA.)

The PPA was passed due to 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. The purpose of this statute is to limit searches for materials held by persons involved in First Amendment activities **who are not themselves suspected of participation in the criminal activity for which the materials are sought.** The statute is not intended to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing a crime.

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.

B. WHAT THE PPA PROTECTS

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:

"Work product" materials, which means the materials:

- ⇨ Were prepared, produced, authored, or created "in anticipation of communicating such materials to the public," (newspaper, books, broadcasts, or similar forms of public

communication.),

- ⇨ Include "mental impressions, conclusions, or theories" of its creator; and

- ⇨ 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,"

Examples of PPA/Work Product materials include: a newspaper article the creator intends to have published (draft or final); a web page the creator intends to post to the Internet; a speech a person intends to give on radio or TV; a letter to the editor the creator intends to send to his local newspaper; a draft of a newsletter to fellow members of the local garden club.

"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 .." and which:

- ➔ Contain information, and

- ➔ Are possessed by a person "in connection with a purpose to disseminate to the public" some form of "public communication."

C. EXCEPTIONS TO THE PPA

1) Contraband, instrumentalities, or the fruits of a crime.

2) There is reason to believe that the immediate seizure of such materials is necessary to prevent death or serious bodily injury.

3) 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) 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.

Examples applying the exceptions when the target's computer contains: child pornography images for posting on the Internet or in a magazine (contraband); a web page or newsletter promoting a fraud scheme; or an advertisement to sell software to manufacture false identification documents.

D. 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.

E. APPLICATION OF THE PPA TO COMPUTER SEARCHES AND SEIZURES

PPA issues arise in computer cases because of the widespread 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 their computer.

In addition, PPA issues arise frequently in computer cases because 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. For example, 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.

Some courts have decided that the PPA language "to which the materials relate" to be quite broad and will allow incidental seizures of PPA materials. 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). Other courts have not been so generous. In Steve Jackson Games, Inc. v. Secret Service, 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") during a search relating to probable cause a person on SJG's computer network was involved in a hacking incident.

Agents 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.

ATTACHMENT A

Steps	Product / Issues
1: Assemble a team to plan and execute the search	Identity the agent, AUSA and the computer technician/expert that will draft the warrant and oversee/execute the search. Assign roles to each. Remember to designate non-LEOs that are needed to execute the warrant.
2: Collect special information needed in most computer searches	Through undercover work as necessary, determine the types of equipment, software, and network environment the target uses. This information is critical to determine where the evidence might be located.
3: Determine exactly what to search for and where the evidence is located.	**A**. Satisfy the 4th Amendment particularity requirement. What exactly are agents looking for (the hardware, the data, or both) and where is the data and hardware located? **B**. In data searches, where do the agents want to look for the data? Which computer(s)? On a network?
4: Determine the "legal role" of the computer	**A**. Is what agents want to look for contraband, or evidence, fruits, instrumentalities or evidence of crime? Which category will affect the search strategy. **B**. Searching a "computer" or "network" may not be sufficiently particular to meet 4th Amendment requirements. Identify the components to be searched or seized.
5: Determine if there is a need for multiple warrants (Network Searches.)	If evidence agents want to search for is located in more than one district (because it is on a network or the Internet), ensure the judge is one with "jurisdiction over the offense under investigation."

6: Determine the search strategy.	**A**. This is what makes a computer search different from a traditional one. **B**. Determine if agents can search on site or must they remove the computer off-site to search. **C**. If seizing hardware, do agents need a warrant to search the computer or data media? **D**. If a data only search, justify why the search cannot be conducted on-site. **E**. If the plan is to search on-site, what might occur that would require an off-site search? **F**. Can you convince the Judge that seizing the hardware to search off-site is justified if such a seizure would disrupt a business or bring down a network? **G**. How will agents conduct the search to stay within the scope of the warrant and avoid seizing and reviewing innocent files that are commingled with targeted files? **H**. Is the search strategy drawn broadly enough to accomplish the objective of the search but not so broadly that it would be in "flagrant disregard" of the scope of the search?
7: Draft the search warrant and the affidavit.	With the facts and strategy from the previous steps, draft the warrant. Include the factors and factors from this list.

ATTACHMENT B
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. 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), 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) (cash obtained in drug transaction), and stolen goods. See United States v. Burkeen, 350 F.2d 261, 264 (6th Cir. 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 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 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 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, 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 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, 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, 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?

CASE CITATIONS

Chimel v. California, 395 U.S. 752 (1969)

Colorado v. Bertine, 479 U.S. 367 (1987)

Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997)

Florida v. Wells, 495 U.S. 1 (1990)

Horton v. California, 496 U.S. 128 (1990)

Illinois v. Lafayette, 462 U.S. 640 (1983)

Illinois v. Rodriguez, 497 U.S. 177 (1990)

Katz v. United States, 389 U.S. 347 (1967)

Michigan v. Tyler, 436 U.S. 499, 508 (1978)

Nat'l City Trading Corp. v. United States, 635 F.2d 1020, 1026 (2d Cir. 1980)

Preston v. United States, 376 U.S. 364 (1964)

Richards v. Wisconsin, 520 U.S. 385 (1997)

Schneckloth v. Bustamonte, 412 U.S. 218 (1973)

South Dakota v. Opperman, 428 U.S. 364 (1976)

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)

United States v. Alfonso, 759 F.2d 728 (9th Cir. 1985)

United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996)

United States v. Le, 173 F.3d 1258 (10th Cir. 1999) and United States v. Matias, 836 F.2d 744 (2d Cir. 1988)

United States v. Lyons, 992 F.2d 1029 (10th Cir. 1993)

United States v. Matlock, 415 U.S. 164 (1974)

United States v. Ortiz, 84 F.3d 977 (7th Cir. 1996)

United States v. Robinson, 414 U.S. 218 (1973)

United States v. Tamura, 694 F.2d 591 (9th Cir. 1982)

United States v. Turner, 169 F.3d 84 (1st Cir. 1999)

COURTROOM EVIDENCE

I. INTRODUCTION 229
A. FORMS OF EVIDENCE 230
1. Testimonial 230
2. Real 230
3. Demonstrative 230
B. ADMISSIBILITY 230
C. THE FEDERAL RULES OF EVIDENCE (FRE) 231

II. THE PROCEDURAL STAGES OF A CRIMINAL TRIAL 231
A. SUPPRESSION HEARINGS (MOTIONS HEARINGS) 231
B. VOIR DIRE 231
C. OPENING STATEMENTS BY COUNSEL 232
D. THE CASE IN CHIEF 232
E. THE DEFENSE CASE 232
F. THE REBUTTAL CASE 232
G. CLOSING ARGUMENT 233
H. THE CHARGE TO THE JURY 233
I. SENTENCING 233
J. POST-TRIAL PROCEEDINGS 233

III. RELEVANT EVIDENCE 233
A. THE REQUIREMENT FOR EVIDENCE TO BE RELEVANT 233
B. WHEN RELEVANT EVIDENCE IS NOT ADMISSIBLE 234
C. OTHER CRIMES, WRONGS, AND ACTS OF THE DEFENDANT 235
1. Motive 235
2. Intent 235
3. Knowledge 235
4. Plan or Preparation 235
5. Opportunity to Commit the Crime 236
6. Modus Operandi 236
7. Identity of the Perpetrator 236
8. Impeachment 236
9. Predisposition 236

IV. DIRECT AND CIRCUMSTANTIAL EVIDENCE 236

V. LAY (AND EXPERT) WITNESS TESTIMONY 237
A. HANDWRITING 238
B. VOICE 238
C. EMOTIONAL CONDITION 238

VI. WITNESS CREDIBILITY AND IMPEACHMENT 238
A. IMPEACHMENT 239
B. FACTORS THAT AFFECT A WITNESS' CREDIBILITY 239
1. Bias 239
2. Motive to Fabricate Testimony 240
3. Inability to Observe or Accurately Remember 240
4. Contradiction 240
5. Prior Inconsistent Statements 241
6. Character for Truthfulness 241
7. Specific Instances of Conduct 241
8. Prior Convictions (FRE 609) 241
9. Character (opinion or reputation) (FRE 404(a)) 242

VII. PRIVILEGES 242
a. HOLDERS OF A PRIVILEGE 243
B. WAIVER OF PRIVILEGES 243
C. PRIVILEGES AND THE RULES OF EVIDENCE 243
D. THE FEDERAL PRIVILEGES 244
E. NON-FEDERALLY RECOGNIZED PRIVILEGES 244
F. THE ATTORNEY-CLIENT PRIVILEGE 245
G. THE HUSBAND-WIFE PRIVILEGES 246
H. THE PSYCHOTHERAPIST-PATIENT PRIVILEGE 247
I. THE CLERGY-COMMUNICANT PRIVILEGE 247
J. THE GOVERNMENT-INFORMANT PRIVILEGE 248

VIII. EVIDENTIARY FOUNDATIONS 249
A. LAYING A FOUNDATION 250
B. MARKING/TAGGING EVIDENCE 250
C. CHAIN OF CUSTODY 250
D. PRESERVING TRACE EVIDENCE CHARACTERISTICS 251
E. CONDITION OF THE EVIDENCE AT THE TIME OF TRIAL 251

IX. HEARSAY 252
A. HEARSAY DEFINED 252

B. HEARSAY EXAMPLES 253
C. APPLICABILITY OF THE HEARSAY RULE..... 253
D. REASON FOR THE HEARSAY RULE..... 253
E. WHAT IS A STATEMENT?..... 253
F. "TRUTH OF THE MATTER ASSERTED" 254
G. NON-HEARSAY..... 254
1. Statements of the Defendant..... 254
2. Other Statements 254

X. EXCEPTIONS TO THE HEARSAY RULE..... 254
A. "EXCITED UTTERANCES"..... 255
B. STATEMENTS FOR PURPOSES OF MEDICAL DIAGNOSIS OR TREATMENT 255

XI. STATEMENTS, REPORTS AND TESTIMONY 256

XII. BUSINESS RECORDS AND PUBLIC DOCUMENTS 257
A. THE BEST EVIDENCE RULE (FRE 1001; 1002) 257
1. An "Original" 257
2. "Duplicates" 257
B. SELF-AUTHENTICATION..... 258
1. Public Records and Documents..... 258
2. Business Records..... 258
C. HEARSAY ISSUES 259

XIII. AUTHENTICATING COMPUTER INFORMATION 259
A. INVOLVING COMPUTER FORENSICS EXPERTS 259
B. RULES OF EVIDENCE ISSUES 260
C. ADMISSIBILITY OF DIGITAL EVIDENCE..... 260
D. THE BEST EVIDENCE RULE 261
E. HEARSAY ISSUES 261

I. INTRODUCTION

Evidence is the backbone of every criminal prosecution. Unless evidence is properly collected, preserved, and presented, the evidence will not be admissible in court, and the jury cannot consider it no matter how important or powerful it may be. To ensure that evidence is collected and preserved in a way that it can be admitted, Law Enforcement Officers (LEOs) must have a general appreciation of some fundamentals of the Federal Rules of Evidence (FRE).

The jury decides what to do with the evidence and how much weight - consideration - to give it. The jury may consider the evidence as powerful proof or they might disregard it all together. Collecting evidence in a way that it complies with the Federal Rules of Evidence also makes the evidence more convincing and more likely the jury will give it the weight it deserves.

Even when evidence is to be used primarily by administrative decision-makers, the FREs are still important. Evidence that is collected and preserved consistent with the Federal Rules of Evidence standards is more helpful to agency decision-makers because the evidence is more reliable.

The law enforcement community uses the word "evidence" in many ways. "Go out and get some evidence that proves this." "What evidence do you have that the defendant did that." For our purposes, evidence refers to anything that either side - the prosecution or the defense - offers in court to prove or disprove something. Rarely does a single piece of evidence completely prove or disprove anything.

A. FORMS OF EVIDENCE

Evidence comes in several forms:

1. Testimonial

A witness takes the stand, is placed under oath, and answers questions.

2. Real

Real evidence is physical - it is something you can actually touch. Items that are found, collected, seized or otherwise obtained become exhibits and can be offered into evidence. Guns, drugs, or documents, are common forms of real evidence. Real evidence will be given an exhibit number when offered into evidence (Prosecution Exhibit ___; Defense exhibit: ____).

3. Demonstrative

This consists of items that demonstrate or illustrate something to the jury such as models, charts, and graphic aids.

B. ADMISSIBILITY

The judge decides the admissibility of the evidence. The jury decides what weight to place on it. When evidence is offered, the other party may object. If the objection is overruled, the evidence is received and the jury may consider it in deciding the verdict. If the objection is sustained, the evidence is not admitted and the jury may not consider it. The judge applies the FREs in deciding whether to admit evidence.

C. APPLICABILITY OF THE FEDERAL RULES OF EVIDENCE (FRE)

The complete criminal trial process involves many stages and proceedings such as: Initial Appearances, Preliminary Examinations, Arraignments, Grand Jury hearings, pre-trial motions to decide whether evidence will be suppressed, sentencing proceedings, and appeals. With the exception of the FREs that apply to privileges, the FREs apply only to the actual trial itself - where the jury (or the judge in a bench trial) hears evidence on the question of whether the defendant is guilty or not guilty. The FREs do not apply to what information an LEO may consider when investigating a case. For example, though hearsay is inadmissible in a trial, an LEO may consider hearsay information when conducting an investigation or in deciding whether there is reasonable suspicion or probable cause.

II. THE PROCEDURAL STAGES OF A CRIMINAL TRIAL

A. SUPPRESSION HEARINGS (MOTIONS HEARINGS)

If there is evidence one side does not want the jury to hear, they will file a motion to suppress. Most often, it is the defense that files suppression motions and most frequently because they claim that evidence was illegally seized or a confession illegally obtained. Law enforcement officers frequently testify at suppression hearings. The jury is not present and the judge will decide whether the evidence will be received into evidence and go to the jury. If evidence is suppressed, the jury will not know about it.

B. VOIR DIRE

During voir dire, the lawyers question the potential jurors and the jury is selected.

C. OPENING STATEMENTS BY COUNSEL

At this stage lawyers tell the jury what they expect the evidence will show. The defense may reserve their opening statement until after conclusion of the prosecution's case.

D. THE CASE IN CHIEF

The prosecution's "case-in-chief" is also known as the case on "the merits." The government presents its evidence by calling witnesses and offering exhibits. The defense may cross-examine any witness that is called and may challenge the admissibility of exhibits. If the witness is cross-examined, the prosecution may conduct a "re-direct" examination. There can be further re-cross and re-direct. The prosecution always goes first because the burden is on them to prove the defendant's guilt beyond reasonable doubt.

E. THE DEFENSE CASE

The defense is NEVER required to present any evidence because the burden is and always remains on the government to prove the defendant's guilt. Just like in the prosecution's case, defense witnesses can be cross-examined, their exhibits can be objected to, and there can be re-direct of witnesses.

F. THE REBUTTAL CASE

If the defense presents a case, the prosecution may offer rebuttal evidence. In the rebuttal case, the prosecution may only present evidence that rebuts or challenges the evidence that the defense presented. If the prosecution presents a rebuttal case, the defense may then rebut what the prosecution just presented. The rebuttal cases continue until all rebuttal evidence has been presented.

G. CLOSING ARGUMENT

During closing arguments, the lawyers tell the jury what they think the evidence showed. The lawyers may argue only that which was admitted into evidence.

H. THE CHARGE TO THE JURY

During "the charge" (instructions) to the jury, the judge will tell the jury what the law is so the jury may apply the law to the facts in reaching the verdict. After deliberation, the jury will announce the verdict.

I. SENTENCING

If the defendant is found guilty of any offense, the judge will conduct a sentencing hearing. This does not involve the jury unless the case is a capital (death penalty) one in which the jury will be asked to make certain findings.

J. POST-TRIAL PROCEEDINGS

There are many different appeal procedures the defendant may attempt to use.

III. RELEVANT EVIDENCE

A. THE REQUIREMENT FOR EVIDENCE TO BE RELEVANT

Evidence must be relevant to be admissible. There are no exceptions. (FRE 402). Evidence is relevant if it has "any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." By this legal definition, we see that evidence is relevant if it has any tendency to prove or disprove a fact that is in issue in the trial.

Evidence does not have to prove an element of a crime or be the smoking gun. If evidence (testimony or exhibits) has any tendency to prove a part of the case - directly or indirectly - the evidence is relevant. LEOs must find and collect all evidence because what might not appear relevant now may become relevant later.

Evidence that is always relevant is that which tends to: (a) prove (or disprove) an element of the crime charged, (b) prove or rebut a defense, or (c) concerns the credibility (believability) of a witness.

B. WHEN RELEVANT EVIDENCE IS NOT ADMISSIBLE

Though evidence must be relevant to be admissible, not all relevant evidence is admissible. For example, evidence that is privileged - such as what a defendant has told his lawyer - cannot be introduced at trial. In addition, one FRE (FRE 403) provides that evidence that is relevant may still be excluded if the ability of the evidence to prove a fact in dispute is substantially outweighed by the danger of unfair prejudice, confusion of issues, misleading to the jury, undue delay, waste of time, or needless presentation of cumulative evidence. Some examples:

1) The prosecution does offer evidence that is prejudicial to the defense case. If the evidence is <u>unduly</u> prejudicial (its probative value is substantially outweighed by its prejudicial effect), the judge may exclude it. A good example is if the prosecution had a substantial number of detailed and gory autopsy photos. If the government could make its point with less than all the photos, the judge might exclude some of them.

2) Trials can be long and complex. When the evidence becomes repetitive, wastes the court's time, or is of a nature that it would confuse or mislead the jury, the judge can refuse to admit the evidence.

C. OTHER CRIMES, WRONGS, AND ACTS OF THE DEFENDANT

The prosecution cannot offer evidence of things that the defendant did to prove he "did it before, he did it again" or that the defendant is a bad person. This is called "propensity evidence" and is disallowed. The prosecution may offer other acts of the defendant - to include bad or criminal acts - if it goes to *prove the charged crime itself*. Examples:

1. Motive

Does a prior act tend to prove the defendant's motive to commit the charged crime? A prior altercation between the defendant and the victim admissible to prove motive for a later assault. In a bank fraud case, evidence that the defendant had outstanding civil judgments is admissible to prove the motive for using a false name on a bank loan.

2. Intent

Does a prior act tend to prove whether the defendant has a specific intent to commit the charged offense? For example, falsely identifying oneself and evading identification right *after* a charged offense is admissible to provide intent to defraud.

3. Knowledge

Do the defendant's acts tend to prove the defendant knew a certain fact? Evidence of a large number of firearms in the defendant's house would be admissible to prove the defendant knew he had firearms in his home.

4. Plan or Preparation

Do the defendant's acts tend to prove how the defendant planned or prepared for the charged crime? In a trial for carnal knowledge (sex with a minor,) evidence that the defendant gave marijuana to the victim

before having sex is admissible to show the defendant's plan to lower the victim's resistance.

5. Opportunity to Commit the Crime

6. Modus Operandi

If the defendant has a particular way of committing an offense, evidence of prior offenses may be admitted to prove the defendant committed the offense being tried.

7. Identity of the Perpetrator

Evidence that on a prior occasion that the defendant, under "signature-like" circumstances, committed an offense may be admissible to prove that the defendant was the person who committed the charged offense.

8. Impeachment

Impeachment by contradiction. If the defendant makes a factual claim while testifying, that fact can be contradicted. The contradiction might include evidence the defendant engaged in prior misconduct.

9. Predisposition

Predisposition to defeat entrapment. If a defendant raises an entrapment defense, prior criminal acts are admissible to prove that the defendant was predisposed to commit the crime.

IV. DIRECT AND CIRCUMSTANTIAL EVIDENCE

Direct evidence is that which tends to prove a fact directly and without the need to draw an inference or a conclusion. Direct evidence

most often comes from what a witness sees, hears, smells, tastes, or touches. In contrast, circumstantial evidence tends to prove a fact indirectly through an inference, deduction, or a conclusion. For example, testimony that, "The street was wet when I got up in the morning" is circumstantial evidence it rained during the evening.

Sometimes we hear, "That is just circumstantial evidence" or "The case was entirely circumstantial." Circumstantial evidence can be very powerful and more reliable and convincing than eyewitness testimony. Most physical evidence is circumstantial because it proves something indirectly. For example, a ballistics test proves that a certain gun fired a certain bullet leading the jury to the conclusion that the defendant (who was found in possession of the gun) killed the victim. There is no rule that one type of evidence is more powerful than another. The power of different types of evidence always depends on the case and the other evidence.

V. LAY (AND EXPERT) WITNESS TESTIMONY

Generally, a witness may only testify from personal knowledge. Witnesses may offer their opinion only if they are an expert or if the matter is the proper subject of a "lay witness opinion."

Many criminal trials involve expert witness testimony due to advances in forensic evidence such as fingerprint identification, ballistics, toxicology, blood splatter, handwriting identification, fiber comparison, tool and die marks, questioned documents and similar disciplines. To testify about a scientific or technical matter or other area of specialized knowledge, the witness must be qualified by their knowledge, skill, expertise, training, or education. (FRE 702).

Most LEOs are not qualified to testify as an expert on most forensic areas if they have only generalized police training. For example, while most LEOs have had training in collecting latent prints and fingerprint identification basics, they have insufficient qualifications to testify in court about a fingerprint comparison. LEOs who have had specialized training,

education, knowledge or experience can be qualified as experts.

A person who is not an expert witness is called a lay witness. A lay witness may give an opinion only when: (a) the opinion is rationally based on the witness' perception and personal knowledge, (b) the opinion is helpful to a clear understanding of the witness' testimony or the determination of a fact in issue, and (c) the opinion is not one that is based on scientific, technical, or other specialized knowledge. In sum, a lay witness may testify about things that are within the perception of an ordinary person that results, as one court said, "from a process of reasoning familiar in everyday life." Some examples of a proper lay witness opinion are:

A. HANDWRITING

Identification of handwriting if the witness has sufficient familiarity with that handwriting. A secretary or co-worker, for example, might be sufficiently familiar with someone's handwriting to say, "That's it."

B. VOICE

Identification of a person's voice (whether hearing it first hand or from a recording) provided the witness has heard the voice before under circumstances where they knew who the speaker was.

C. EMOTIONAL CONDITION

"She looked nervous." "He was in pain."

VI. WITNESS CREDIBILITY AND IMPEACHMENT

A witness is credible if they are believable. Each side in a trial wants their witnesses to be believed, and the jury (or the judge in a bench

trial) decides whether a witness is credible and can elect to believe all, nothing, or parts of what a witness says.

A. IMPEACHMENT

Impeachment is an attack on the credibility of a witness. Any witness who testifies can be impeached. The impeachment evidence can be offered during cross-examination or can be offered through the testimony of another witness. Examples:

1) Impeachment through cross-examination. "Isn't it true that you must wear glasses to see distances?"

2) Impeachment by calling another witness. "Mr. Smith, who testified earlier, wears thick glasses, doesn't he?"

If a witness is impeached, the jury may find the witness' testimony less believable. The side that called the witness will then be allowed to "rehabilitate" to restore the witness' credibility. For example, if a witness was impeached with questions about wearing glasses, the witness could be rehabilitated with evidence that the prescription was current and the witness was wearing clean glasses in a correct manner.

While impeachment or rehabilitation occurs in the courtroom, they are based upon facts, and it is often the duty of the LEO to develop these facts. LEOs must collect evidence that can be used to impeach defense witnesses, can be used by the defense to impeach government witness so the AUSA can anticipate and prepare for it, and can be used by the prosecution to rehabilitate prosecution witness who are impeached at trial.

B. FACTORS THAT AFFECT A WITNESS' CREDIBILITY

1. Bias

A witness may be biased for or against another witness or an issue

in trial because witnesses with a bias may tend to color or slant their testimony. Bias can arise when witnesses are related by blood or marriage or when they are members in similar groups (gangs, Church-Temple-Synagogue or other place of worship, college fraternities or sororities etc.). Bias may also exist in other relationships such as fellow LEOs, former prison cellmates, or partners in crime.

2. Motive to Fabricate Testimony

A witness with a stake in the outcome of the trial or a vendetta against another witness or the other side may have a motive to lie (motive and bias are similar). Motive is illustrated by witnesses who are financially or emotionally dependent on the defendant or witnesses who have a reason to help (or hurt) the defendant. Co-defendants and co-conspirators are easily attacked if they try to shift the blame toward the defendant.

3. Inability to Observe or Accurately Remember

If a witness was unable to see or hear what happened or has an impediment to being able to remember or recall, these matters may be used to impeach the testimony. Examples are: concerns about vision or hearing; witness who were not in a physical position to see or hear what occurred; alcohol or other drug intoxication at the time of the events; or mental impairments.

4. Contradiction

A common form of impeachment is to challenge the testimony of a witness to show what they said is not true. If a witness says the car was green, they can be impeached with evidence that the car was in fact red.

5. Prior Inconsistent Statements

Perhaps the best possible impeachment is to contradict witnesses with their own words from testimony at another proceeding, reports, notes, and statements to others.

6. Character for Truthfulness

Character evidence is a special kind of evidence that permits a witness to testify they have an opinion of a certain character trait of the witness or they are aware of the witness' reputation for having a certain character trait. If a witness testifies, the other side may offer opinion or reputation testimony (character evidence) that the witness is untruthful. The following is character evidence and would be would be allowed: "I have known Mr. Smith for 5 years and in my opinion he is a not a truthful person," or "I know Mr. Smith and he has the reputation in our community for being untruthful." If character evidence of untruthfulness is admitted, rehabilitation character evidence that the witness is truthful is admissible.

7. Specific Instances of Conduct that Indicate a Witness is Untruthful

A witness may be cross-examined about conduct that would indicate they engaged in acts that would indicate they are untruthful. The conduct does not have to relate to the case being tried. Examples would be having lied in an investigation, forging checks, or engaging in acts of deceit. LEOs who have engaged in such conduct, on or off duty, might have that conduct exposed in court.

8. Prior Convictions to Show Untruthfulness (FRE 609)

A prior conviction (NOT an arrest) can be used to impeach any witness who testifies though the judge may decide that the conviction is "too prejudicial" for the jury to hear it. The idea behind allowing prior convictions is one who has been convicted may be the type of person who

is untruthful. A prior conviction is NOT admissible to show the defendant "did it before so he did it again" or that he is a bad person and therefore might have committed the charged crime. Convictions that are less than 10 years old that are either felony convictions for any offense, or misdemeanor convictions for perjury or false statement, may be used to impeach a witness who has testified. The ten years is measured from the date of conviction or the date of release from confinement whichever is later. If the conviction is under appeal it may still be used. Convictions that have been reversed or the subject of a pardon may not be used. Generally, a juvenile adjudication may not be used but the AUSA should be told about them.

9. Character (opinion or reputation) other than Truthfulness - limitations on propensity evidence. (FRE 404(a))

In the government's case in chief, the prosecution may *not* offer evidence that any person has a particular character trait to prove that the person "acted in conformity therewith." For example in a fraud case, the prosecution cannot offer evidence that the defendant is a swindler. The defense *may* offer character evidence that the defendant or the victim has a certain trait. This means the defense can offer evidence that the defendant is an honest person and would not swindle anyone. The defense can also offer character evidence that the victim is the real swindler and the defendant should be viewed as the victim. If the defense offers character evidence of the defendant or the victim, the defense has "opened the door" and the government can respond with its own character evidence.

VII. PRIVILEGES

When a privilege exists, it means that a person cannot be required to provide certain information and can prevent others from doing so. While ordinarily a witness can be required to testify at a Grand Jury or a trial under threat of being held in contempt, if the information is

privileged, a person cannot be compelled to give the information no matter how relevant and important it may be. The courts developed the privileges used in Federal criminal trials.

Privileges exist because the law reflects societal concerns that certain information - though relevant and important - will not be revealed in order to promote some other societal good. For example, in order to ensure that criminal defendants will candidly communicate with their defense attorneys, the law makes their communications privileged. Society has decided that it is better to have clients talk to their lawyers than to reveal attorney-client discussions.

A. HOLDERS OF A PRIVILEGE

As the privileges are discussed, one should identify who holds the privilege. The holder is the one who can refuse to divulge the privileged information. In some cases, certain persons can exercise the privilege on behalf of the holder such as when attorneys refuse to reveal what clients tell them.

B. WAIVER OF PRIVILEGES

The holder can waive any privilege. If a person waives the privilege, the information can be used. Unlike a waiver of Miranda rights, there is no special method or writing to have a person waive the privileges discussed here. If the LEO knows that a person holds a privilege, the LEO may still question the person. If the person answers the question, they are waiving their privilege. The LEO should presume that the person may later attempt to invoke their privilege at a Grand Jury, trial, or other proceeding. The LEO should then obtain independent information that proves or corroborates what the holder of the privilege told the LEO in case the person later invokes their privilege.

C. PRIVILEGES AND THE RULES OF EVIDENCE

The general rule is that FREs apply only to trials. They do not

apply to other proceedings such as Grand Jury investigations, preliminary examinations, suppression hearings, sentencing hearings, and the like. The exception is that privileges apply to all Federal criminal proceedings to include Grand Jury proceedings, preliminary examination, and other proceedings.

D. THE FEDERAL PRIVILEGES

Not all Federal privileges are discussed in this text but only those that LEOs will commonly encounter.

1) The 5th Amendment privilege against self-incrimination. This is the subject of self-incrimination training and will not be further discussed here.

2) The attorney-client privilege.

3) The husband-wife privileges.

4) The psychotherapist-patient privilege.

5) The government informant privilege.

6) The clergy-communicant privilege.

E. NON-FEDERALLY RECOGNIZED PRIVILEGES

Privileges that are commonly discussed that are *not* recognized in Federal criminal trials.

1) Doctor-patient (unless the doctor was a psychotherapist).

2) Accountant-Client.

3) Journalist-Source.

4) Parent-Child.

F. THE ATTORNEY-CLIENT PRIVILEGE

The privilege covers communications - written or oral - between attorney and client made during professional consultation. It includes communications before payment for services, and the privilege remains even if the attorney-client relationship is severed such as when a client fires the lawyer. The privilege exists to encourage clients charged or under investigation with a crime to speak candidly with their attorney in order to obtain an adequate defense.

Elements of the privilege: (a) The attorney must be acting in the capacity as an attorney in a professional capacity, (b) the communication must have been intended to be confidential, and (c) the communication must have been confidential in fact.

The client holds the privilege. The attorney may exercise the privilege for the client by refusing to divulge what the client told the attorney.

The privilege does not apply when the attorney is serving in some function other than a legal adviser such as a mere conduit for funds, real estate transactions, stock sales, and ordinary business transactions. Such dealings are not strictly attorney functions.

Joint criminal ventures between the attorney and client. While the privilege applies to communications about past crimes, it does not apply to the commission of future crimes such as when the client was engaged in (or was planning) criminal or fraudulent activity. Communications intended to facilitate or conceal criminal or fraudulent activity are also unprotected.

The presence of a third person during the communication will usually destroy the confidentiality of the communication and therefore the privilege such as when the communication is made in a public place where people can overhear. The law recognizes, however, that if the presence of the third person is essential for the attorney to perform the function as a legal advisor in preparing a defense in a criminal case, then these third persons fall under the "umbrella" of the privilege. Examples would be a legal secretary or paralegal, investigator working for the attorney, or a messenger.

G. THE HUSBAND-WIFE PRIVILEGES

There are actually two forms of the husband-wife privilege. One privilege allows a spouse to refuse to testify against their spouse about anything. The other privilege allows one to prevent their spouse or former spouse from revealing private, martial communications. This text will not make the distinction between these two husband-wife privileges because the distinction is not critical to how LEOs perform their duties.

Spouses can refuse to testify against each other or to prevent the other spouse from doing so. This encourages husbands and wives to communicate with each other and to preserve marriages. The privileges apply to what a spouse saw or heard as well as private, marital communications between the husband and wife. The privilege does not apply when the marriage was a sham as determined by state law, when a spouse or the child of either spouse is the victim of the crime charged, and in most Circuits, when both spouses participated in the crime.

In many situations, spouses will provide information to LEOs and even testify at a Grand Jury. Circumstances may change and at the time of trial, the witness may decide to exercise the privilege and not testify. Unless the LEO has developed independent corroborating evidence, there may be no way to prove the information the spouse provided earlier.

H. THE PSYCHOTHERAPIST-PATIENT PRIVILEGE

Confidential communications between licensed psychiatrists, psychotherapists or social workers and their patients in the course of psychotherapy diagnosis or treatment are privileged. Though there is not a general doctor-patient privilege, if the doctor is a psychiatrist or other mental health professional, the psychotherapist-patent privilege may exist. This privilege exists because effective psychotherapy depends upon an atmosphere of confidence and trust.

A party asserting the psychotherapist-patient privilege must show that the communications were made: (a) confidentially, (b) between a licensed psychotherapist and the patient, and (c) in the course of diagnosis or treatment. The patient holds the privilege. The person providing the psychotherapy may exercise the privilege on behalf of the patient.

The privilege does not apply if the communications were not confidential. Statements made during the course of a group therapy session or statements made by patients about what they said to the psychotherapist would not be confidential. Since this is a relatively new Federal privilege, the Supreme Court may later recognize other exceptions that some States already observe. For example, the privilege might not be recognized if the patient communicates serious threats to himself or others, or the patient and therapist were engaged in a criminal enterprise.

I. THE CLERGY-COMMUNICANT PRIVILEGE

The Supreme Court has not specifically adopted the clergy-communicant privilege though most Federal Circuits have recognized it. This privilege arises infrequently because AUSAs are reluctant to call a member of the clergy to testify against a defendant.

The elements of this privilege are: (a) a communication is made to a member of the clergy, (b) in the clergy's spiritual and professional capacity, and (c) with a reasonable expectation of confidentiality. "Clergy" includes minister, priest, pastor, rabbi, or other similar

functionary of a religious organization, or an individual reasonably believed to be so by the person consulting him. The presence of others necessary to communicate the information does not defeat the privilege. The privilege exists to encourage people to communicate with members of the clergy on spiritual matters.

The communicant holds the privilege. The clergy may exercise the privilege for the client by refusing to divulge what the communicant said. If the communication was not on a spiritual matter - such as a joint criminal enterprise - the privilege will not apply.

J. THE GOVERNMENT-INFORMANT PRIVILEGE

In the other privileges discussed so far, the privileged information is generally what the person holding the privilege said. The government-informant privilege is different in two respects: (a) What is privileged is not the communication, but the identity of the informant and information that would reveal the informant's identity and (b) The holder of the privilege is not the person who made the communication, but to whom the communication was made (the government). The privilege exists to encourage people to report crime and cooperate with the police.

Not everyone who provides information to the government is an informant for the purposes of this privilege. For example, victims of crimes and LEOs provide information that does not fall within the privilege. All agencies have special rules and procedures to follow that bring informants under the umbrella of this privilege, and LEOs must be sure that confidentiality is not promised contrary to agency policy.

The government holds the privilege. The AUSA will exercise the privilege on behalf of the government. The LEO may NOT reveal the identity of the informant unless directed to do so by a judge or the AUSA.

A judge may reveal the informant's identity. If the judge decides

that the informant's identity should be revealed, the AUSA must either do so or dismiss the case. The informant's identity will not be revealed unless the informant's identity is relevant and helpful to the defense of an accused, or is essential to a fair determination of the case. The proper balance depends on the particular circumstances of each case taking into consideration the crime charged, the possible defenses, the possible significance of the informant's testimony, and other relevant factors.

⇒ If the informant is just a tipster or the source of probable cause, the informant's identity will not usually be revealed.

⇒ If the informant introduces the defendant to an undercover agent, this will not usually require the informant's identity to be revealed since what transpires between the undercover agent and the defendant is what is relevant.

⇒ If the informant witnessed activities that are part of either the government's or the defense's case, the judge will have to decide whether revealing the informant's identity is relevant and helpful to the defense or necessary to a fair trial. Here the chances that the informant's identity will be revealed becomes more likely.

⇒ If the informant is a co-accused, conspirator, confederate, or a party to a charged offense, it is likely that the informant's identity will be revealed.

VIII. EVIDENTIARY FOUNDATIONS

Evidence must be authenticated. Authentication shows that there are facts to prove that the item is what the person offering claims it to be. The process of authenticating evidence in court is called "laying a foundation."

Even if the judge admits 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.

A. LAYING A FOUNDATION

The party offering an item into evidence is required to lay a foundation for it. 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. A foundation is laid through the testimony of a witness who can testify from personal knowledge that the exhibit being offered in court is the one they saw, seized, or collected.

B. MARKING/TAGGING EVIDENCE

The evidence tag documents where and when the evidence was found and who found it. Proper marking/tagging and bagging will ensure the LEO can identify the evidence discovered is the same exhibit shown to the LEO in court. The evidence should be marked, tagged, or bagged in such a way the LEO will recognize it in court.

C. CHAIN OF CUSTODY

While an evidence tag documents where and when the evidence was found and who found it, a properly prepared chain of custody documents where the evidence has been and who has handled it since the time it was discovered until the time it is offered in court. It also documents alterations to the evidence. The first entry on the chain of custody should be the person who found the evidence. A chain of custody does not eliminate the need to call witnesses to lay a foundation, and does not substitute for having the item in court. It can, however, reduce the number of witnesses required and better ensure a foundation

and protect the foundation from attack.

D. LEGAL ADMISSIBILITY AND PRESERVING TRACE EVIDENCE CHARACTERISTICS

When collecting evidence to ensure you can lay a foundation for it later, the evidence must still be collected in a way to preserve trace evidence such as fingerprints, hair and fiber evidence, blood splatter and the like. Laying a foundation for the admissibility of evidence does not satisfy evidence-handling techniques designed to preserve trace evidence. Handling evidence that preserves trace evidence may not always satisfy legal admissibility rules. The LEO must keep both aspects in mind when collecting physical evidence.

E. CONDITION OF THE EVIDENCE AT THE TIME OF TRIAL

There is no established legal standard that evidence has to be in a certain condition in court when compared to how it appeared when it was collected. Whether the judge decides there is a proper foundation depends on a multitude of factors. Usually it is sufficient that the evidence is in the same or substantially the same condition as when collected, and if there have been alterations, that the alterations can be explained and are documented. Mishandling evidence or alterations that cannot be documented may mean the witness is unable to lay a proper foundation and the evidence may be inadmissible. There is no limit to the ways an evidentiary foundation can be challenged but here are some examples:

1. Mis-marked or incomplete tags, bags, or chain of custody documents. (Take your time.)

2. Transfers of evidence improperly recorded on chain of custody documents ("broken" chain of custody).

3. Failing to wear gloves or other protective garb obliterating

trace evidence or contaminating the scene (use proper trace evidence handling techniques; bring in a specially trained evidence team when necessary).

4. Improperly storing evidence such as unrefrigerated biological materials or computer disks and magnetic tapes stored near excessive heat or a magnetic source (consult evidence handling experts).

5. Reusing evidence tape, swabs, bags, or seals (these items are cheap; discard contaminated or used supplies).

6. Marking documents or evidence in such a way the evidence is "altered" (Did the LEO obliterate a fingerprint when the item was marked? Did page numbering of documents alter the meaning or authenticity of the document?).

7. Working with originals of computer disks, photos, documents, tape recordings or the like (make copies and work with copies).

8. Preserve originals in ways they cannot be altered (break tabs from cassette and video tapes; lock out computer disks and media storage disks; document when this is done).

IX. HEARSAY

A. HEARSAY DEFINED

Hearsay occurs when: (a) a statement is made out of court, (b) the out of court statement is offered in court (trial), and (3) the out of court statement is offered for the truth of the matter asserted in the statement.

B. HEARSAY EXAMPLES

In each case, the witness wants to offer the quoted statement in court.

(1) "Susan said Bob stole her purse." (To prove that Bob is a thief).

(2) "John said he saw the green car that night." (To prove there was a green car at the scene).

C. APPLICABILITY OF THE HEARSAY RULE

The hearsay rule applies only to trials. Officers can and often do rely on hearsay to develop probable cause, reasonable suspicion, guide their decisions, and develop leads. Hearsay may be used in criminal complaints, search warrant affidavits, Grand Jury hearings, suppression hearings and other, non-trial proceedings. At trial, hearsay for which there is no exception is inadmissible.

D. REASON FOR THE HEARSAY RULE

Hearsay is inadmissible because it is not possible to confront and cross-examine the person with the first hand knowledge, the jury is unable to assess the witness' demeanor and credibility, and the original statement was probably not made under oath or subject to cross examination. Hearsay is just not considered sufficiently trustworthy to let the jury consider it.

E. WHAT IS A STATEMENT?

A "statement" can be verbal, written (such as a written statement of a person) or an act intended to communicate information (nodding the head, pointing, gesturing). Memoranda, writings, and reports that the LEO prepares are "statements" within the meaning of hearsay.

F. "TRUTH OF THE MATTER ASSERTED"

The third component of the hearsay rule is that the out of court statement is being offered for the truth of the matter asserted. If the jury is asked to believe the statement is true, the statement is hearsay. If the statement is being offered for a legitimate reason other than to prove that the statement is true, then the statement is not hearsay. For example, if the statement offered is "Bill told me that Joe shot him" to prove Joe shot Bill, the statement is hearsay. If the statement is offered to show why the officer was looking for Joe or part of the probable cause to arrest Joe, the statement is not hearsay because it is not offered to prove Joe shot Bill.

G. NON-HEARSAY

1. Statements of the Defendant

Because the prosecution cannot call the defendant to the stand to testify, statements made by the defendant and offered by the prosecution are specifically excluded from the definition of hearsay. For the LEO, it really does not matter whether the statement is classified as an admission, confession or just plain information.

2. Other Statements

Statements of the defendant's co-conspirators made during and in furtherance of the conspiracy are excluded from the definition of hearsay (this is taught in the Conspiracy course). Also, prior consistent statements of a witness to show the witness "just didn't make up" their testimony, but what the witness had claimed all along, is also excluded from the definition of hearsay.

X. EXCEPTIONS TO THE HEARSAY RULE

If an exception to the hearsay applies, the statement is admissible.

There are many hearsay exceptions and this text will discuss only two of them. It is important that if the LEO receives a statement that might be hearsay, the LEO must document the facts and circumstances under which the statement was made; this might make the statement admissible under another exception to the hearsay rule.

A. "EXCITED UTTERANCES"

The law recognizes that a statement made under emotional stress is unlikely to be fabricated. This is the reason for the excited utterance hearsay exception. The elements of the exception are: (a) the person making the statement experienced a startling event, (b) the statement was made while the person was under the stress or excitement (influence) caused by that event, and (c) the statement was about the startling event. For example, while yelling, holding their hand over a gunshot wound, and in a high emotional state, a victim runs up to a law enforcement officer and says, "Joe shot me!" would meet this exception.

B. STATEMENTS FOR PURPOSES OF MEDICAL DIAGNOSIS OR TREATMENT

The law recognizes that when a person is speaking to health care providers about why they are sick or injured, they are unlikely to fabricate. The elements of this exception are: (a) a statement is made for the purposes of medical diagnosis or treatment, (b) the statement concerns medical history, past or present symptoms, pain, sensations, or the cause of the medical problem, and (c) the statement is pertinent to diagnosis or treatment. The person who receives the statement does not have to be a physician. If the person making the statement believes that the person they are speaking to is someone who is going to help them medically, the statement can qualify under this exception. Such statements can be made to nurses, Emergency Medical Technicians, or those working in the medical field who are treating the person. In child sex abuse and domestic abuse cases, the identity of the assailant is pertinent to the treatment because such injuries involve emotional and psychological injury as well physical. In treating such injuries, knowing the identity of

the perpetrator will assist in the medical treatment.

XI. STATEMENTS, REPORTS AND COURTROOM TESTIMONY

Except for some expert witnesses and other very limited circumstances, witnesses cannot testify from their reports or notes. LEOs should check with their AUSA about whether to bring reports or notes to trial.

An officer's reports and notes, as well as written statements and notes of other witnesses, can be used *against* a witness to impeach the witness' in court testimony. For example, if a witness testifies that the license plate of a certain car was ABC but their report or their on-scene notes indicate otherwise, the defense can use the contradiction to impeach the witness.

If a witness forgets a fact while testifying, their memory can be "refreshed." The rule is that "anything can be used to refresh a witness' memory." Sketches, photos, physical objects, reports, notes, and even "unofficial items" such as documents prepared by other LEOs or non-LEOs can be used. Documents or statements used to refresh memory do not have to be under oath. When a witness' memory is refreshed, the witness can then testify from memory. The report or item that was used to refresh memory is neither read nor given to the jury as the witness will be testifying from their refreshed memory.

Notes, reports, statements or other writings that are used to refresh a witness' testimony are available to the other side. These items can be used to cross-examine the witness and for other purposes.

XII. FOUNDATIONS FOR BUSINESS RECORDS AND PUBLIC DOCUMENTS

A. THE BEST EVIDENCE RULE (FRE 1001; 1002)

This is best remembered as the "Original Document Rule." Before copy machines, carbon paper, and other duplicating processes, copies of documents were made by hand. This process lent itself to errors in copying and what was supposed to be an exact copy was not always so. For primarily this reason we have the Best Evidence Rule. Though many of the Rule's concerns have been resolved by technology, the Rule must be followed.

1. An "Original"

The original of a document is the actual document itself or counterparts intended to be the equivalent of the original such as identical documents executed by both parties at the same time. An original of a photograph is any print made from the negative. As to computer data, any visible printout of the data is an original.

2. "Duplicates"

Duplicates include carbon copies, photocopies ("Xerox" copies), or copies made from other techniques that accurately reproduce the original. A duplicate is admissible to the same extent as the original unless a genuine question is raised as to the authenticity of the original, or it would be unfair to use a duplicate instead of the original such as when a duplicate is of poor quality or otherwise not legible.

The Best Evidence Rule states that to prove the contents of a writing, the original writing itself must be admitted into evidence; witnesses are not permitted to testify what a document says. If the document is available, it must be admitted into evidence. There are exceptions such as when all originals have been lost or are unobtainable, or the other side has the original and will not produce it. Remember that

in most cases, duplicates are the evidentiary equivalent of originals.

B. SELF-AUTHENTICATION

A foundation is required to introduce a business record or public record. Ordinarily the foundation is laid by the custodian of the record who can state how the record was created and maintained. Special rules, however, allow certain documents and records to be "self-authenticating." Self-authenticating records and reports do not require a witness to testify and lay a foundation.

1. Public Records and Documents

The FREs permit public records and documents to be self-authenticating if they are accompanied by a seal or certified as correct by the custodian. Federal agencies have established procedures and the necessary forms to provide public documents and records under seal or to be certified. If the document or record is certified or under seal, the custodian does not have to be called to lay a foundation for the document. The LEO does not have to personally obtain the record by hand.

2. Business Records

Before December 2000, to admit any business record (a cancelled check, phone record, contracts, and other business records), a custodian was required to personally appear to authenticate the record. A change to the FREs now permits business records to be self-authenticating similar to public documents and reports. To make business records self-authenticating, and avoid calling the custodian to testify, the custodian must certify that:

1) The record was made at or near the time to which the record pertains by a person with knowledge of the matter,

2) The record was kept in the ordinary course of business,

and

3) The business made such a record as a regular practice (and not specially generated just for the trial).

C. HEARSAY AND PUBLIC RECORDS AND DOCUMENTS AND BUSINESS RECORDS

Offering the contents of public records and documents and business records for the truth of their contents can be hearsay, but there is a specific hearsay exception for them. If there is a seal or certificate that complies with the self-authentication rules, then not only will the business records or the public documents or records be self-authenticating, the contents will be admissible to prove the truth of the contents as an exception to the hearsay rule. As an "exception to the exception," matters observed by law enforcement do not come under this exception, that is, even self-authenticated police reports are still subject to the hearsay rule.

XIII. AUTHENTICATING INFORMATION CONTAINED IN COMPUTERS

A. INVOLVING COMPUTER FORENSICS EXPERTS

Computer forensics experts should participate in all phases of determining whether probable cause exists to search computers, in drafting the search warrant, or in executing the search. When such experts are assisting in the search, the LEO must be mindful of 18 U.S.C. § 3105 that provides that no person, except in the aid of the officer requiring it, may be present and acting in the execution of a search warrant. Not having an computer expert can jeopardize the admissibility of the evidence seized. If a computer forensics expert is needed, ensure the warrant indicates one is needed to aid in the search.

B. RULES OF EVIDENCE ISSUES WHEN AUTHENTICATING "DIGITAL (OR ELECTRONIC) EVIDENCE"

Digital evidence is nothing but an electronic series of 0s and 1s that is interpreted by a computer program. Below are some of the special, significant challenges in having digital evidence admitted into court.

1. Were the records altered, manipulated, or damaged after they were created?

2. Who was the author of the record?

3. Was the program that converted the digital evidence to words or graphics reliable?

Proving authorship is usually solved by collecting circumstantial and other evidence during the search such as where the storage device (drive, disk, or other medium) was found; who had access to the data; trace evidence, passwords and screen names and who had access to them; names on folders containing the data or passwords; and sources of emails that contain attachments.

C. ADMISSIBILITY OF DIGITAL EVIDENCE

To be admissible, there must be a showing that there is a reliable computer program that converted the digital evidence to something that a human can read. 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. For example, Windows based computers associate certain file types with the software designed to create and read them so it is 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. Much software embeds when a document was created and modified and identifies the computer on which this was done. Investigators should have forensic experts look for this data.

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 (7th Cir. 1990), cert. denied 498 U.S. 863.

D. THE BEST EVIDENCE RULE REQUIREMENT FOR AN "ORIGINAL"

Is the digital data (the 0s and 1s) an original so to satisfy the Best Evidence Rule? Yes according to FRE 1001(3): "[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." An accurate printout of computer data satisfies the Best Evidence Rule. Doe v. United States, 805 F. Supp. 1513 (D. Hawaii 1992).

E. HEARSAY ISSUES

Whether the hearsay rules apply depends on whether the document is one generated by a computer or contains statements of a human being. Documents created by humans that are stored on a computer are "statements" if the document is offered into evidence for the "truth of the matter asserted." 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.

Records that are generated by a computer are NOT hearsay. Hearsay rules apply only to statements of humans. 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.

Other "statements" that are seized from a computer must meet a hearsay exception or the author located who can authenticate and testify to the statement. So, 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.

BRIBERY / GRATUITIES

I. INTRODUCTION AND DEFINITIONS 264
A. INTRODUCTION 264
B. DEFINITIONS..... 264

II. THE STATUTE – BRIBERY 264

III. THE STATUTE - GRATUITIES..... 267

I. INTRODUCTION AND DEFINITIONS

A. INTRODUCTION

Title 18 U.S.C. § 201 is the federal bribery statute. It prohibits the giving, offering, demanding or receiving of bribes or gratuities by government employees or witnesses.

B. DEFINITIONS

(a) For the purpose of this section,

(1) The term "public official" means Member of Congress, Delegate, or Resident Commissioner, either before or after such official has qualified, or an officer or employee or person acting for or on behalf of the United States, or any department, agency or branch of Government thereof, including the District of Columbia, in any official function, under or by authority of any such department, agency or branch of Government, or a juror;

(2) The term "person who has been selected to be a public official" means any person who has been nominated or appointed to be a public official, or has been officially informed that such person will be nominated or appointed; and

(3) The term "official act" means any decision or action on any question, matter, cause, suit, proceeding or controversy, which may at any time be pending, or which may by law be brought before any public official, in such official's official capacity or in such official's place of trust or profit.

II. THE STATUTE – BRIBERY

Title 18 U.S.C. § 201 is the federal bribery statute. It provides as follows:

(b) Whoever -

(1) directly or indirectly, corruptly gives, offers or promises anything of value to any public official or person who has been selected to be a public official, or offers or promises any public official or any person who has been selected to be a public official to give anything of value to any other person or entity, with intent -

(A) to influence any official act; or

(B) to influence such public official or person who has been selected to be a public official to commit or aid in committing, or collude in, or allow, any fraud, or make opportunity for the commission of any fraud, on the United States; or

(C) to induce such public official or such person who has been selected to be a public official to do or omit to do any act in violation of the lawful duty of such official or person;

(2) being a public official or person selected to be a public official, directly or indirectly, corruptly demands, seeks, receives, accepts, or agrees to receive or accept anything of value personally or for any other person or entity, in return for:

(A) being influenced in the performance of any official act; or

(B) being influenced to commit or aid in committing, or to collude in, or allow, any fraud, or make opportunity for the commission of any fraud, on the United States; or

(C) being induced to do or omit to do any act in violation of the official duty of such official or person;

(3) directly or indirectly, corruptly gives, offers, or promises anything of value to any person, or offers or promises such person to give anything of value to any other person or entity, with intent to influence the testimony under oath or affirmation of such first-mentioned person as a witness upon a trial, hearing or other proceeding, before any court, any committee of either House or both Houses of Congress, or any agency, commission, or officer authorized by the laws of the United States to hear evidence or take testimony, or with intent to influence such person to absent himself therefrom;

(4) directly or indirectly, corruptly demands, seeks, receives, accepts, or agrees to receive or accept anything of value personally or for any other person or entity in return for being influenced in testimony under oath or affirmation as a witness upon any such trial, hearing, or other proceeding, or in return for absenting himself therefrom;

shall be fined under this title or not more than three times the monetary equivalent of the thing of value, whichever is greater, or imprisoned for not more than fifteen years, or both, and may be disqualified from holding any office of honor, trust, or profit under the United States.

In sum, it is illegal to offer a federal official something of value to influence an official act. It is unlawful for federal officials to allow themselves to be influenced by accepting something of value. The bribery statute is simply as it is stated. It is illegal to give a bribe to a federal official or for such official to accept a bribe.

The concept of a bribe involves a corrupt intent. Therefore, in order to prosecute for bribery, the government must demonstrate that something of value was offered or accepted to influence an official act. For example, if a Customs Inspector accepts $5,000.00 from a criminal to allow a shipment of drugs to pass through a port of entry, both are guilty of bribery.

Sometimes federal officials are given something of value because of an official act they have done or are going to do. This is not given to influence an official act, but as a gratuity, or "tip". This is also unlawful. However, as noted below, it is different from a bribe because there is no corrupt or evil intent to influence the actions of the federal official.

III. THE STATUTE - GRATUITIES

Accepting a gratuity is also a crime under the bribery statute, and occurs when a public official requests or accepts something of value that relates to their official duties. Such an act is punishable as a felony, with a maximum punishment of two years in prison.

Note: Government employees may also be prohibited from receiving or taking gifts of all types and value by their agency's administrative policies. Though some acts may not be worthy of criminal prosecution, the employee could be punished for violations of the agency policy.

Giving or receiving a gratuity is a lesser offense than bribery, because there is no requirement the item of value be given corruptly. This means that to obtain a conviction, it is not necessary to demonstrate that the gift was given with the intent to influence an official act. It is sufficient to demonstrate that a gratuity was requested and/or accepted for the performance of an official act. It is irrelevant that the gratuity had no effect upon the actions taken by the public official.

(c) Whoever -

(1) otherwise than as provided by law for the proper discharge of official duty

(A) directly or indirectly gives, offers, or promises anything of value to any public official, former public official, or person selected to be a public official, for or because of any official act performed or to be performed by such public official, former public official, or person selected to be a public official; or

(B) being a public official, former public official, or person selected to be a public official, otherwise than as provided by law for the proper discharge of official duty, directly or indirectly demands, seeks, receives, accepts, or agrees to receive or accept anything of value personally for or because of any official act performed or to be performed by such official or person;

(2) directly or indirectly, gives, offers, or promises anything of value to any person, for or because of the testimony under oath or affirmation given or to be given by such person as a witness upon a trial, hearing, or other proceedings before any court, any committee of either House or both Houses of Congress, or any agency, commission, or officer authorized by the laws of the United States to hear evidence or take testimony, or for or because of such person's absence therefrom;

(3) directly or indirectly, demands, seeks, receives, accepts, or agrees to receive or accept anything of value personally for or because of the testimony under oath or affirmation given or to be given by such person as a witness upon any such trial, hearing, or other proceeding, or for or because of such person's absence therefrom;

shall be fined under this title or imprisoned for not more than two years, or both.

Paragraphs (c)(2) and (c)(3) provide for punishment for gratuities to persons named in paragraphs (b)(3) and (b)(4) in case of rewards given for or because of testimony. These paragraphs do not prohibit the payment or receipt of lawful witness fees.

If a Federal officer believes they or anyone affected by section 201 has been offered a bribe or gratuity, they should immediately report it!

FALSE STATEMENTS

I. INTRODUCTION 270

II. THE STATUTE 270

III. ELEMENTS 271
A. REGARDING CERTAIN FEDERAL MATTERS 272
B. KNOWINGLY AND WILLFULLY - INTENT 273
C. MAKES A FALSE MATERIAL STATEMENT OR CONCEALS OR COVERS UP A MATERIAL FACT 273

I. INTRODUCTION

In 1863, during the Civil War, Congress enacted the False Claims Act to penalize the filing of false claims with the United States Government. In 1934, Congress added to this statute a section prohibiting the giving of false statements to government agents. In 1948, Congress separated these two statutes into different sections of Title 18 of the United States Code: False Claims (Title 18 U.S.C. § 287) and False Statements (Title 18 U.S.C. § 1001).

After the Supreme Court limited the reach of the statute to executive branch agencies in Hubbard v. United States, Congress passed the False Statements Accountability Act of 1996, Pub. L. No. 104-292, HR 3166 (October 11, 1996), 110 Stat. 3459, which restores the statute to its previous effect on executive, legislative and judicial branch activities, effectively overruling Hubbard, with certain limitations concerning legislative and judicial actions.

II. THE STATUTE

Title 18 U.S.C. § 1001, provides as follows:

(a) Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully--

(1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact;

(2) makes any materially false, fictitious, or fraudulent statement or representation; or

(3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry;

shall be fined under this title or imprisoned not more than 5 years, or both.

(b) Subsection (a) does not apply to a party to a judicial proceeding, or that party's counsel, for statements, representations, writings or documents submitted by such party or counsel to a judge or magistrate in that proceeding.

(c) With respect to any matter within the jurisdiction of the legislative branch, subsection (a) shall apply only to--

(1) administrative matters, including a claim for payment, a matter related to the procurement of property or services, personnel or employment practices, or support services, or a document required by law, rule, or regulation to be submitted to the Congress or any office or officer within the legislative branch; or

(2) any investigation or review, conducted pursuant to the authority of any committee, subcommittee, commission or office of the Congress, consistent with applicable rules of the House or Senate.

III. ELEMENTS

In order to successfully prosecute a defendant for violating section 1001, the following elements must be met:

WHOEVER,

Regarding certain federal matters...

knowingly and willfully...

makes a false material statement, or

conceals or covers up a material fact...

shall be fined/imprisoned 5 years.

A. REGARDING CERTAIN FEDERAL MATTERS

Section 1001 applies to false statements made in a matter within the criminal jurisdiction of the executive, legislative, or judicial branches. The statute applies to statements made during administrative, civil, or criminal investigations, or during regulatory or rule-making activities, with the following limitations:

1. Section (a) of the Act does not apply to a party or their counsel for any statements, representations, writings or documents submitted by them to a judge or magistrate during a judicial proceeding. Thus, non-parties could be prosecuted for any false statements made during a judicial proceeding, while a party could only be prosecuted for false submissions made to a judicial entity during administrative housekeeping matters. Such entities include, for example, the Office of Probation and the Clerk of the Court.

2. Section (a) of the Act applies to matters within the jurisdiction of the legislative branch only if they relate to administrative matters or Congressional investigations conducted consistent with applicable Congressional rules. Administrative matters would include such things as financial disclosure filings, claims to the House Finance Office, and submissions to legislative entities, such as the General Accounting Office, the Government Printing Office, the Library of Congress, the Office of the Inspector General of the House, and the Capitol Police.

Duly authorized investigations or reviews are those that are initiated through a formal action of a House or Senate committee, or the whole House or Senate. Inquiries by members of Congress or their staff are not a duly authorized investigation under section 1001.

The statute covers false statements made to a federal agency by a witness/informant about alleged criminal acts within the jurisdiction of

the agency, even when no such criminal acts actually occurred. False statements made to an agency regarding the regulatory functions of a federal department or agency fall under section 1001. Courts have upheld convictions under this section where individuals have made false statements to state agencies which are recipients of federal funds.

B. KNOWINGLY AND WILLFULLY - INTENT

In order to be a violation of section 1001, a statement must be capable of affecting the exercise of a government function. The intent must be to deceive or mislead. Intent to defraud is not required for a successful section 1001 prosecution.

C. MAKES A FALSE MATERIAL STATEMENT OR CONCEALS OR COVERS UP A MATERIAL FACT

The false statement must be *material* for a person to be convicted of making a false statement under section 1001. The Supreme Court has held that a material statement ... must have a natural tendency to influence, or be capable of influencing, the decision of the decision making body to which it was addressed. Materiality is a mixed question of law and fact for the jury.

THEFT, EMBEZZLEMENT AND CONVERSION

I. INTRODUCTION 275

II. THE STATUTE 275

III. THEFT 276
A. ELEMENTS 276
B. EXAMPLE 276

IV. EMBEZZLEMENT 277
A. ELEMENTS 277
B. EXAMPLE 278

V. CONVERSION 279
A. ELEMENTS 279
B. EXAMPLE 279

VI. RECEIPT OF STOLEN PROPERTY 280
A. ELEMENTS 280
B. EXAMPLE 281

I. INTRODUCTION

Title 18 U.S.C. § 641, titled "Public Money, Property or Records," is a comprehensive statute designed to address four crimes which, at common law, were separate and distinct offenses. The statute applies to theft, embezzlement, conversion, and receiving stolen property of the United States government or any department or agency thereof. The purpose behind consolidating these offenses into a single statute was to collect from scattered sources crimes that were so closely related as to belong in one category.

II. THE STATUTE

Title 18 U.S.C. § 641 provides as follows:

Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted-

Shall be fined under this title or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $1,000, he shall be fined under this title or imprisoned not more than one year, or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

For purposes of the statute and this text, "property" refers to any records, vouchers, money, or things of value of (or any property made or being made under contract for) the United States or any department or agency thereof . If the value of the property stolen, embezzled, converted, or received is more than $1,000, the offense is a felony and could result in

ten years confinement and a maximum fine of $250,000. If the value of the property stolen, embezzled, converted, or received is $1,000 or less, the offense is a misdemeanor and could result in confinement of up to one year and, pursuant to Title 18 U.S.C. § 3571, a maximum fine of $100,000.

III. THEFT

Title 18 U.S.C. § 641 codifies the common law crime of larceny. "Theft" is defined as the wrongful taking and carrying away of property belonging to the United States government or any agency thereof with the intent to deprive the United States government of the use or benefit of the property so taken.

A. ELEMENTS

Three elements must be proven to convict a defendant of "theft" under section 641. These elements are:

1) That the defendant voluntarily, intentionally, and knowingly;

2) Stole property belonging to the United States or any department or agency thereof;

3) With the intent to deprive the United States of the use or benefit of the property so taken.

B. EXAMPLE

A defendant takes a vehicle that belongs to the United States government, intending to keep it for his own use and enjoyment. The defendant is guilty of theft of government property. He knowingly stole property belonging to the United States with the intent to deprive the United States of the use of the property.

A defendant "steals" property when he or she takes and carries away property belonging to another with the intent to deprive the owner of the property . To successfully prosecute a defendant for theft under section 641, the government must prove that the defendant had, at the time of the taking, the specific intent to deprive the United States of the use or benefit of the property. The defendant is not required to know that the item he stole belonged to the United States or one of its departments or agencies. Rather, all that needs be proven is that the defendant knew he was taking something that did not belong to him. The fact that the item belonged to the United States government is something the government must show in order to furnish a basis for federal jurisdiction over the crime. The defendant's knowledge of this jurisdictional fact is irrelevant. In order to prove that an item belongs to the United States, the government must prove that it had "title to, possession of, or control over" that item. If the defendant takes the property believing that it was abandoned, that is a defense to a prosecution brought under section 641. In cases where the crime is alleged to have been a felony, the government must prove one additional element: That the value of the item stolen is greater than $1,000.

IV. EMBEZZLEMENT

"Embezzlement" is defined as the wrongful, intentional taking of property of another by an individual to whom the property had been lawfully given by reason of some office, employment, or position of trust (such as a bank manager). In other words, the original taking of the property is lawful or done with the express or implied consent of the owner. However, once the property is lawfully acquired by reason of the defendant's position of trust (sometimes referred to as a "fiduciary" relationship), the defendant intentionally applies the property to an illegal use.

A. ELEMENTS

In order to prove the crime of embezzlement, the government must again prove three elements. With the exception of element #2, the

elements of embezzlement are the same as those for theft. The elements of embezzlement are:

1) That the defendant voluntarily, intentionally, and knowingly;

2) Embezzled property belonging to the United States or any department or agency thereof;

3) With the intent to deprive the United States of the use or benefit of the property so taken.

B. EXAMPLE

A federal employee is responsible for selling stamps to the public. Instead of depositing the money received into a government account, the employee keeps the money for his personal use. The employee has committed the crime of embezzlement. The money was property of the United States; the employee was entrusted with the money legally; he deprived the United States of the use of the money taken; and intentionally appropriated the money to his own personal use.

While the elements are virtually identical for both crimes, embezzlement and theft are separate and distinct offenses. With the crime of embezzlement, the original acquisition of the property is lawful; there is no fraud or crime committed in the original obtaining of the property. It is only after the property has been entrusted to him or her that the defendant forms the intent to deprive the owner of the use of the property taken. This is the primary difference between embezzlement and theft of government property. In embezzlement, the original taking was lawful or with the consent of the owner, and the intent to deprive the United States of the property originated later. In theft, the intent to deprive the United States of the property must exist at the time of the taking. Again, if the

crime is alleged to have been a felony, the government must also prove that the value of the property embezzled was over $1,000.

V. CONVERSION

"Conversion" is defined as wrongfully depriving the United States or any department or agency thereof of its property. In its most basic form, "conversion" simply means that an individual lawfully comes into possession of United States property and wrongfully converts it to his or her own use. The property can be converted either permanently or for an indefinite period of time. Conversion does not require that the defendant intend to keep the property permanently, nor does it require an unlawful taking by the defendant. Under section 641, conversion may include misuse or abuse of government property, as well as use of the property in an unauthorized manner or to an unauthorized extent.

A. ELEMENTS

Like theft and embezzlement, there are three elements necessary to convict a defendant of conversion under section 641. Again, with the exception of element #2, the elements of conversion are identical to those of theft and embezzlement. The government must prove:

1) That the defendant voluntarily, intentionally, and knowingly;

2) Converted property belonging to the United States or any department or agency thereof;

3) With the intent to deprive the United States of the use or benefit of the property so taken.

B. EXAMPLE

A federal agency has a government vehicle for its employees to use for official purposes. At lunch one afternoon, one of the employees uses

the government vehicle to go shopping for a couple of hours at a local mall. The employee is guilty of conversion under section 641. The employee wrongfully deprived the United States government of its property during the unauthorized use of the government vehicle.

VI. RECEIPT OF STOLEN PROPERTY

The statute also prohibits knowingly receiving stolen, embezzled, or converted United States government property. Because the individual receiving the stolen property knows that it has been stolen, he or she does not have any legal interest in the property, which continues to belong to the party from which it was stolen (i.e., the United States).

A. ELEMENTS

In order to convict a defendant of receiving stolen property, the government must prove four elements:

1) That the defendant voluntarily, intentionally, and knowingly received;

2) Stolen, embezzled, or converted property belonging to the United States government or any department or agency thereof;

3) Knowing that the property had been stolen, embezzled, or converted;

4) With the intent to deprive the United States of the use or benefit of the property by using it for his or her own gain or purposes.

B. EXAMPLE

A federal employee steals a computer belonging to the United States government. The employee takes it to a friend and asks him if he would like to buy it at a discount. When asked about the origin of the computer, the employee admits to the friend that it was stolen. The friend decides to purchase the computer anyway for his own use. While the federal employee is responsible for theft of government property, the friend is responsible for receiving stolen property. The friend knowingly received the computer; the computer had been stolen from the United States government or any agency or department thereof; the friend had knowledge that the computer had been stolen; and the friend received the property with the intent to deprive the United States of the use of the property by converting it to his own use.

As with theft, a defendant accused of receiving stolen property under section 641 need not have knowledge that the stolen property belonged to the United States government or any agency or department thereof, although he does need to know that the property was stolen. Knowledge of who actually owned the property is a jurisdictional issue, not an element of the offense. If the value of the property is over $1,000, the crime is a felony.

OFFICER LIABILITY

I. INTRODUCTION 284
A. CIVIL RIGHTS 284
1. 13th Amendment 285
2. 14th Amendment 285
3. 15th Amendment 286
B. CIVIL LIABILITY 286
1. Definition of a Tort 286
2. Torts Versus Crimes 286

II. FEDERAL CRIMINAL REMEDIES 288
A. TITLE 18 U.S.C. § 241, CONSPIRACY AGAINST RIGHTS 288
1. Elements 289
B. TITLE 18 U.S.C. § 242, DEPRIVATION OF RIGHTS UNDER COLOR OF LAW 290
1. Elements 291
2. "Under Color of Law" 291
3. "Specific Intent (Willfully)" 292

III. FEDERAL CIVIL REMEDIES 293
A. NEGLIGENT TORTS 294
1. Elements 294
a. Duty 294
b. Breach of Duty 296
c. Causation 297
d. Damages 298
B. INTENTIONAL TORTS 298
1. Elements 298
C. CONSTITUTIONAL TORTS 299
1. Title 42 U.S.C. § 1983, Civil Action for Deprivation of Rights 299
a. elements 300
2. Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics 301
a. Bivens analogy 301

IV. COMMON INCIDENTS OF PERSONAL CIVIL LIABILITY... 302
A. NEGLIGENT AND INTENTIONAL TORTS... 302
B. CONSTITUTIONAL TORTS... 302
1. Unlawful Arrest and Searches Without Probable Cause... 303
2. Knowingly False and/or Misleading Probable Cause Affidavits... 304
3. Fourth Amendment Excessive Force Claims During Arrest... 305
4. Failure to Intervene when Excessive Force is Used... 306

V. AVAILABLE DEFENSES TO PERSONAL CIVIL LIABILITY.. 307
A. IMMUNITY... 307
1. Sovereign Immunity... 307
2. Absolute Immunity... 308
B. THE FEDERAL TORT CLAIMS ACT... 308
1. Purposes... 309
2. Definitions... 309
3. Negligent Torts... 310
4. Intentional Torts... 310
5. "Scope of Employment"... 311
a. determination... 311
b. state/local crimes... 312
c. the federal Good Samaritan Act... 312
d. government vehicles... 313
e. certification... 314
6. Procedure... 314
C. QUALIFIED IMMUNITY... 315
D. COMMON DEFENSES... 317
1. Negligent Torts... 317
a. assumption of risk... 317
b. contributory/comparative negligence... 317
2. Intentional Torts... 317
a. consent... 317
b. self-defense/defense of others... 317
c. necessity... 318
E. LEGAL REPRESENTATION BY THE DOJ... 318

I. INTRODUCTION

Law enforcement work is dangerous. Contact with the public is constant, often confrontational and charged with emotion. Within this context, law enforcement officers and agents are responsible for preventing and investigating crimes against "the people," including violations of "civil rights." And, the Constitution and Federal laws protect against the unjustified infringement of those civil rights by law enforcement officers themselves. It is imperative that all law enforcement officers perform their duties in accordance with the Constitution and Federal law. A law enforcement officer who discharges duties unreasonably, recklessly, or indiscriminately, and/or who exceeds the scope of employment and authority may be both civilly and criminally liable for violations of civil rights. Even when civil rights are not violated, the acts of a government employee under color of law or within the scope of employment may give rise to civil liability on the part of that individual employee as well as the employee's respective Federal or state/local governments for the injuries and/or property damage caused by such acts.

A. CIVIL RIGHTS

"Civil rights" are guaranteed to individuals by the Constitution and protected by Federal law. Constitutionally enumerated civil rights include, but are not limited to, the First Amendment's freedom of speech, freedom of religion, and freedom of assembly; the Fourth Amendments protection against unreasonable searches and seizures; the Fifth Amendment's protection against self incrimination and the right of due process; and, the Eighth Amendment's protection against cruel and unusual punishment. Federal statutes add to the list of civil rights, including rights established in the areas of education, employment, voting, and access to public facilities and accommodations.

1. 13th Amendment

Protections for individual civil rights grew out of the period immediately following the Civil War. Congress faced the immediate task of restoring the union and assuring the rights of the former slaves. In 1865, Congress proposed and the States ratified the Thirteenth Amendment, which provided that neither slavery nor involuntary servitude could exist within the United States or any place subject to its jurisdiction. The second section of the Thirteenth Amendment gave Congress the power to "enforce this article by appropriate legislation." This language prompted Congress to pass criminal statutes to enforce the provisions of the Thirteenth Amendment.

However, simply enacting the Thirteenth Amendment failed to ensure the rights and safety of the former slaves. To protect the rights of its newest citizens, the Federal government had to overcome the resistance of some states to recognize the rights of former slaves. In the winter of 1865-66, Congress established a committee to investigate reports of racial violence in the South. The South had created what were called "Black Codes." Under the "Black Codes," people who were black could not own land, vote, marry, enter into contracts, or enter the many normal legal relationships afforded white citizens.

2. 14th Amendment

One of the greatest obstacles to ensuring the rights of former slaves lay in the Constitution itself. Because the Constitution was considered a covenant between the Federal Government and the people, the first ten amendments, commonly known as the Bill of Rights, only applied to the Federal government and did not apply to state and local governments. The Senate had deleted a proposal in the original draft of the Bill of Rights that would also have prohibited the states from violating the Bill of Rights. Consequently, State and local jurisdictions were not required to recognize such Federal individual rights as the protection against unreasonable searches and seizures, the right to due process, and the protection against cruel and unusual punishments.

Because the Federal Government lacked Constitutional authority to prohibit state and local governments from violating individual rights, the Fourteenth Amendment was proposed and ratified in 1868. Through Supreme Court interpretation, this amendment became the cornerstone of Federal protection of individual liberties from infringement by state and local governments. It reads in part, "No *State* shall ... deprive any person of life, liberty, or property, without due process of law." In addition, the Amendment gave authority to Congress to enact legislation, including criminal statutes, to enforce the Amendment's provisions.

3. 15th Amendment

In 1870, the Fifteenth Amendment was ratified. It provides that "The right of citizens of the United States to vote shall not be denied or abridged by the United States or by any State on account of race, color, or previous condition of servitude." In addition, the Fifteenth Amendment granted Congress the power to pass legislation to enforce the Amendment.

B. CIVIL LIABILITY

1. Definition of a Tort

The civil liability of a federal law enforcement officer is predominantly an issue of tort law. The word "tort" is derived from the Latin *tortus*, which means twisted. Broadly speaking, a tort is a civil wrong, other than breach of contract, for which the court will provide a remedy in the form of an action for damages.

2. Torts Versus Crimes

Torts differ from crimes in many respects, primarily in the interests affected by each and in the remedies afforded by each. For instance, a crime is an offense against the public at large, for which the state, as the

representative of the public, will bring proceedings in the form of a criminal prosecution. The style, or blame line, of a Federal criminal prosecution is "The United States v. Defendant." A tort, on the other hand, is a civil action commenced and maintained by the injured person. The style, or blame line, in a civil lawsuit is "Plaintiff (the injured party) v. Defendant (the wrongdoer)." The intent of a criminal prosecution is to protect and vindicate the interests of the public as a whole, by punishing offenders, eliminating them from society, reforming them, and by deterring others from committing similar acts. The penalty upon conviction of a crime is a fine, imprisonment, and sometimes death. Criminal law is not primarily concerned with compensating the victim, although restitution and victim assistance programs may accomplish this end. Tort actions are intended to compensate the victim for the damage they have suffered, at the expense of the wrongdoer. A defendant who loses a lawsuit is assessed money damages (usually the amount that will compensate the victim, but, in certain cases, it can be punitive). An injunction may also be imposed. Torts are private matters that are not usually a concern of the government or the public (unless, of course, the government is a party).

Both criminal prosecutions and civil lawsuits require the proof of "elements." Elements are like the ingredients in a recipe. If you want to cook a particular food dish, you must put in the right amounts of the right stuff or when you pull it out of the oven, you are not going to get what you want. To achieve a conviction in a criminal prosecution, the government must present evidence that proves each and every element of each offense charged beyond a reasonable doubt. To succeed in a civil action, the plaintiff must prove each and every element of each tort alleged by a preponderance of the evidence.

Although there are significant differences between crimes and torts, the remedies are not mutually exclusive. The same act or conduct can be the subject of both criminal prosecution and civil suit.

II. FEDERAL CRIMINAL REMEDIES

In the wake of the ratification of the 13th, 14th, and 15th Amendments, Congress passed criminal statutes designed to punish those who violate the civil rights of others.

A. TITLE 18 U.S.C. § 241, CONSPIRACY AGAINST RIGHTS

This is a Federal criminal conspiracy statute with historical antecedents in the Civil Rights Act of 1870. This statute allows the Federal Government to prosecute anyone, including Federal, state, and local law enforcement officers, who conspire to violate a person's civil rights. It reads as follows:

> *If two or more persons conspire to injure, oppress, threaten, or intimidate any person in any State, Territory, Commonwealth, Possession, or District in the free exercise or enjoyment of any right or privilege secured to him by the Constitution or laws of the United States, or because of his having so exercised the same; or*
>
> *If two or more persons go in disguise on the highway, or on the property of another, with intent to prevent or hinder his free exercise or enjoyment of any right or privilege so secured-*
>
> *They shall be fined under this title or imprisoned not more than ten years, or both; and if death results from the acts committed in violation of this section or if such acts include kidnapping or an attempt to kidnap, aggravated sexual abuse or an attempt to commit aggravated sexual abuse, or an attempt to kill, they shall be fined under this title or imprisoned for any term of years or for life or both, or may be sentenced to death.*

There are two distinct ways in which to violate this statute.

1. Elements

The elements of the first way are:

a. A conspiracy
b. To injure, oppress, threaten or intimidate
c. Any person
d. In the exercise or enjoyment of any Constitutional or Federal civil right.

The conspiracy under this statute is an agreement between two or more persons to injure, oppress, threaten, or intimidate any person in the exercise of a constitutional or federally guaranteed right. Title 18 U.S.C. § 241 differs from Title 18 U.S.C. § 371, the general federal conspiracy statute, by not requiring an overt act; that is, an act in furtherance of the conspiracy. Under § 241, the agreement by two or more persons, coupled with the specific intent to violate a person's civil rights, is sufficient to establish the crime.

"Any person" should be taken literally and includes citizens, visitors, legal and even illegal aliens.

The elements of the second way are:

a. Two or more persons go in disguise on the highway or on the property of another
b. To prevent or hinder
c. Any person
d. In the exercise or enjoyment of any Constitutional or Federal civil right

Going in disguise on the highways or the property of another with the intent to prevent or hinder any person in the free exercise of any Constitutional or federally guaranteed right is also a violation of the

statute. The historical context of this law is apparent. It was specifically designed to go after the Ku Klux Klan.

The crime is always a felony, punishable by up to death.

B. TITLE 18 U.S.C. § 242, DEPRIVATION OF RIGHTS UNDER COLOR OF LAW

This statute, a part of the Civil Rights Act of 1866, empowers the Federal Government to prosecute federal, state, and local law enforcement officers and other public officials who, under the mantel of their official authority, intentionally violate the civil rights of prisoners, suspects, or other persons. It reads as follows:

> *Whoever, under color of any law, statute, ordinance, regulation, or custom, willfully subjects any person in any State, Territory, Commonwealth, Possession, or District to the deprivation of any rights, privileges, or immunities secured or protected by the Constitution or laws of the United States, or to different punishments, pains, or penalties, on account of such person being an alien, or by reason of his color, or race, than are prescribed for the punishment of citizens, shall be fined under this title or imprisoned not more than one year, or both; and if bodily injury results from the acts committed in violation of this section or if such acts include the use, attempted use, or threatened use of a dangerous weapon, explosives, or fire, shall be fined under this title or imprisoned not more than ten years, or both; and if death results from the acts committed in violation of this section or if such acts include kidnapping or an attempt to kidnap, aggravated sexual abuse, or an attempt to commit aggravated sexual abuse, or an attempt to kill, shall be fined under this title or imprisoned for any term of years or for life or both, or may be sentenced to death.*

1. Elements

The elements of this offense are:

a. An activity "under color of law"
b. With the specific intent (willfully)
c. To deprive any person
d. Of any Constitutional or Federal civil right

2. "Under Color of Law"

"Under color of law" means a colorable claim or pretense of authority. It necessarily involves actions on the part of a law enforcement officer or public official, but not everything done by a law enforcement officer is done "under color of law." If status as law enforcement officer did not materially facilitate the wrong committed, the officer is deemed to have acted in a purely private capacity, and will not be criminally liable under this statute. Whenever a law enforcement officer is engaged in the performance of his duties, he is at a minimum asserting a "colorable claim" or "pretense" of Federal, state, or local authority for his conduct. Certainly, when an officer does an act of a general law enforcement nature, such as make an arrest, conduct a search, question a suspect, or quiet down a disorderly person, the officer will be considered to have acted "under color of law." Whether the officer was in uniform or "on duty" in a strict sense are important but not controlling factors in an "under color of law" determination. Law enforcement officers can act "under color of law" even when off duty and out of uniform.

"Under color of law" is a broader legal concept than "within the scope of employment." Even if the law enforcement officer does not purport to have acted in the line of duty and even if the conduct is clearly violates the law and/or agency policy, it will still be treated as "under color" of his Federal, state, or local authority if his status as a law enforcement officer materially facilitated the wrong. Therefore, an officercan act outside the scope of employment and even contrary to law, policy and practice and still be considered to have acted "under color of

law." Misuse of power, possessed by virtue of law and made possible only because the wrongdoer is clothed with the authority of law, is action taken "under color of law." One may not remove, literally and/or figuratively, the badge or mantel of authority, disavow it and thereby avoid prosecution under this statute.

Private persons may be prosecuted under this statute as having acted "under color of law" if they act in concert and jointly engage with law enforcement in the violation of civil rights.

3. "Specific Intent (Willfully)"

It is not enough that the officer intended to do the act that resulted in the deprivation of a constitutional or Federal civil right. To convict of violating § 242, the government must prove the law enforcement officer possessed specific intent to deprive a person of a civil right. Specific intent to injure, or the reckless use of excessive force, without more, does not satisfy the intent requirement of § 242. This statute is not intended to allow prosecution of officers who act negligently. There must be the specific intent to punish or prevent the exercise of a Constitutionally guaranteed right. "Willfully" implies not merely the conscious purpose to do wrong, but intent to deprive person of a right which has been made specific either by terms of the Constitution or Federal law, or by court decisions interpreting them. Requisite intent can be established by all attendant circumstances, such as malice of defendant, weapons used in the assault, the character and duration of the assault, and provocation, if any.

The fact that the law enforcement officer's conduct is also a crime under state law does not insulate him from federal prosecution. The officer can be tried and convicted in both the federal and state courts. In addition to criminal prosecution, the officer may also be subject to administrative action and civil suit.

The crime is always a felony, punishable by up to death.

III. FEDERAL CIVIL REMEDIES

In addition to criminal prosecution, the acts of a government employee under color of law or within the scope of employment may give rise to civil claims against that individual employee as well as the employee's respective Federal or state/local governments even when those acts do not violate "civil rights." As mentioned earlier, the civil liability of a Federal law enforcement officer is predominately an issue of "tort" law.

Since there is no general federal law of torts, tort actions against the Federal government and its employees are defined by the tort law of the state where the damage occurs, even though the action is brought in federal court. Some limitations, however, are imposed by the Federal Tort Claims Act (discussed later).

Tort actions against the federal government and its employees can generally be classified as common law torts (the torts that were recognized under English common law) or as constitutional torts (torts based on a violation of the United States Constitution, often referred to as Bivens or "1983" actions). The traditional common law torts are:

1. **Negligent torts** (such as traffic accidents)

2. **Intentional torts** (such as assault, battery, and false imprisonment)

3. **Strict liability torts** (such as dealing with explosives or other ultra-hazardous activities)

Negligent torts, intentional torts and constitutional torts are the more prevalent forms of liability officers and agents may encounter. For the Federal law enforcement officer, negligence is the most frequently

occurring of the common law torts due to the operation of government motor vehicles.

A. NEGLIGENT TORTS

1. Elements

For a plaintiff to prevail in a tort action, each element of the tort must be proven by a preponderance of the evidence. The general elements of an action for negligence are:

a. Duty
b. Breach of Duty
c. Causation
d. Damages

a. Duty

Generally, there is no affirmative duty to act. That is, the law does not usually require that people intercede, even in situations in which they could prevent property damage, injury, or loss of life at no risk to themselves. Failure to intercede will not create civil liability for death and/or injury and/or property damage. There are, however, exceptions to this general rule.

There is an affirmative duty to act when the plaintiff's peril results from the defendant's own negligence. When the defendant puts the plaintiff in peril, he is expected to intercede to aid the plaintiff.

1) Law Enforcement

In a public service context, courts have held that there is no right to basic public services and, therefore, no requirement that governmental units act when members of the general public are imperiled. This general

rule applies in the law enforcement context as well. There is no general duty to protect the public at large that would create civil liability for the officer and/or agency for failure to do so. There are, however, exceptions to this general rule.

Special relationships can exist between a plaintiff and law enforcement creating an affirmative duty to act, such as when the police promise to protect the target of a threat (i.e. Witness Protection Program, 18 U.S.C. § 3521, et seq.), or when they assure a caller that they are responding to their request for assistance. Failure to do so can result in civil liability when reliance on those specific promises of protection causes the plaintiff to forego steps to protect themselves.

A special relationship will also exist when law enforcement officers have someone in their custody. Once the government takes a person into its custody restricting the person's liberty and, therefore, their ability to protect themselves, there is a duty to assume responsibility for the person's safety and general well being.

Law enforcement officers have an affirmative duty to prevent or stop the violation of civil rights by fellow officers/agents. Failure to do so will result in civil (and possibly criminal) liability to those non-actors who look the other way.

2) Good Samaritan Statutes

Acting when not required to do so will create civil liability when there would otherwise be none. When there is no affirmative duty to act, one who voluntarily acts for the benefit of another assumes a duty to act like a reasonable person. The actor may then be civilly liable for injuries and/or property damage suffered by the person whom they are trying to aid. To encourage medical professionals to intervene to save lives and prevent serious injury when they would otherwise have no legal duty to do so, many states have enacted "Good Samaritan" statutes. These laws protect licensed doctors, nurses, paramedics, EMTs, etc., from civil

liability when they voluntarily render emergency treatment. They are still liable, however, for gross negligence.

b. Breach of Duty

For those to whom the defendant owes or has assumed a duty, the basic standard of care required is that of an objective "reasonable person." A fundamental question in all negligence actions is, "What would a reasonable person have done under the same or similar circumstances?"

Sometimes however, special standards will apply, and the defendant may be required to exercise care beyond that which would be expected of an ordinary "reasonable person." For example, professionals are required to possess and exercise the knowledge and skill of a member of their profession in good standing in the same or similar locality. In such cases, the fundamental question becomes, "What would a reasonable professional have done under the same or similar circumstances?" Furthermore, a professional is required to use such superior judgment, skill, and knowledge as the professional actually possesses.

For law enforcement officers acting within the scope of their employment, for acts of an inherently law enforcement nature, the fundamental question becomes, "What would a reasonable law enforcement officer have done under the same or similar circumstances?"

Breach of duty is proven by showing that the defendant failed to meet the appropriate standard of care. This can be shown by proving that:

1) The defendant exercised care below the standard established by custom or usage

2) The defendant violated a pertinent statute such as a violation of statutory

rules of the road by a Federal employee in driving a motor vehicle in the course of his or her employment

3) The defendant violated agency policies and practices.

c. Causation

The defendant's act which breaches the duty of care must be the cause of plaintiff's damages. There are two aspects to causation: (1) causation in fact and (2) proximate (legal) cause.

Causation in fact is sometimes called "but for ..." causation. If the plaintiff would not have suffered damages "but for the defendant's breach of duty," then there is causation in fact. If the defendant's breach did not in fact cause the plaintiff's damages, the defendant should not be liable.

The second aspect of causation, "proximate (legal) cause," is more complex. There is a limit to legal liability even when causation in fact does exist. At some point, other intervening acts and/or too much time separate the defendant's breach of duty and plaintiff's damages. "Proximate cause" is intended to limit a defendant's liability for damages that are just too far removed in time and/or circumstance.

Acts occurring between defendant's act and the subsequent injury (intervening acts) relieve defendant of liability if such intervening acts are considered to be superseding. Acts such as subsequent medical malpractice, negligence of rescuers, efforts to protect persons or property, subsequent disease, and subsequent accident are reasonably foreseeable are not superseding. Defendant is still liable. Acts such as criminal acts of third persons, intentional torts of third persons, grossly negligent acts of third persons, and acts of God are not reasonably foreseeable. They are superseding and do relieve the defendant of liability.

d. Damages

The last element to be proved in a negligent tort action is damages. Plaintiffs must show that they have suffered personal injury and/or property damage. In civil suits, the plaintiff may recover for the personal injury and/or property damage caused by defendant's breach of duty. The recovery is generally compensatory, designed to make the injured party whole by reimbursing actual expenses and providing for pain and suffering and permanent injury/damage.

B. INTENTIONAL TORTS

1. Elements

For a plaintiff to prevail in a suit alleging an intentional tort, the plaintiff must prove five elements:

a. Duty
b. Act which Breaches Duty
c. Done willfully and intentionally
d. Causation
e. Damages

What distinguishes negligent and intentional torts is that in intentional torts, the act is done purposefully to cause damages. Otherwise, the elements of intentional torts are identical to those for negligent torts.

Intentional torts may be subdivided into intentional torts to the person and intentional torts to property. Examples of intentional torts to the person include:

Assault (plaintiff's reasonable apprehension of an immediate offensive or harmful contact to the plaintiff's person)

Battery (an offensive or harmful contact to the plaintiff's person by the defendant)

False imprisonment (the defendant confining or restraining the plaintiff to a bounded area; in certain cases, confining the plaintiff's personal property may give rise to a suit alleging false imprisonment)

False arrest (a special category of false imprisonment involving the invalid use of the defendant's legal authority in order to confine the plaintiff)

Intentional infliction of emotional distress (plaintiff's emotional distress caused by a defendant's extreme and outrageous conduct)
Examples of intentional torts to property include:

Trespass to land (protection of a persons interest in the real property)

Trespass to chattels (protection of a persons interest in personal property)

Conversion (major interference with a persons possessory rights in property)

C. CONSTITUTIONAL TORTS

1. Title 42 U.S.C. § 1983, Civil Action for Deprivation of Rights

Based on a law first enacted in 1871, Title 42 U.S.C. § 1983, Civil Action For Deprivation of Rights, provides that:

> *Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any*

citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress. For the purposes of this section, any Act of Congress applicable exclusively to the District of Columbia shall be considered to be a statute of the District of Columbia.

This statute provides a civil cause of action against state and local law enforcement officers who, acting under color of law, deprive an individual of any civil right. This is not a criminal statute, but a civil statute that permits state and local law enforcement officers to be civilly sued in federal court for civil rights violations.

a. elements

The elements for an action under this civil statute are:

1. An Action
2. Under Color of Law of State, Territory, or District of Columbia
3. Depriving Any Person
4. Of Rights or Privileges Secured by the Constitution or Federal Law

"Under color of law" is the same legal principle as discussed regarding Title 18 U.S.C. § 242. However, by its express language, this statute applies only to state and local law enforcement and does not apply to Federal officers and agents.

No specific intent to violate a Constitutional or Federal civil right is required. The plaintiff must only prove intent to do the act which results in the deprivation of civil rights. It must, however, be a volitional act and not accidental or the result of misadventure.

The result of an action under this statute may be judgment for actual (compensatory) damages, punitive (exemplary) damages, attorney's fees, and/or injunction.

2. Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics

Until the 1971 Supreme Court decision in Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics, 403 U.S. 388, a person whose civil rights were violated by a federal officer or agent was unable to sue the federal officer or agent in federal court. Title 42 U.S.C. § 1983 was not available since by its language, it applied only to civil rights violations committed by state and local officials. In the Bivens case, Mr. Bivens alleged that agents from the Federal Bureau of Narcotics (now the Drug Enforcement Administration) entered and searched his apartment without a warrant. Mr. Bivens, through his attorney, filed civil suit against the federal agents in federal court. Bivens' attorney argued that these acts violated his client's 4th Amendment right to be safe in his own home from unreasonable searches and seizures, and, therefore, the case raised federal questions appropriately adjudicated in a federal court. Eventually, Mr. Bivens' case reached the Supreme Court on the issue of whether federal agents may be sued in federal court for violations of Constitutionally protected rights. The Supreme Court decided the alleged behavior, if true, would constitute a federal Constitutional wrong which should be determined by a federal court rather than a state court. The Supreme Court also stated that since there was no remedy in state law for wrong doing committed by federal agents, the Court should create such a remedy. The Supreme Court noted that Congress had never explicitly forbidden such suits. Based upon the Bivens decision, federal officers and agents are subject to civil suits alleging intentional civil rights violations.

a. Bivens analogy

The Supreme Court in Bivens, in essence created an analogy to Title 42 U.S.C. § 1983 under which Federal officers and agents may be sued in civil court for violating a person's Constitutional rights. The lawsuit is

commonly called a "Bivens action. Specifically, the Supreme Court has held that a person alleging a violation of rights protected by the 4th Amendment, 5th Amendment (Due Process), and/or 8th Amendment (Cruel and Unusual Punishment) may recover in civil suit for such damages.

Bivens actions are against the individual Federal officer who is personally responsible for defending the lawsuit and paying any resulting settlement or judgment. The Federal officer may request legal representation by the Department of Justice and that the United States Government pay the settlement or judgment. However, the government is under no obligation to do so.

IV. COMMON INCIDENTS OF PERSONAL CIVIL LIABILITY OF FEDERAL LAW ENFORCEMENT OFFICERS

A. NEGLIGENT AND INTENTIONAL TORTS

Without question, the most common type of tort liability incurred by government employees, including law enforcement officers, is negligence. The most common incidents of negligent tort liability are road wrecks, collisions involving government vehicles being driven by government employees during the course of their duties. Intentional torts are the second most frequent type of civil liability involving government employees, especially law enforcement officers. As mentioned earlier, the most common intentional torts are assault, battery, false imprisonment, and false arrest. Individual liability and/or government liability for damages resulting from negligent and intentional torts will be discussed in more detail under The Federal Tort Claims Act.

B. CONSTITUTIONAL TORTS

Although constitutional torts occur much less frequently, they often attract media attention and are much more likely to result in individual

civil liability. The following are the four most common constitutional torts in the law enforcement context.

1. Unlawful Arrest and Searches Without Probable Cause

In Bivens, the Supreme Court held that federal law enforcement officers are civilly liable for violations of the Fourth Amendment to the Constitution. Thus, where a federal law enforcement officer makes an arrest without probable cause, or unlawfully searches without a warrant, consent, or exigent circumstance, a Bivens suit is possible.

In determining whether a Bivens suit for an unlawful warrantless arrest is appropriate, the courts must determine whether "a reasonable officer in the position of the defendant could have believed the arrest to be lawful, in light of clearly established law and the information the arresting officers possessed." In other words, at the moment the arrest was made, were the facts and circumstances within the officer's knowledge and of which he had reasonably trustworthy information sufficient to warrant a prudent man in believing that the person arrested had committed or was committing an offense?

It is inevitable that law enforcement officers will in some cases reasonably but mistakenly conclude that probable cause is present. It is possible for officers of reasonable competence to honestly and fairly disagree over whether probable cause exists.

In determining whether a law enforcement officer is civilly liable for a warrantless arrest, "the issue is not probable cause in fact, but 'arguable' probable cause." There is "arguable" probable cause if a reasonable law enforcement officer could conclude that probable cause exists. Where "arguable" probable cause exists, law enforcement officers who reasonably but mistakenly conclude that probable cause is present are not civilly liable. Officers who act in ways they reasonably believe to be lawful should not be held personally liable.

2. Knowingly False and/or Misleading Probable Cause Affidavits

In Franks v. Delaware, 438 U.S. 154 (1978), the Supreme Court held that a law enforcement officer violates the 4th Amendment if, in order to obtain a search warrant, he perjures himself or testifies in reckless disregard for the truth. It is clearly established that the 4th Amendment requires a truthful, factual showing sufficient to constitute probable cause. Specifically, the Court noted that:

> *Where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause,… and, with the affidavit's false material set to one side, the affidavit's remaining content is not sufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.*

The rationale of Franks also applies where law enforcement officers obtain a warrant through the intentional or reckless omission of material facts.

If the arrest warrant is invalid because probable cause did not, in fact, exist, then the arrest is illegal. If the search warrant is invalid because probable cause did not, in fact, exist, then the search is illegal and the evidence found is excluded. But what about the civil liability of the officer? The Franks standard, although developed in the criminal context, also defines the scope of civil liability in civil rights actions, including Bivens suits. A Franks claim focuses on the statements made by the law enforcement officer in support of the request for a warrant. Where the law enforcement officer reasonably believes that information in a warrant

affidavit is truthful, a Bivens suit is not appropriate. However, where the affidavit contains "information the officer knew to be false or would have known was false had he not recklessly disregarded the truth," the officer violates the 4th Amendment. In such circumstances, a Bivens suit may be properly brought, because the law enforcement officer "cannot be said to have acted in an objectively reasonable manner."

3. Fourth Amendment Excessive Force Claims During Arrest

In Graham v. Connor, 490 U.S. 386 (1989), the Supreme Court established the proper framework for analyzing a claim that a law enforcement officer used excessive force in making an arrest. "The Fourth Amendment's prohibition against unreasonable seizures of the person ... depends not only on *when* it is made, but also on *how* it is carried out." Even when a law enforcement officer has full legal authority to seize someone, the seizure must be done in a reasonable manner. Any claim of excessive force must be analyzed under the general reasonableness requirement of the 4th Amendment. As such, it is necessary to focus on the "objective" reasonableness of the law enforcement officer's actions.

The Supreme Court has long recognized that "the right to make an arrest or investigatory stop necessarily carries with it the right to use some degree of physical coercion or threat thereof to effect it." In cases involving claims of excessive force, the question to be asked is whether the arresting officer's actions were "objectively" reasonable "in light of the facts and circumstances, without regard to their underlying intent or motivation." This "reasonableness" analysis "must be judged from the perspective of a reasonable officer on the scene, rather than with the 20/20 vision of hindsight." If the law enforcement officer acted reasonably based on the facts and circumstances known to the officer at the time of the seizure, then there is no civil liability. Finally, while Graham involved an excessive force claim brought under Title 42 U.S.C. § 1983, the Supreme Court noted that "the same analysis applies to excessive force claims brought against federal law enforcement and correctional officers under Bivens."

4. Failure to Intervene when Excessive Force is Used

A law enforcement officer has an affirmative duty to intercede on the behalf of a person whose constitutional rights are being violated in his presence by other officers. Accordingly, a federal law enforcement officer may, in certain circumstances, be sued pursuant to Bivens for failing to intervene to protect a victim from another officer's unlawful use of excessive force. By accepting appointment as a federal law enforcement officer, each of you accepts the responsibility to uphold the Constitution of the United States, including an individual's 4th Amendment right to be free from the excessive use of force by law enforcement officers. One who is given the badge of authority of a police officer may not ignore the duty imposed by his office and fail to stop other officers who summarily punish a third person in his presence or otherwise within his knowledge.

It is not necessary that an officer actually participate in the excessive use of force to be held liable. Rather, an officer who is present at the scene and who fails to take reasonable steps to protect the victim from another officer's use of excessive force can be held liable for his nonfeasance.

An officer who fails to intercede is liable for the preventable harm caused by the actions of the other officers where that officer observes or has reason to know: (1) that excessive force is being used; (2) that a citizen has been unjustifiably arrested; or (3) that any constitutional violation has been committed by a law enforcement official.

A Federal officer who "fails or refuses to intervene when a constitutional violation such as an unprovoked beating takes place in his presence" can be held liable under Bivens. However, the excessive use of force must be "of sufficient duration to support a conclusion that an officer who stood by without trying to assist the victim became a tacit collaborator." In order for liability to attach, there must have been a realistic opportunity to intervene to prevent the harm from occurring.

While most of the cases that recognize this cause of action involve state officials being sued under § 1983, "the general trend in the appellate courts is to incorporate § 1983 law into Bivens suits." Since the remedial purposes of Bivens and § 1983 are essentially the same, appellate courts have generally looked to the principles established in the case law construing § 1983 when deciding cases brought under Bivens.

V. AVAILABLE DEFENSES TO THE PERSONAL CIVIL LIABILITY OF FEDERAL LAW ENFORCEMENT OFFICERS

There are several possible defenses to civil liability. Immunity is an entitlement not to stand trial or face the other burdens of litigation. The privilege is an immunity from suit rather than a mere defense to liability. It does not depend so much on the specific facts of a given case, but rests primarily on the status of the defendant. These immunities include "sovereign immunity," "absolute immunity," and "qualified immunity." In addition, there are "common defenses" to civil liability. Common defenses go to the merits of the allegations and focus primarily on the particular facts of the case. Common defenses to negligent torts include "assumption of risk" and "contributory/comparative negligence." For intentional torts, they include "consent," "self defense/defense of others," and "necessity." Finally, failure of the plaintiff to prove each and every element of the tort alleged by a preponderance of the evidence should result in a verdict that the defendant is not liable.

A. IMMUNITY

1. Sovereign Immunity

Sovereign (governmental) immunity has its common law roots in the theory that "the King can do no wrong." This theory was an outgrowth of the divine rights of kings, and, in effect, prevented any and all lawsuits against the Crown. What arm of the government had the power and authority to order the divinely appointed supreme ruler to pay damages or cease and desist certain actions?

When the individual sovereign was replaced by the broader concept of the modern state, the principle was adapted to provide that a suit against a ruling government without its consent was inconsistent with the very idea of supreme executive power. In 1821, Chief Justice Marshall wrote that no suit could be commenced or prosecuted against the United States without its consent. This concept was reinforced in 1907, when Mr. Justice Holmes wrote that, "A sovereign is exempt from suit not because of any formal conception or absolute theory, but on the logical and practical ground that there can be no legal right as against the authority that makes the law on which the right depends." Public policy and necessity dictate that "the United States as sovereign is immune from suit save as it consents to be sued…and the terms of its consent to be sued in any court define the court's jurisdiction to entertain the suit."

2. Absolute Immunity

"Absolute immunity" avoids personal, civil liability. It is conferred because of the status or position of the favored defendant. Officials, such as the President, legislators, judges, and prosecutors, whose special functions or constitutional status requires complete protection from suit, may assert the defense of absolute immunity for acts within the performance of their duties.

B. THE FEDERAL TORT CLAIMS ACT

Before 1946, if a person was injured and/or suffered property damage as the result of an act by an employee of the Federal government within the scope of employment, the principal way of redressing such torts was through special legislation. The injured parties would contact their Congressman and request that a bill be introduced in Congress to compensate them for their loss. Thousands of "private bills" were considered each year, clogging the legislative process. The injured party could also sue the employee individually, but that was often unfair and impracticable. Shortly after World War II, several disasters involving

possible negligence by government employees clearly demonstrated the need for a more effective procedure for compensation. Congress responded by enacting the Federal Tort Claims Act (FTCA) in 1946. This act, as amended, makes the United States liable under the local law of the place where the tort occurs for the negligent or wrongful acts or omissions of Federal employees within the scope of their employment "in the same manner and to the same extent as a private individual under like circumstances."

1. Purposes

The purposes of the FTCA are (1) to provide persons injured by the common law torts of Federal employees with an appropriate remedy against the United States (a waiver of sovereign immunity), and (2) to protect Federal employees from personal liability for common law torts committed within the scope of their employment (absolute immunity).

However, the FTCA is not a total waiver of sovereign immunity. For example, the FTCA provides that the United States shall not be liable for punitive damages; there is no provision for attorney's fees against the government; there is no right to trial by jury; and, there are a number of exceptions to the general rule of tort liability of the United States.

2. Definitions

Most of the FTCA can be found at 28 U.S.C. §2671 et seq. Two of the key definitions contained in §2671 are:

"**Federal Agency**" includes the executive departments, the judicial and legislative branches, the military departments, independent establishments of the United States, and corporations primarily acting as instrumentalities or agencies of the United States, but expressly excludes any contractor with the United States.

"**Employee of the government**" includes officers or employees of any Federal agency, members of the military or naval forces of the United

States, members of the National Guard while engaged in training or duty, and persons acting on behalf of a Federal agency in an official capacity.

3. Negligent Torts

The FTCA provides a remedy against the United States for property damage, personal injury or death arising or resulting from the negligent or wrongful act or omission of any employee of the government while acting within the scope of office or employment. It is the exclusive remedy. In other words, such a claim must be brought against the United States, and a lawsuit against the individual Federal employee personally is prohibited. The Federal employee has absolute immunity.

The United States has waived sovereign immunity and consented to be liable "in the same manner and to the same extent as a private individual under like circumstances," reserving the right to assert judicial or legislative immunity, as well as any other defense to which it is entitled.

The United States also has not waived sovereign immunity regarding any claim based upon intentional torts.

4. Intentional Torts

The Act specifically excludes government liability for intentional torts committed by Federal employees. Assault, battery, false imprisonment, false arrest, malicious prosecution, abuse of process, libel, slander, misrepresentation, deceit, or interference with contract rights are specifically listed.

Since assault, battery, false imprisonment, false arrest, malicious prosecution, and abuse of process are common allegations against law enforcement officers, the exclusion from coverage of these acts created a real hardship for law enforcement officers and agents. Therefore, in 1974

the Act was amended to provide that if the act was that of an **"investigative or law enforcement officer,"** the government will permit itself to be sued with respect to assault, battery, false imprisonment, false arrest, malicious prosecution, or abuse of process.

"Investigative or law enforcement officer" means any officer of the United States who is empowered by law to execute searches, ***or*** to seize evidence, ***or*** to make arrests for violations of Federal law. All three are not required; any one or more of those criteria will qualify.

5. "Scope of Employment"

The United States is liable for the negligent or wrongful acts or omissions of Federal employees within "the scope of their employment." If the property damage and/or personal injury was caused while the Federal employee was acting "outside the scope of employment," the United States is not liable. The Federal employee would, however, be personally liable. Scope of employment is defined by reference to the general concept of tort law called respondeat superior.

a. determination

Was the employee performing the employer's (Federal government) business at the time of the occurrence? The answer is determined by consideration of all the facts and circumstances, the employee's job description, and agency policies as promulgated through directives and general orders.

Scope of employment can be limited in a number of different ways. Law enforcement officers for some agencies and departments have broad authority to investigate and arrest anywhere for any federal crime. Others are limited to certain federal offenses and/or certain defined geographical areas. Exceeding these limitations can mean that the law enforcement officer is "outside the scope of employment."

b. state/local crimes

What about state/local crimes? Generally, Federal law enforcement officers who intervene in purely state/local criminal offenses are outside the scope of employment. There is no affirmative duty to intervene and, therefore, no civil liability for failure to do so. However, voluntary intervention in state/local incidents can create liability for both the individual law enforcement officer and the agency or department when there would otherwise be none. Even though states my grant varying degrees (up to full) of peace officer status to Federal law enforcement officers, many agency and department policies prohibit officers and agents from getting directly involved in state/local incidents.

c. the federal Good Samaritan Act

Many federal agents/officers were reluctant to intercede in state criminal violations occurring in their presence for fear of being outside their "scope of employment" and, therefore, personally liable. In 1998, Congress enacted the "Federal Law Enforcement Officers' Good Samaritan Act." It applies only to law enforcement officers as defined in 5 U.S.C. 8401(17). Not every federal law enforcement officer is covered, but for those who are, the Act provides that they are "within the scope of employment" when taking reasonable action, including the use of force:

1) To protect an individual in the presence of an officer from a crime of violence;

2) To provide immediate assistance to individuals who have suffered or who are threatened with bodily harm; or

3) To prevent the escape of any individual whom the officer reasonably believes to

have committed in the presence of the officer a crime of violence.

In essence, it extends the federal scope of employment to non-federal crimes of violence being committed in the federal officer's presence. But, because this law is still relatively new, the contours of its protections are not clearly defined. Does it obligate the Department of Justice to provide legal counsel to the federal officer/agent? Does it mandate that the United States indemnify the officer/agent for any damages, even for Constitutional torts, should the claim be successful? There are no clear answers. There remains some risk that intervening in purely state/local incidents will be outside the scope of employment and outside the purview of the FTCA, exposing the individual officer/agent to personal, civil liability.

d. government vehicles

Another common scope of employment issue involves the use of government vehicles. When is the use of a government vehicle considered outside the scope of employment? Agency/department policies and procedures generally outline authorized and prohibited uses. State law often defines scope of employment in the use of government vehicles in terms of "official business" and "personal frolic." State laws vary over how much of a deviation (both in purpose and distance) is required to put the use outside the scope of employment. A law enforcement officer found to have used a government vehicle outside the scope of employment will not be protected by the FTCA and will, therefore, be personally liable for the injury and damages caused. KNOW, UNDERSTAND, AND FOLLOW pertinent agency policies and procedures.

Once the facts are determined, the law of the state where the alleged injury occurred is applied to decide whether the employee was "within the scope of employment."

e. certification

The agency makes the initial decision on scope of employment when presented with a claim. If the agency refuses to certify that the employee was acting within the scope of employment, the employee may request the Attorney General to so certify. If the Attorney General refuses to certify scope of employment, the employee may petition the U.S. District Court to find and certify that the employee was acting within the scope of employment. Upon certification by the Agency, the Attorney General, or the Federal District Court that the defendant employee was acting within the scope of employment, the United States shall be substituted as the party defendant.

6. Procedure

Before filing a lawsuit against the government, a claimant must exhaust administrative remedies. A claim is first filed with the employee's agency. That agency has 180 days during which to investigate the claim. Most Federal agency heads may settle tort claims of $25,000 or less, but settlements in excess of $25,000 require the prior approval of the Attorney General. Acceptance of a settlement by a claimant is final and conclusive, and constitutes a complete release of any claim against the United States and against the employee of the government whose act or omission gave rise to the claim.

The claimant may file suit only after the claim has been administratively denied; that is, the agency has outright denied responsibility or the claimant has refused the Government's final offer of settlement. The U.S. District Court has exclusive jurisdiction over civil actions on Federal Tort Claims against the United States. Furthermore, the trial in District Court will be a bench trial without a jury.

A tort claim against the United States is barred unless it is presented in writing to the appropriate federal agency within two years of

the date of the injury/damage. Suit may be filed beyond that two year limit so long as it is within six months of the date of the final denial of the claim by the agency to which it was presented.

C. QUALIFIED IMMUNITY

The absolute immunity afforded Federal employees under the FTCA against personal liability for common law torts does not apply in a Bivens action alleging a constitutional tort.

Qualified immunity (sometimes called "good faith" immunity) can shield government officials, including law enforcement officers, from personal liability for damages in constitutional torts provided they (1) act reasonably and in good faith, and (2) their conduct does not violate clearly established statutory or constitutional rights of which a reasonable law enforcement officer would have known.

In Hanlon v. Berger, 526 U.S. 808 (1999), and Wilson v. Layne, 526 U.S. 603 (1999), the plaintiffs sued federal agents under Bivens, alleging violations of the 4th Amendment when the agents brought the media along during the service of an arrest warrant and a search warrant at a residence. In Wilson, Federal Marshals took a newspaper reporter and photographer along when they attempted to serve an arrest warrant at the home of the suspect's parents. In Hanlon, Federal Fish and Wildlife Service agents took CNN along when they served a search warrant at the Berger ranch. Both followed established agency ride along policies.

The Supreme Court had two questions to decide:

1. Would the facts as alleged by plaintiff be a constitutional tort? In this case, is the sanctioned presence of media at the service of arrest and/or search warrants in residences unreasonable under the 4th Amendment?

The Supreme Court held that police violate the 4th Amendment rights of homeowners by bringing members of the media or other third parties into homes during the execution of a warrant, when the presence of the third parties in the home is not in aid of the warrant's execution. In other words, these federal agents had committed a constitutional tort.

2. Are these agents entitled to qualified immunity? Was the right violated clearly established at the time the officers acted?

In assessing whether a law enforcement officer is protected by qualified immunity, the test to be applied is one of objective reasonableness. The subjective beliefs of an officer regarding the reasonableness of his actions are irrelevant. In these cases, the Supreme Court held that the agents acted reasonably and in good faith, relying on their established policy for media "ride alongs" and/or the fact that media ride alongs were a widespread practice. The Court focused on the second requirement. Was the right violated clearly established at the time of the officers' action? At that time, would a reasonable law enforcement officer have known that media ride alongs on search/arrest warrants at residences violated the 4th Amendment? In assessing whether the right that was allegedly violated is "clearly established," the test is whether, in the light of preexisting law, the unlawfulness of the act is apparent. Put another way, the contours of the right must be sufficiently clear that a reasonable law enforcement officer would understand that what he is doing violates that right. The Court held that it was reasonable for these agents to have believed that bringing the media along during the execution of an arrest or search warrant (even in a home) was lawful. The right was not clearly established. Therefore, the agents were entitled to qualified immunity.

To broadly summarize, where the qualified immunity is applicable, officers will *not* be held personally liable as long as their actions are reasonable in light of current, established law.

D. COMMON DEFENSES

There are several common defenses available to every defendant to the extent that the defenses are recognized in the state where the tort occurred.

1. Negligent Torts

a. assumption of risk

If a plaintiff has voluntarily placed himself in a position of harm, knowing the dangers involved, the defendant will not be responsible for the subsequent injury to plaintiff. Plaintiff has assumed the risk of such injury.

b. contributory/comparative negligence

If the plaintiff has been negligent, and that negligence is a cause of the plaintiff's damages, then, depending on the law of the state where the incident occurred, the plaintiff may be prevented from recovering anything against the defendant or may have the recovery apportioned according to the degree of culpability of each.

2. Intentional Torts

a. consent

Knowing and voluntary consent by plaintiff will bar recovery against defendant. However, defendant's actions must stay within the bounds of the consent. In other words, defendant's actions must not exceed what a reasonable person would believe they are giving defendant permission to do.

b. self-defense/defense of others

Reasonable force may be used to defend oneself and others against

harmful or offensive bodily contact. "Reasonable force" is a fact intensive concept. The general rule is that only such minimal force as is necessary to prevent the harm is allowed. If excessive force is used, this defense is not available.

c. necessity

A defendant who acts to prevent a threatened injury from some force of nature or other cause not brought on by the defendant is acting under necessity. Such a defendant may not be liable for a lesser harm committed to prevent or avoid a greater harm.

E. LEGAL REPRESENTATION BY THE DEPARTMENT OF JUSTICE

The authority for the Department of Justice (DOJ) to provide legal representation for employees named individually as defendants in civil actions is found in Title 28 U.S.C. §516-519. It is the responsibility of the Attorney General to "attend to the interests of the United States" in any court in the land and "to supervise all litigation to which the United States, an agency, or officer thereof is a party,…." Among the "interests" of the United States is the representation of its employees who are sued for acting within the scope of their employment. This representation is provided more to protect the interest of the United States than the individual interest of the employee, although the private and public interests usually coincide. However, there is no obligation to any particular employee to provide representation.

A Federal employee may be provided representation in civil proceedings and in state criminal proceedings in which he is sued, subpoenaed, or charged in his individual capacity when:

1. The actions for which representation is requested reasonably appear to have been performed within the scope of the employee's employment, and

2. Providing representation would otherwise be in the interest of the United States.

There is usually an interest in the United States in defending the conduct of the program in which the employee was engaged. There is also an additional interest in employees' morale. However, interest of the United States has been found to be lacking in cases:

1. That were of *de minimis* nature (e.g. minor traffic ticket);

2. That involve a swearing contest between two co-equal employees arising out of an altercation;

3. Where the subject employees apparently did not tell the truth or otherwise covered up wrongdoing in the course of an official investigation following the incident; and

4. Where the Department has been asked to undertake representation at so late a stage in the representation as to be handicapped in effectively doing so.

A Federal employee confronted with a civil suit or state criminal action which he believes to be based on his performance of official duties should submit "forthwith" a request for DOJ representation. This request should be forwarded through his immediate supervisor or the person designated by his agency head, together with all process and pleadings already served. DOJ will determine whether the employee's actions "reasonably appear to have been performed within the scope of his employment," and whether providing representation would be in the interest of the United States.

DOJ attorneys participating in a determination of whether to provide representation "undertake a full and traditional attorney-client relationship with the employee with respect to application of the attorney-client privilege." Thus, adverse information communicated by the client-employee to the attorney "shall not be disclosed to anyone, either inside or outside DOJ, unless such disclosure is authorized by the employee."

Representation is not available in Federal criminal proceedings, and if the employee is the subject of Federal criminal investigation concerning the act for which he seeks representation, DOJ will not provide attorneys in any related civil or state criminal proceeding. But DOJ, in its discretion, may furnish a private attorney to the employee at Federal expense, provided that no decision has been made to seek an indictment or file an information against the employee.

DOJ will not assert any legal defense on behalf of any employee sued in his individual capacity which is deemed not to be in the interest of the United States.

The government is not obligated to pay or to indemnify the defendant employee for any judgment for money damages which may be rendered against the employee, but the employee may apply for such indemnification from his employing agency upon entry of an adverse verdict, judgment, or other monetary award.

If conflicts exist between the legal and factual positions of various employees in the same case which make it inappropriate for a single attorney to represent them all, the employees may be separated into as many compatible groups as is necessary to resolve the conflict problem, and each group may be provided with separate representation.

SELF-INCRIMINATION

I. INTRODUCTION 323
A. FIFTH AMENDMENT DUE PROCESS ISSUES 323
B. LINE-UPS, SHOW-UPS AND PHOTO DISPLAYS 324

II. THE PRIVILEGE AGAINST SELF-INCRIMINATION 325
A. FOURTH AMENDMENT ISSUES 325
1. Testimonial Evidence 325
2. Non-Testimonial Evidence 325
B. GENERALLY 326
C. CORPORATE/PARTNERSHIP RECORDS 328
D. IMMUNITY 328
E. ADMINISTRATIVE INVESTIGATIONS 330
F. VOLUNTARINESS 330

III. MIRANDA 331
A. THE DECISION: MIRANDA v. ARIZONA 331
B. UNITED STATES v. DICKERSON 333
C. WHEN THE WARNINGS ARE REQUIRED 334
1. Police 334
2. Interrogation 335
3. Custody or Otherwise Deprived of Their Freedom of Action in a Significant Way 336
D. EXCEPTIONS TO MIRANDA 337
1. Officer/Public Safety 337
2. Impeachment 337

IV. WAIVER OF MIRANDA RIGHTS 338
A. VOLUNTARY 339
B. KNOWING AND INTELLIGENT 339

V. INVOKING MIRANDA RIGHTS 339
A. SILENCE 340
B. COUNSEL 340
C. THE RULE IN ARIZONA v. ROBERSON 341

VI. THE SIXTH AMENDMENT RIGHT TO COUNSEL 342
A. ADVERSARIAL JUDICIAL PROCESS 343
B. QUESTIONING 344
C. STATEMENTS ON UNCHARGED MATTERS 344
D. WAIVER OF THE SIXTH AMENDMENT RIGHT TO COUNSEL ... 345

I. INTRODUCTION

Admissions constitute the strongest evidence of guilt. This text is intended to acquaint the student with legal issues the government may encounter presenting these statements to a jury. In deciding whether such evidence is admissible, courts consider the Fourth Amendment prohibition against unreasonable search and seizures, the Fifth Amendment due process clause and the privilege against compelled self-incrimination, and the defendant's Sixth Amendment right to assistance of counsel for their defense.

A. FIFTH AMENDMENT DUE PROCESS ISSUES

The Due Process clause of the Fifth Amendment applies to testimonial and non-testimonial evidence. Due process is a principle of justice that requires each case be resolved in a manner consistent with fundamental fairness. The government cannot deprive a person of rights except by observing procedural requirements. To deny a person of due process is to deny fundamental fairness.

Due process issues may arise when a defendant claims that an identification procedure is impermissibly suggestive. Foster v. California. A lineup, show-up or photo display may not be so impermissibly suggestive as to create a substantial likelihood of misidentification of the suspect as the perpetrator of a crime. While many crimes are committed in an instant, police officers must take care not to taint the witnesses' identifications of suspects by pointing out physical characteristics, location of apprehension or other factors. Eyewitnesses must be able to identify the perpetrators of crimes based on their memory of the event, not the prodding or carelessness of a police officer. Impermissibly suggesting that the arrested individual is the perpetrator of the crime is a violation of that person's due process right to be treated fairly.

B. LINE-UPS, SHOW-UPS AND PHOTO DISPLAYS

Officers may use line-ups, show-ups and photo displays in their investigations. Each is a tool that assists the government in determining if the person it has arrested is the perpetrator of the crime. A line-up consists of the arrested individual and several others with similar physical appearances. The government then anonymously presents these individuals to eyewitnesses to determine if they can identify the perpetrator of the crime. It is important that the government refrain from suggestive activity to the eyewitnesses. Once the eyewitnesses have identified the perpetrator, they are inclined to recall the physical appearance of the suspect from their encounter in the line-up instead of their encounter with the perpetrator at the crime scene. If the eyewitnesses' identification was from the line-up was tainted by inappropriate government suggestion, the trial court will most likely disallow the eyewitness from repeating their identification of the defendant at trial.

Show-ups consist of police officers presenting just the arrested individual an eyewitness to determine the soundness of the arrest. For this reason, show-ups are inherently suggestive. A show-up may be appropriate in certain instances to preserve identification of a suspect. For instance, the police may have to, out of necessity, return an apprehended suspect to the scene or present that person to a witness to preserve identification evidence. In one instance where a doctor was murdered and his wife, the only witness, was severely injured, police took the suspect to the victim's hospital room where the victim identified the suspect as her husband's murderer. The victim/wife was the only witness who could clear the suspect and her injuries were such that she too might pass on. The Supreme Court held these compelling exigent circumstances necessitated the show-up. The only feasible procedure was the show-up. Stovall v. Denno.

II. THE PRIVILEGE AGAINST SELF-INCRIMINATION

The self-incrimination clause of the Fifth Amendment applies only to testimonial evidence, i.e., evidence that is communicative in nature. It comes from a person's thought processes and can be oral, written, nonverbal, or conduct. The Fourth, Fifth, and Sixth Amendments protect testimonial evidence.

Non-testimonial evidence is that which tends to identify a person, such as fingerprints, blood samples, handwriting exemplars, voice prints, the uttering of certain words at a line-up, etc. Non-testimonial evidence is *not* protected by the self-incrimination clause of the Fifth Amendment, but is protected by the Fifth Amendment's due process clause and the Fourth Amendment.

A. FOURTH AMENDMENT ISSUES

1. Testimonial Evidence

Evidence obtained because of an illegal arrest generally will be inadmissible in a subsequent criminal trial. A confession made at a police station after the accused was "picked up for questioning" could not be used at trial where the initial detention was an arrest without probable cause and the confession was the fruit of that illegal action by the police. Dunaway v. New York.

If an arrest is otherwise legal (e.g., an arrest in a person's residence with probable cause but without an arrest warrant), any statement made after the accused is removed from the residence and taken to jail would not be a product of unlawful custody. New York v. Harris.

2. Non-Testimonial Evidence

Non-testimonial evidence is divided into two groups: evidence that is obtained by either (1) an intrusive or (2) a non-intrusive search or seizure. Non-intrusive evidence is that which is outside the body;

intrusive evidence is that which the government obtains from inside the body. To obtain intrusive evidence, such as a bullet or blood, the Fourth Amendment requires either a warrant or an exception to the warrant requirement. This evidence is non-testimonial in nature, as the government is not asking the suspect to provide information from his or her mental processes. The Supreme Court held that taking of intrusive evidence was a seizure under the Fourth Amendment and, unless exigent circumstances exist, police must get a search warrant before obtaining such evidence. Courts measure exigent circumstances against whether or not there is sufficient time to obtain a search warrant. For example, obtaining blood to determine a blood alcohol level would constitute an exigency as the alcohol level in blood diminishes with time. Schmerber v. California.

The government can obtain non-intrusive evidence without a search warrant. Compelling one to stand in a line-up, utter certain words (for voice identification), write a specific statement (for handwriting analysis), etc., are examples of non-testimonial evidence that the government can obtain without the requirement of a warrant. United States v. Dionisio, United States. v. Mara.

B. GENERALLY

The Fifth Amendment states, in part, that "no person... shall be compelled in any criminal case to be a witness against himself." The privilege applies when a testimonial communication is introduced at trial, and that communication is proven to be compelled.

Evidence seized from the accused's home or office pursuant to a search warrant is not privileged because the accused has not been compelled to produce the evidence. Any evidence seized would be the result of a search pursuant to the warrant. Andresen v. Maryland. The Supreme Court has made it clear that the Fifth Amendment does not protect the contents of private papers that are voluntarily created. While

the contents of private papers are not protected, producing such records under a subpoena is privileged if the production is used to authenticate or otherwise connect the individual producing the records to them and cannot be compelled without a grant of immunity. United States v. Doe.

Third parties are not privileged when asked to turn over records belonging to another. Couch, a sole proprietress, turned over records to her accountant who, in turn, was ordered to turn these records over to the Internal Revenue Service. The Supreme Court held that compelling the accountant to turn over the records was not compelling him to do anything. Couch v. United States.

The target of a grand jury investigation can be compelled to sign a form authorizing foreign banks to disclose records of their accounts because such action compels nothing of a testimonial nature. The person is not being asked to admit that certain accounts exist; the signature is to satisfy the banks' requirements of authorization to release any information on accounts maintained by the person. Doe v. United States.

Generally, silence in the presence of police questioning cannot be used to indicate guilt or impeach the witness. Likewise, the fact that an accused has invoked the right to remain silent after given Miranda warnings cannot be introduced to infer guilt; i.e., a witness who testifies on direct examination that the defendant exercised Miranda rights may create a mistrial. However silence in response to an accusation made by someone other than a law enforcement officer may constitute an adoptive admission of the accusation.

The privilege does not apply when the statute of limitations has run. When the statue of limitations has run, there can be no criminal prosecution of a person for that crime. Therefore, it does not violate the privilege to compel testimony in this situation.

C. CORPORATE/PARTNERSHIP RECORDS

The privilege does not apply to corporations. Since corporations can act only through their officers and employees, the custodian of corporate records can be compelled to produce the records even though there is information in the records that will incriminate the custodian. The courts reason that the custodian only holds the records in a representative capacity; i.e., the records belong to the corporation and not to the custodian. Of course, the custodian may not be compelled to answer questions about the records to the extent that the records would tend to incriminate.

The production of corporate records can be compelled under the Fifth Amendment even when the custodian of those records is the only person involved in the operation of that corporation. Evidence that the custodian produced the records cannot be used to authenticate or otherwise establish the source of the records. Braswell v. United States.

A partnership is treated like a corporation for Fifth Amendment purposes. A partnership is a collective entity of persons formed for the purpose of doing business. A partner cannot rely upon the privilege to avoid producing records of the partnership which are in their possession in a representative capacity as custodian of records. This might not be the case if the partnership is a small family partnership. Bellis v. United States.

D. IMMUNITY

The privilege does not apply to persons who have been granted immunity from prosecution. There are two types of immunity: use and transactional. The Supreme Court has ruled that the government has the discretion of whether to grant immunity and which type of immunity to grant. Title 18 U.S.C. §§ 6002-6005 provides statutory guidance on immunity and the type of immunity the government is allowed to grant in

return for a person's testimony.

Title 18 U.S.C. § 6002 provides as follows:

> *Whenever a witness refuses, on the basis of his privilege against self-incrimination, to testify or provide other information in a proceeding before or ancillary to-*
>
> *(1) a court or grand jury of the United States,*
>
> *(2) an agency of the United States, or*
>
> *(3) either House of Congress, a joint committee of the two Houses, or a committee or a subcommittee or either house,*
>
> *and the person presiding over the proceeding communicates to the witness an order issued under this title, the witness may not refuse to comply with the order on the basis of his privilege against self-incrimination; but no testimony or other information compelled under the order (or any information directly or indirectly derived from such testimony or other information) may be used against the witness in any criminal case, except a prosecution for perjury, giving a false statement, or otherwise failing to comply with the order.*

Under a grant of use immunity, also called testimonial immunity, the government may not prosecute the witness with immunized testimony or any information derived from it. The witness could be tried for an offense to which the immunized testimony related using evidence already in the government's possession or obtained subsequently from an independent source.

Transactional immunity means that the witness may not be tried subsequent to their testimony for *any crimes related* to their testimony. A person does not have a constitutional right to transactional immunity instead of use immunity.

E. ADMINISTRATIVE INVESTIGATIONS

Most agencies require their employees to cooperate in official investigations and agency directives state that failure to cooperate with an investigation can lead to disciplinary action. When interviewing a suspect under these circumstances, officers must take care to advise the suspect of the privilege against self-incrimination and that no penalty will ensue from the exercise of that right. If the suspect proves that their confession was the result of their fear of being fired, the statements may be excluded in a criminal case. Garrity v. New Jersey. Gardner v. Broderick.

If the Department of Justice has decided it will not prosecute the case, the suspect need not be provided the Miranda warnings. A person does not have a constitutional right to federal employment. A person who is being questioned under these circumstances must first be advised that their answers can be used against them in any administrative action but not in subsequent criminal actions. These warnings are commonly referred to as the Garrity or Kalkines warnings. After being advised of these warnings, employees must truthfully answer any questions asked regarding the investigation. Failure to answer truthfully can result in a criminal prosecution for making a false statement. Garrity v. New Jersey. Kalkines v. United States.

F. VOLUNTARINESS

To be admissible at trial, admissions and confessions must be voluntarily given. An admission is any statement or act of a party that an opponent is offering into evidence against that person. A confession is a comprehensive statement of a person that admits all the necessary elements of the offense. In cases where the warnings required by the Miranda decision have been provided a defendant will rarely be able to make a plausible claim that an incriminating statement was obtained involuntarily as a matter of law. United States v. Dickerson

Officials of the government may not overcome the defendant's will. A statement is not voluntary if obtained by force, threats or promises of reward. On the other hand, an admonition to tell the truth or the standard statement about cooperation ("Your cooperation will be called to the attention of the U.S. Attorney and/or the Judge") will not render a subsequent statement involuntary.

Voluntariness turns upon the "totality of the circumstances." In addition to tactics used by law enforcement officers to induce a person to confess, courts consider such things as the person's age, education, intelligence, the use of drugs or alcohol, and whether there was any delay in taking the person to the magistrate judge for an initial appearance.

The key inquiry is whether the actions of law enforcement officers would overbear a person's will to resist. Some deception is permissible. For example, falsely telling a suspect that officer found his fingerprints at the scene of the crime did not invalidate a subsequent confession since an innocent person would know his fingerprints could not have been found at the scene. Oregon v. Mathiason.

Voluntariness is at issue when there is pressure to admit to wrongdoing in return for protection while in prison. In one case, a government informant was trying to obtain incriminating information relating to a murder case from a fellow inmate who was in prison on weapons charges. The informant told the defendant that if he confessed to the murder, the informant would provide protection from other inmates. The Supreme Court said this was unacceptable coercion since knowledge of threats was used to obtain the confession. Arizona v. Fulminante.

III. MIRANDA

A. THE DECISION: MIRANDA V. ARIZONA

On March 13, 1963, police arrested Ernesto Miranda and took him to a Phoenix police station where the victim identified him. The police then took Miranda to an interrogation room where two police officers

questioned him. The officers emerged from the interrogation room two hours later with a written confession signed by Miranda. At the top of the statement was a typed paragraph stating that the confession was made voluntarily, without threats or promises of immunity and "with full knowledge of my legal rights, understanding any statement I make may be used against me."

At trial, the officers admitted that they did not advise Miranda that he had a right to have an attorney present. The trial court admitted the written confession into evidence over the objection of defense counsel, and the officers testified to the prior oral confession made by Miranda during the interrogation. The jury found Miranda guilty.

On appeal, the Supreme Court of Arizona held that Miranda's constitutional rights were not violated in obtaining the confession and affirmed the conviction. In reaching its decision, the court emphasized the fact that Miranda did not specifically request counsel.

The United States Supreme Court reversed the Arizona court, stating,

> *[F]rom the testimony of the officers and the admission of respondent, it is clear that Miranda was not in any way apprised of his right to consult with an attorney and to have one present during the interrogation, nor was his right not to be compelled to incriminate himself effectively protected in any other manner.*

The Court said the mere fact that he signed a statement that contained a typed-in clause stating he had full knowledge of his legal rights was not sufficient notice.

The Supreme Court held:

> *[W]hen an individual is taken into custody or otherwise deprived of his freedom of action in any significant way, and is subjected to questioning... [h]e must be warned prior to any questioning that he has the right to remain silent, that anything he says can be used against him in a court of law, that he has the right to the presence of an attorney, and that if he cannot afford an attorney one will be appointed for him prior to any questioning if he so desires.*

The Court went on to say that the opportunity to exercise the rights must be afforded throughout questioning. The Court does not require law enforcement officers to advise people that they may stop the questioning at any time.

The majority opinion said:

> *[C]onfessions remain a proper element in law enforcement. Any statement given freely and voluntarily without any compelling influences is, of course, admissible in evidence.*

The opinion indicates that what the Court fears is not that the accused might confess but that the accused might be motivated or forced to confess by the compulsion "inherent in custodial surroundings" of a police station or a government established atmosphere in which their freedom of action is curtailed.

B. UNITED STATES V. DICKERSON

In United States v. Dickerson, the Supreme Court rendered an opinion that held Miranda and cases following the decision govern the admissibility of statements during custodial interrogations. The court concluded that *Miranda* was a constitutional decision of the Court that could not be overruled in effect by an Act of Congress, 18 U.S.C. § 3501. The Court declined to overrule *Miranda* and reaffirmed the decision's core ruling.

C. WHEN THE WARNINGS ARE REQUIRED

The warning mandated by Miranda v. Arizona is meant to preserve the privilege during "incommunicado interrogation of individuals in a police dominated atmosphere" said to generate "inherently compelling pressures which work to undermine the individual's will to resist.... Fidelity to the doctrine requires that it be enforced strictly but only in those types of situations in which the concerns that empowered the decision are implicated." Illinois v. Perkins. Simply stated, Miranda applies to situations involving incommunicado interrogation during police custody.

Miranda warnings are required only when there is police interrogation of a person who is in custody or otherwise deprived of their freedom of action in a significant way. Several Supreme Court cases clarify that an officer's unarticulated plan to arrest does not trigger the requirement of Miranda warnings. Stansbury v. California, Beckwith v. United States, Berkemer v. McCarty. It should be noted that military personnel interviewing another military person who is a suspect must advise that person of certain warnings under Article 31, UCMJ.

1. Police

The Supreme Court designed the Miranda warnings to protect persons when being questioned in a police-dominated coercive atmosphere. There can be no violation of the Miranda requirement if the suspect is not aware that someone other than a government agent is presenting the questioning. For example, an undercover officer posing as an arrested burglar locked up in the county jail could question the suspect about the case against him without having to present the suspect with his Miranda warnings.

Statements given to undercover officers or informants do not require the Miranda warnings because the person being questioned is not

confronted with known governmental authority. This is true even when the person being questioned is in custody (unless the person's Sixth Amendment right to counsel has attached, as discussed later in this chapter).

Miranda warnings are designed to protect a person's Fifth Amendment interest when being questioned in a compulsive police environment. When a person talks to an undercover officer, informant, or a private citizen, they are not talking because of a compulsive police environment. Illinois v. Perkins.

2. Interrogation

There is no interrogation where an accused volunteers a statement. For example, a suspect that enters a police station lobby of his own free will and states to the sergeant "I am the guy who killed that man out behind the gas works last Thursday." The Miranda warnings do not apply since there was no questioning. In Miranda, the Court held:

> *There is no requirement that police stop a person who enters a police station and states that they wish to confess to a crime, or a person who calls the police to offer a confession or any other statement they desire to make. Volunteered statements of any kind are not barred by the* Fifth Amendment*, and their admissibility is not affected by our holding today.*

The Supreme Court has held that questions pertaining to a person's identification do not require any warnings. Officers ask such questions administrative purposes to identify the subject and to complete the booking process. Answers to questions of this nature are admissible against the subject even if they would tend to incriminate them. Pennsylvania v Muniz.

3. Custody or Otherwise Deprived of Their Freedom of Action in a Significant Way

A person is in custody or otherwise deprived of their freedom of action in a significant way when a reasonable innocent person would conclude they were not free to leave. Courts determine whether a person is free to leave based on a reasonable person's perceptions at the time of the interrogation. An officer's suspicions or plan to arrest is not relevant to custody unless the officer discloses them to the suspect. If a reasonable, innocent person would not believe he or she was free to leave based on the facts before them and their rational perceptions drawn from those facts, they are in custody. Orozco v. Texas. A person is not in custody nor are they in a police-dominated coercive atmosphere simply because they are being questioned in a police station. The issue is whether a reasonable person would conclude they would be free to leave during the interview. Oregon v. Mathiason.

Courts look at several factors in determining whether one is deprived of his freedom of action in a significant way. If officers told the suspect he or she was under arrest, the officers initiated the interview, or the officers escorted the suspect throughout the interview are critical elements to determining custody. United States v. Griffin. The use of force during an investigative detention, while permissible under the Fourth Amendment, may escalate this "seizure" (government's meaningful interference with freedom of movement) into "custody" (deprived of their freedom of action in a significant way). If officers stop an individual, with weapons drawn, place him face down on the ground, and began to question him, a reasonable person would conclude they were not free to leave. United States v. Perdue.

In Berkemer v. McCarty, the Supreme Court considered whether officers must administer Miranda warnings during routine traffic encounters. The roadside questioning of McCarty was temporary, brief and in a public place (highway). This is similar to a Terry type

investigative detention and, even though the person is not free to leave in this situation, the Court held that the government has *not* deprived freedom of action in a significant way.

D. EXCEPTIONS TO MIRANDA

There are times when person in custody or deprived of their freedom of action in a significant way is questioned without Miranda warnings but the courts allow their statements to be used against them. The basis for allowing exceptions stems from the idea that the warnings mandated by the Miranda decision are not in themselves constitutional rights, but rather a set of procedural rules enunciated to protect a constitutional right.

1. Officer/Public Safety

At the moment of detention or arrest or upon entering to serve a warrant, officers' concerns are not in advising someone of their rights but in securing any weapons or persons that may be a danger to them. Courts allow the government's admission of responses to security questions against the person making the statement. This is true even when the security questions, asked for the safety of officers or the public, may fall within the area of when Miranda warnings are required. New York v. Quarles. If the questions are not related to safety issues, Miranda warnings must be given. United States v. Castellana.

2. Impeachment

The government may be able to use a defendant's voluntary statement that was otherwise inadmissible for the limited purpose of impeaching the defendant's credibility. If the defendant elects to take the witness stand at trial and provides testimony inconsistent with early statements obtained in violation of his Miranda protections, the original statement may be introduced to rebut the defendant's testimony. Harris v. N.Y.

IV. WAIVER OF MIRANDA RIGHTS

After an officer has advised a suspect of his or her Miranda rights, the officer must obtain a valid waiver of rights before asking any questions. The Supreme Court specifically stated in Miranda that "the defendant may waive…these rights provided the waiver is made voluntarily, knowingly and intelligently." The burden is on the government to prove that it obtained a waiver and that the suspect gave the waiver voluntarily, knowingly and intelligently.

The suspect may orally provide the waiver. This type of waiver is more difficult to prove and is generally done by the testimony of officers or others who were present when the oral waiver was given. If the defendant gives an oral waiver and agrees to talk, but refuses to sign a waiver statement, it is a good practice to write down their exact words or their statement regarding refusal to sign and have it witnessed by another officer. Courts do not presume that the suspect gave a valid waiver. If, after agreeing to talk, the accused decides they do not wish to continue the interview or that they wish to consult an attorney, questioning must stop immediately.

It is not necessary to repeat the warning when a person has received the Miranda warnings before questioning and police wish to question about other matters. Miranda does not require police officers to prompt a defendant to reconsider their decision to answer questions. Colorado v. Spring.

Failure to provide the Miranda warnings to a person questioned while in custody will not cause future statements to be suppressed. For instance, Elstad, was questioned while in custody and voluntarily made incriminating remarks without having received Miranda warnings. Officers later advised him of his Miranda warnings. Elstad waived his rights and made incriminating statements after officers questioned him

again. The Supreme Court upheld the confession, saying that Elstad voluntarily confessed after waiving his rights. Oregon v. Elstad.

A. VOLUNTARY

The decision to waive one's rights must be the product of one's free and deliberate choice. The Supreme Court held that coercive police activity is necessary to find that a waiver is not voluntary. Colorado v. Connelly.

B. KNOWING AND INTELLIGENT

When discussing waivers of Miranda rights, courts generally mention knowing and intelligent waivers together. No specific language or incantation is required for a knowing waiver. A person must be advised of the four warnings stated in Miranda: the right to remain silent, anything said can be used against the accused, the right to have an attorney, and the right to appointed counsel if the accused cannot afford one. A person can give a knowing waiver when they are advised of their rights in terms they can understand, thus the question: "do you understand your rights?" Duckworth v. Eagan.

The suspect need not know all of the consequences of their action to constitute a waiver. Where one is mistaken as to the use of an oral statement, (defendant said he would speak but he would not write anything down) the oral statement is still admissible. Connecticut v. Barrett.

V. INVOKING MIRANDA RIGHTS

Suspects may invoke their rights in either of two ways: the defendant states that he or she does not wish to say anything or that they wish to have an attorney to represent them. There has been no waiver if, after being advised of the Miranda warnings, the accused does not respond.

A. SILENCE

When a person indicates that they do not want to talk, they have invoked the right to remain silent. The Supreme Court said that when a person invokes the right to remain silent, questioning must cease for a reasonable period. At some point, officers may again approach to determine if the defendant is willing to answer questions. In Michigan v. Moseley, the Supreme Court approved of officers waiting approximately two hours before re-approaching the suspect to determine if he wanted to remain silent.

B. COUNSEL

While the Fifth Amendment does not mention the right to counsel, the Supreme Court in Miranda stated that the right to have counsel present during interrogation is indispensable to the protection of the privilege against self-incrimination. Law enforcement officers must understand the impact of a request for counsel and know the limitations incurred by such a request.

In Edwards v. Arizona, officers arrested the suspect and advised him of his Miranda warnings. After some discussion, the suspect said that he wanted an attorney before making any deals. The next morning, detectives went to see him. The suspect did not want to see the detectives, but was told that he had to see them. After listening to a taped statement of an accomplice, the suspect made a statement. The Supreme Court held that the government could not approach the suspect, having expressed his desire to deal with the police only through counsel, until counsel had been made available.

The requirement that counsel be made available to the accused refers to more than an opportunity to consult with an attorney. When the suspect requests counsel, questioning must cease and officials may not reinitiate questioning without counsel being present, whether or not the

accused has consulted with an attorney. Law enforcement officials must scrupulously honor a person's request for counsel. Minnick v. Mississippi.

The Court held that the request for an attorney must be clear and unambiguous. If the request for an attorney is not clearly stated, the law does not require the officer to stop questioning to clarify whether the comment is or is not a request for an attorney. While it may be good practice to clarify if a statement is or is not a request for counsel, officers are under no legal obligation to do so.

The Court quoted Edwards, where they held that the suspect must affirmatively invoke the right to counsel. The Court calls this a bright line rule that officers can apply without having to make a judgment about whether or not a person has invoked the right to counsel. Therefore, law enforcement officers, after obtaining a voluntary waiver of Miranda rights, may continue questioning until the suspect clearly requests an attorney or to remain silent. Davis v. United States.

If the accused invokes the right to counsel but later initiates the conversation, police may then question the person (after obtaining a waiver). This requires two steps to ensure the officers do not violate the suspect's rights. First, did the accused initiate the conversation? If so, then, second, did the accused, without police inducement, waive his or her right to counsel? If so, then any statement made by the accused will be admissible. Oregon v. Bradshaw.

C. THE RULE IN ARIZONA V. ROBERSON

Officers arrested Roberson at the scene of a just-completed burglary. He invoked his right to counsel. Three days later, while still in custody, another police officer questioned Roberson about an unrelated crime. This officer advised Roberson of his Miranda warnings, Roberson waived his rights, and made an incriminating statement. The second officer was unaware of Roberson's earlier invocation of the right to counsel.

The Supreme Court held that once a person has requested an attorney, all questioning must cease until an attorney is made available to the person. A request for counsel indicates that the suspect feels unable to deal with the pressures of custodial interrogation without legal assistance. This inadequacy does not disappear simply because the police have approached the suspect about a separate investigation. The government cannot demonstrate a valid waiver of the right to counsel by showing only that the accused responded to further police-initiated *custodial* interrogation even if they have been readvised of their rights. Arizona v. Roberson.

The Court found immaterial the fact that the officer conducting the second interrogation did not know that Roberson had previously requested counsel. It is also immaterial that the officer wanted to speak with Roberson about a different crime and that the officers were from two different police agencies.

Officers must know which right a person is invoking when they are advised of the Miranda warnings. The best course of action is not to advise a person of the Miranda warnings if officers are not going to question the individual. When providing the warnings, officers should first ask if the accused is willing to answer questions. A negative response will indicate they do not wish to talk, which is invoking the right to silence. Recall that officers may re-approach suspects after an appreciable time to determine if they wish to continue their silence. Officers and agents from other agencies may also approach without fear of violating the rule set out in Roberson.

VI. THE SIXTH AMENDMENT RIGHT TO COUNSEL

The Sixth Amendment provides, in part, "In all criminal prosecutions, the accused shall enjoy the right to...have the assistance of counsel for his defense." This right to counsel arises at the time the adversarial judicial process begins. After that point, the accused is

entitled to have counsel present during critical stages of the proceedings.

This right should not be confused with Miranda. The purpose of the Sixth Amendment right to be represented by counsel is to assist the accused in preparing their defense for trial. The Sixth Amendment right to counsel applies to critical stages of the proceedings, which includes government questioning. Miranda warnings require the government to advise a person of the right to counsel during questioning *only* to protect the Fifth Amendment privilege not to incriminate oneself.

The right to counsel applies whether or not the suspect is in custody. An undercover officer, a cooperating co-defendant, or informant cannot attempt to elicit incriminating statements from the subject unless the defendant has waived the right to counsel after the adversarial judicial process has begun.

A. ADVERSARIAL JUDICIAL PROCESS

The adversarial judicial process begins when the government takes steps to prosecute one for a criminal act. The government takes formal steps to initiate a criminal prosecution through an initial appearance, securing an indictment, or filing an information. Following one of these three events, the government has commenced the adversarial process and the accused has the right to have counsel present at any critical stage of the process that may have an impact on the final outcome, i.e., the trial. Powell v Alabama.

Critical stages of the proceedings include events occurring before trial and at trial that may affect the outcome at trial. The right to be represented by counsel at such proceedings is necessary to protect the person's right to the assistance of counsel for their defense. Questioning, lineups, and all court appearances, including the trial, are critical stages of the proceedings requiring advice of the right to counsel and a subsequent waiver of that right before proceeding. For example, if officers ask an indicted person to stand in a lineup, they must advise the person of the

right to have an attorney present during the lineup. There is no right to an attorney at a lineup held before the adversarial judicial process.

B. QUESTIONING

The limitations on questioning under the Sixth Amendment are different from questioning under Miranda. After the adversarial judicial process begins, questioning violates the defendant's right to the assistance of counsel for trial preparation whether or not the questioner is known to be a government officer. While Miranda protects against the compulsive aspects of in-custody interrogation by a known police authority, the Sixth Amendment protects against *any* questioning without the presence of counsel.

In Massiah v. United States the government used statements at trial purposely elicited from the defendant following the initiation of the adversarial judicial process. His counsel was not present and he had not waived his right to counsel. Since questioning is a critical stage of the proceeding, the statements were held to be inadmissible.

On the other hand, officers instructed an informant to refrain from asking the suspect any questions, but to "keep his ears open." The defendant later made incriminating statements to the informant. The Supreme Court held that the statements were admissible since there was no questioning, just passive listening. Kuhlman v. Wilson. Had the informant engaged the defendant in conversation for obtaining admissions, this would constitute questioning in violation of the Sixth Amendment right to counsel. United States v. Henry.

C. STATEMENTS ON UNCHARGED MATTERS

Officers can ask persons about crimes for which they have not been arrested or charged. The Sixth Amendment right to counsel only affords protection in the adversarial process for which the defendant is presently

engaged. This is because there has been no formal proceeding at which the government has taken steps to prosecute. Questioning on these matters cannot lead into an area covered under the Sixth Amendment. Maine v. Moulton.

The purpose of the Sixth Amendment right to counsel is to protect the accused at critical confrontations. The Court held that the invocation of the Sixth Amendment right to counsel is offense specific and cannot be invoked regarding crimes unrelated to those for which the accused has been charged. One might be willing to speak to police on unrelated matters without counsel present, and the courts will allow such interrogations without the presence of counsel. If the suspect is not in custody, Miranda warnings are not required.

D. WAIVER OF THE SIXTH AMENDMENT RIGHT TO COUNSEL

Once the Sixth Amendment right to counsel has attached, the accused may waive the right to counsel. Officers may not question the accused without a valid waiver. The Sixth Amendment right to counsel exists whether or not the person is in custody and whether or not they know the true status of the person conducting the questioning. A valid warning and waiver of Miranda warnings is sufficient to waive the Sixth Amendment right to counsel. Michigan v. Jackson. Patterson v. Illinois.

LEGAL RESOURCE WEB SITES

This list of web sites and descriptions was compiled by
Senior Instructor Holly Coffey.

http://www.ojp.usdoj.gov/nij/international/welcome.html
The National Institute of Justice International Center collects and disseminates information on local, national, and transnational crime, and on best practices for crime control.

http://www.ojp.usdoj.gov/nij/
The National Institute of Justice is the research and development agency of the U.S. Department of Justice and is the only Federal agency solely dedicated to researching crime control and justice issues. NIJ provides objective, independent, and non-partisan, evidence-based knowledge and tools to meet the challenges of crime and justice, particularly at the State and local levels.

http://www.law.cornell.edu/federal/
Valuable search web site that accesses U.S. Federal legal materials to include the U.S. Code, Supreme Court decisions, a searchable index of U.S. Court of Appeals decisions, the Code of Federal Regulations, state law by topic and material available from other Internet-accessible sites.

http://www.usdoj.gov/
Department of Justice homepage that accesses antitrust, civil, civil rights, criminal, environmental, immigration and other appellate briefs, case filings, DOJ publications and the U.S. Attorneys Manual.

http://www.usdoj.gov/immigrationinfo.htm
Both the Immigration and Naturalization Service and the Executive Office for Immigration Review have Web sites that provide extensive immigration information. Among the many items to be found are residency issues, INS forms, citizenship, asylum, lawful permanent

residency, employment authorization, refugee status, inter-country adoptions, family and employment related immigration, and foreign student authorization.

http://www.usdoj.gov/prisoninfo.htm
Prison and parole information including federal prison facilities, federal inmate information, state prison inmate locator, prisoner transportation and transfer.

http://www.corrections.com/links/facilities.html
The Corrections Connection is an open forum where practitioners can exchange ideas and utilize best corrections practices, resources, case studies and new technologies. A good resource for Corrections Professionals.

http://www.corrections.com/links/cjschools.html
By state listing of undergraduate and graduate Criminal Justice schools.

http://www.atf.treas.gov/index.htm
Home page for the Bureau of Alcohol, Tobacco and Firearms that has a daily update of law enforcement news, job listings, Federal explosives law and regulations, state laws and published ordinances, explosives and bomb detection resources, and threat assessment guides.

http://oig.state.gov/operations.html
The Office of Inspector General (OIG) is dedicated to improving operations; promoting positive change; and detecting and preventing waste, fraud, abuse, and mismanagement. This web site provides access to the Freedom of Information Electronic Reading Room.

http://www.firstgov.gov/
Good general federal government information site, including how to contact the government, federal laws and regulations, federal forms, statistics and news.

http://www.whitehouse.gov/
White House home page containing Presidential speeches, Executive Orders, current news and pending legislation.

http://www.bxa.doc.gov/factsheets/ExporterAssistance.html
Home page for the Bureau of Export Administration, U.S. Department of Commerce. Contains help for exporters, export regulations, treasury regulations, trade sanctions and related sites.

http://www.defenselink.mil/pubs/
Official Department of Defense home page for DOD news, releases, publications reports forms and personnel locator.

http://www.fletc.gov/
Federal Law Enforcement Training Center homepage provides training overviews, lists facilities, lists staff and support, contains the legal division quarterly review (Supreme Court reviews, interesting developments in the law and legal articles that clarify various legal issues.)

http://www.findlaw.com/
Outstanding legal search site for all legal topics and subject, case law and codes, U.S. Federal resources and legal careers.

www.eeoc.gov
Site containing access to federal laws prohibiting job discrimination, how to file a discrimination charge, mediation procedures and Freedom of Information Act sites.

http://www.medill.northwestern.edu/docket/
Useful site reviewing all cases pending before the United States Supreme Court, from the day the Court accepts review of the case through issuance of opinions.

http://www.access.gpo.gov/nara/cfr/cfr-table-search.html#page1
Government Printing Office web site providing access to government information products for the legislative, executive, and judicial branches as well as access to other federal data bases.

www.cybercrime.gov/searchmanual.htm
Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division web site where the latest version of ***Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*** can be downloaded.

www.cybercrime.gov/searchupdate.html
Regular updates for ***Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.***