CONCLUSION

To face the challenges of the future, law enforcement agencies must cooperate and pool their resources. The Financial Crimes Task Force of Southwestern Pennsylvania consistently demonstrates the effective use of time, money, material, and human resources in a combined effort to attack the growing problem of financial crime. Intelligence from various law enforcement agencies and private financial institutions has streamlined the investigative process. The combined investigative skills of the task force members have yielded a number of creative approaches to the investigation of major conspiracies that impact large numbers of individuals and corporations, not only in southwestern Pennsylvania but also throughout the country.

While no single law enforcement agency has the resources or expertise to address the myriad financial crimes that occur every day in a large city, the collaborative effort that a task force provides can. The Financial Crimes Task Force of Southwestern Pennsylvania can serve as a model for other metropolitan areas as they strive to combat white-collar crime.✦

Endnotes

[1] Originally dubbed the Pittsburgh Credit Card Fraud Task Force and later the Pittsburgh Financial Crimes Task Force, the task force's new name reflects the growth of financial crime in the southwestern Pennsylvania area.

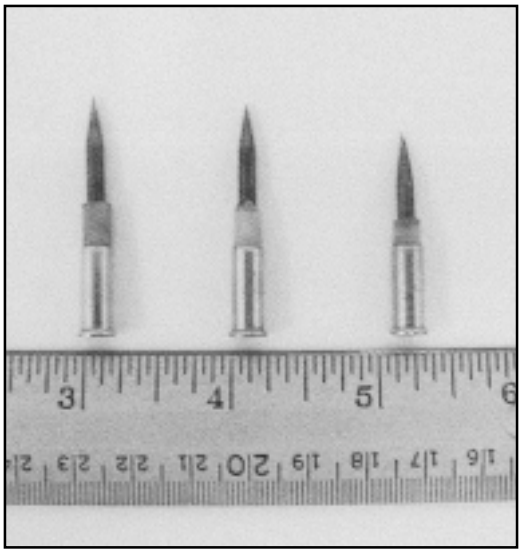
[2] The following agencies participate in the task force: the FBI, the U.S. Secret Service, the U.S. Postal Inspection Service, the U.S. Attorney's Office for the Western District of Pennsylvania, the Pennsylvania State Police, the Westmoreland County District Attorney's Office and its Detective Unit, the Allegheny County District Attorney's Office and its White-collar Crimes Unit, the Allegheny County Police, the City of Pittsburgh Police, and the City of Greensburg Police Department. All local, county, and state officers have been deputized as special deputy U.S. marshals.

Bulletin Alert

Steel Dart Ammunition Cartridges

The Ottawa, Kansas, Police Department seized several modified 22LR ammunition cartridges that did not have the lead projectile in place. A steel dart inside a plastic sleeve was inserted instead. All normal powder from the 22 round and primer were still intact. These darts easily penetrated a standard level II bullet-resistant vest. The pointed steel dart went through the vest and approximately 1 inch further into a 2- by 4-inch wooden board behind the vest. The accuracy between rounds varied greatly. Although these rounds do not function in all firearms because of the length of the overall modified shell, they still pose a serious threat to law enforcement officers.

Submitted by the Ottawa, Kansas, Police Department.



Electronic Surveillance

A Matter of Necessity

By THOMAS D. COLBRIDGE, J.D.

Criminal investigations are becoming increasingly more difficult as criminal targets become even more sophisticated. The challenge for criminal investigators is to keep pace by using increasingly sophisticated investigative techniques. One extremely successful technique has been electronic surveillance, both silent video surveillance and interception of wire, oral, or electronic communications. No jury can ignore watching defendants commit crimes before their very eyes or hearing the defendants talk about their crimes in their own voices. This article focuses on investigators' obligation to demonstrate the necessity for electronic surveillance before the court will authorize its use.

HISTORY

Electronic surveillance is not a new technique. As long ago as 1928, the U.S. Supreme Court wrestled with the constitutional implications of governmental recording of telephone calls. The Court decided in the case of *Olmstead v. United States* [1] that tapping a telephone line from outside a residence was not a search under the Fourth Amendment.[2] The Court reasoned that the government, by tapping the telephone line outside the residence, had not invaded any constitutionally protected area ("persons, houses, papers, and effects..."). In addition, the government had seized mere telephone conversations, instead of tangible objects ("the persons or things to be seized") described in the Fourth Amendment.[3]

In 1934, perhaps partially in response to the *Olmstead* case, Congress passed the Communications Act of 1934.[4] That Act prohibited the unauthorized recording of telephone calls but only if the contents of the recording were disseminated. Consequently, the government could tap telephones as long as it did not reveal the content of the recorded conversations without authorization.

The U.S. Supreme Court completely altered the legal landscape surrounding electronic surveillance with two decisions in 1967. In *Katz v. United States,*[5] the Court redefined a search under the Fourth Amendment. The Court decided that a Fourth Amendment search occurs anytime the government infringes a person's reasonable

Special Agent Colbridge is a legal instructor at the FBI Academy.

> ***"...a Fourth Amendment search occurs anytime the government infinges a person's reasonable expectation of privacy."***

expectation of privacy. Under this new definition, the government does not have to invade a constitutionally protected area for a search to occur. The Fourth Amendment now protects people, not places—the government may not unreasonably invade a person's privacy anywhere, in public or private, as long as the person's expectation of privacy in that activity or place is objectively reasonable.[6] In *Berger v. New York,*[7] the Supreme Court, while reviewing the New York state wiretapping law, clearly held that any form of electronic surveillance that infringes this reasonable expectation of privacy is a Fourth Amendment search. The Court also established the constitutional standards for obtaining authority to wiretap.

In 1968, Congress codified the requirements for obtaining court authority to intercept oral and wire communications in Title III of the Omnibus Crime Control and Safe Streets Act (Title III).[8] This Act subsequently was amended in 1986 to include the interception of electronic communications among its prohibitions[9] and, in 1994, by the Communications Assistance for Law Enforcement Act (CALEA).[10] Most states have enacted electronic surveillance statutes patterned after the federal model.[11]

There is no federal legislation concerning judicial authorization of silent video surveillance.[12] The federal courts have decided that Title III—governing the interception of oral, wire, and electronic communications—neither prohibits nor authorizes the practice.[13] Instead, federal courts have the authority to issue silent video surveillance warrants under Rule 41 of the Federal Rules of Criminal Procedure.[14]

IS A WARRANT NECESSARY?

If a government action in no way infringes upon a reasonable expectation of privacy, it is not a search under the Fourth Amendment.[15] In that case, officers are not governed by the Constitution's warrant requirement. Consequently, court authority for electronic surveillance is not required by the Fourth Amendment where there is no reasonable expectation of privacy.

For example, no warrant is required on the federal level to videotape activity in an open field,[16] or other public places.[17] It also is not a violation of either Title III or the Fourth Amendment to tape record a defendant's prearrest conversation in the backseat of a police car,[18] or outgoing telephone calls from a prison that already are routinely recorded.[19]

Similarly, the federal courts have ruled that there is no expectation of privacy in a conversation or activity when one party to the conversation or activity consents to government monitoring.[20] Such conversations have been specifically exempted from Title III coverage[21] and from the Fourth Amendment's warrant requirement for silent videotaping.[22]

THE WARRANT REQUIREMENT

The courts and Congress have long considered any form of electronic surveillance extremely invasive. As the Supreme Court noted in the *Berger* case: "[I]t is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded. Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."[23] Because of this view, the prerequisites for obtaining a warrant authorizing electronic surveillance of oral, wire, and

electronic communications, as well as silent video, are quite strict.[24] Officers must comply with the Fourth Amendment requirements of probable cause[25] and particularity.[26] In addition, Title III requires that officers seek prior authorization from a particular government official;[27] identify previous electronic surveillance applications regarding the same people, facilities, or places;[28] confine their surveillance to only relevant conversations or activities (the "minimization requirement");[29] specify the length of time the technique will be used;[30] and certify that normal investigative techniques have been tried and failed, are reasonably unlikely to succeed, or too dangerous to attempt.[31] It is this last requirement, the exhaustion of normal investigative techniques, that is the focus of the remainder of this article.

A Matter of Necessity

The courts and Congress view electronic surveillance as extremely invasive. With more traditional investigative techniques, the person targeted knows what the police are doing. Individuals interviewed about criminal activity clearly know they are suspected. If the police search a person's home under the authority of a search warrant, the homeowner is present at the time of the search or learns of the search soon after when a copy of the warrant is found on the premises. Even if the police use an informant or undercover officer to speak to the subject about criminal activity, the subject makes a choice to divulge information and assumes the risk that the information will be given to the police.

The same is not true with electronic surveillance. The subjects are unaware that their words or actions are being recorded by the government until much later. And in some cases, the words and actions recorded were never even exposed to another, so the subject cannot be said to have accepted any risk. Because of this extraordinary invasiveness, electronic surveillance should be authorized only when necessary.[32] In the words of the Supreme Court, electronic surveillance should not be "resorted to in situations where traditional investigative procedures would suffice to expose the crime."[33]

> ***"...court authority for electronic surveillance is not required by the Fouth Amendment where there is no reasonable expectation of privacy."***

The "Exhaustion" Statement

Title III requires that the application for an electronic surveillance order include "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous...."[34] In addition, the surveillance order may be issued only if the reviewing judge makes a specific finding to that effect.[35] While there is no corresponding statutory obligation on the federal level, federal courts have imposed the same requirement on officers seeking authority to surveil an area by means of silent video.[36]

This requirement is commonly known as the "exhaustion" statement. It is an unfortunate description because it implies that law enforcement must exhaust all other standard investigative techniques before resorting to electronic surveillance. Nothing could be farther from the truth. The statutory language of this necessity requirement is disjunctive and actually permits the government to establish the necessity for the electronic surveillance in three different ways. Necessity can be shown by demonstrating that:

1) standard techniques have been tried and failed;

2) standard investigative techniques are reasonably likely to fail; or

3) standard investigative techniques are too dangerous to try.[37]

Necessity Requirement Defined

The courts have recognized that the necessity requirement must be evaluated in a "practical and commonsense" way.[38] This approach requires that the reviewing judge consider all of the unique facts and circumstances of each case when deciding if electronic surveillance is necessary. Consequently, even if the government's application is inartfully drawn, the government still may argue that the facts presented in the

application are sufficient for the reviewing judge to conclude from commonsense that electronic surveillance is necessary. As the U.S. Court of Appeals for the Tenth Circuit has noted: "[T]he government's failure to explain its failure to utilize one or more specified categories of normal investigative techniques will not be fatal to its wiretap application if it is clear, under the government's recitation of the facts of the case, that requiring the government to attempt the unexhausted and unexplained normal investigative techniques would be unreasonable."[39]

Mere conclusions, allegations, and boiler-plate language will not satisfy the necessity requirement. The application for the electronic surveillance order specifically must explain why, in the particular case at hand, ordinary investigative techniques have not worked or would fail or be too dangerous.[40]

For example, the following statement was found to be conclusory: "Search warrants would not produce the full scope of the scheme or the identity of his many associates."[41] That statement, standing alone, offers the reviewing judge no explanation of why search warrants would be futile in this particular case. The officer making that statement might have had years of investigative experience that led him to that conclusion. The court may certainly consider that experience in making its evaluation of necessity. However, because there was no attempt to demonstrate why that conclusion was relevant in this particular case, the court was unpersuaded.

GENERAL INVESTIGATIVE TECHNIQUES

Title III requires that applicants for an order authorizing surveillance of oral, wire, or electronic communications explain in their applications what other investigative techniques have been tried and failed. If these techniques have not been tried, applicants must show why it would be futile or too dangerous to do so.[42] A similar requirement has been attached to applications for authority to use silent video surveillance.[43] What standard investigative techniques must officers consider? What circumstances will make these techniques futile or too dangerous?

> ***"...the electronic surveillance order specifically must explain why... ordinary investigative techniques have not worked, or would fail or be too dangerous."***

A court's view of what techniques are reasonable or futile or too dangerous will be colored by the investigator's explanation of the goals of the investigation. For example, the use of undercover officers may be sufficient and reasonable to reveal the activities of a street-level narcotics dealer. However, if the goal of the investigation is to identify the dealer's associates and suppliers, undercover officers alone may not be sufficient. The broader the goals of the investigation, the greater the need for sophisticated investigative techniques. Investigators should ensure that the court knows what those goals are.

There may be circumstances in which officers need not consider any other techniques at all. If investigators can explain why other standard investigative techniques are either reasonably likely to fail or too dangerous, they have met their burden.[44] Consider the one-person counterfeiting operation. A single individual with no criminal history manufactures counterfeit bills in a small room. The subject then personally takes the bills and deposits them in unsophisticated off-shore banks where the bills are not inspected closely. In such a situation, standard techniques are likely to fail. Perhaps the only successful technique would be the installation of video cameras in the subject's workshop.

What if investigators have tried standard investigative techniques and gotten some favorable results? That does not preclude the possibility of court-authorized electronic surveillance. For example, in *United States v. Maxwell,*[45] officers received useful information from a cooperating defendant, surveillance of individuals identified by the cooperating defendant, and pen registers. The court still found that electronic surveillance was necessary because the officers had not been able to determine the full scope of the suspected conspiracy or develop

enough evidence for a successful prosecution.

It is clear that the government need not exhaust, consider, or explain away all other conceivable investigative techniques before resorting to electronic surveillance. The requirement is designed to ensure that electronic surveillance is not used as a first resort when other standard, less intrusive investigative techniques would expose the crime.[46]

It may be harder for the government to show the necessity for electronic surveillance in areas such as the home where people have a higher expectation of privacy. For example, the U.S. Court of Appeals for the Tenth Circuit has said: "Our holding is narrowly limited to business premises. We leave for another day the details of the higher showing [of necessity] that would *a fortiori* be required to justify video surveillance of the central bastion of privacy—the home."[47]

SPECIFIC INVESTIGATIVE TECHNIQUES

What other standard investigative techniques should investigators consider? The answer, of course, depends upon the unique circumstances of each investigation. Reasonable techniques in one investigation may not be reasonable in another.

However, the legislative history of Title III and the federal case law provide clear guidance regarding what Congress and the courts consider reasonable techniques. In the legislative history of Title III, Congress identified four techniques that investigators should consider:

1) standard visual and aural surveillance;

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

3) the use of search warrants; and

4) the infiltration of criminal groups by undercover agents or informants.[48]

Some courts have added two other techniques, the pen register and the trap and trace.[49]

Because Congress considered these techniques standard and reasonable, investigators seeking court authorization for electronic surveillance should discuss their failure, futility, or danger when applying for that authorization. That discussion must be in terms of the investigation at hand, not in terms of investigations in general. Courts have recognized many circumstances in which these standard techniques would be futile or too dangerous. A discussion of some of these circumstances demonstrates the commonsense approach taken by courts in judging the necessity requirement.

Interrogation

The technique of using standard interviews has obvious drawbacks. Such overt investigation would alert the targets to the investigation.[50] Interviewees would likely fear reprisals if it became known they had talked to law enforcement.[51] No one person is likely to know the full extent of the criminal enterprise.[52]

All of the same drawbacks apply to using the grand jury. In addition, because a grand jury witness may be granted immunity to testify early in the investigation, top-echelon leaders could get immunity before the full extent of the enterprise and its leadership is known.[53]

Search Warrants

The problems of executing search warrants during an investigation also are obvious. Targets are alerted so they can take defensive measures or flee.[54] Records located in one location are unlikely to give investigators a true picture of the entire scope of the criminal enterprise.[55] A search could be futile where the criminal business is done on the telephone[56] or any records discovered are in a code unknown to investigators.[57]

Standard Physical Surveillance

Obviously, the physical location and design of the area to be surveilled are factors the courts must consider. A home in a quiet residential[58] or rural[59] setting would pose

problems for surveillance teams. A home surrounded by high walls may be impossible to watch.[60] The target may have detected surveillance in the past[61] or be known to practice countersurveillance measures.[62] The number of vehicles available to the surveillance target is also a consideration.[63] It also could be impractical and futile to attempt surveillance because the targets are active 24 hours a day.[64] Finally, even if the target successfully is followed, it does not give investigators any information regarding meetings to which the target may have traveled.[65]

Informants and Undercover Officers

Investigators also should consider these techniques prior to applying for court authorized electronic surveillance. Courts have recognized, however, that these techniques at times may be futile or too dangerous.

Informants themselves may pose problems. They may refuse to testify against the defendant.[66] They may have extensive criminal histories making them subject to impeachment.[67] Informants may not have access to crucial meetings where criminality is discussed[68] or may not be able to know the entire scope of the criminal enterprise.[69]

The unique facts of the case may make the use of informants impractical. For example, in *United States v. Oriakhi,*[70] the target was a new immigrant to the United States who knew very few people in the area and spoke a foreign language. Using informants or undercover operatives in this situation would have been problematic at best.

It simply may be too dangerous to insert an informant or undercover officer. The members of the criminal enterprise may have an extremely close relationship in a very closed community. A stranger certainly would arouse suspicions.[71] The target's previous violent response to attempts at infiltration may preclude the possibility of using informants or undercover officers.[72] The target may be too crafty or wary to make attempts to infiltrate the organization safe.[73]

> ***"Reasonable techniques in one investigation may not be reasonable in another."***

Pen Register and Trap and Trace

Some courts have added the pen register and the trap and trace to the list of standard investigative techniques. The pen register is a device that records numbers dialed *from* a telephone. The trap and trace is a device that records numbers dialed *to* a telephone and provides the name of the subscriber to the instrument making the call. They are usually used in tandem. A simplified court order is required to install the devices.[74]

While the devices provide excellent information on possible associates of the owner of the telephone they monitor, courts have recognized their limitations. The devices cannot specifically identify the caller, only the instruments from which the call is made.[75] The devices also cannot reveal the nature of the conversation.[76] Consequently, even if extensive associational information is developed through the use of the devices, more specific proof of criminal activity will be needed to successfully prosecute a criminal case.

Of course, this discussion does not encompass the whole spectrum of investigative techniques available to the criminal investigator, merely those typically identified in the case law as being standard, reasonable techniques. The applicant for the electronic surveillance order should discuss any and all other techniques used and explain their failure to produce a prosecutable case.

CONCLUSION

One of the most powerful investigative tools available to law enforcement is electronic surveillance of wire, oral, and electronic communications, as well as silent video surveillance of areas. While powerful, these techniques are also extremely invasive. Consequently, the federal Congress and courts, and state legislatures and courts, have sought to limit the use of electronic surveillance to only those times when its use is necessary.

The necessity requirement may be satisfied if the standard techniques have been tried and failed or if investigators can explain why each technique would be futile in their particular investigations, why the technique is simply too dangerous to undertake in a particular circumstance.

Electronic surveillance is a Fourth Amendment search when it is used by the government in a manner that infringes a reasonable expectation of privacy. Reasonableness is the standard that should motivate both the investigator and the court. If investigators can reasonably explain the necessity for electronic surveillance, the court will use its reason and commonsense to evaluate their judgment.✦

Endnotes

[1] 277 U.S. 438 (1928).

[2] U.S. Constitution Amendment IV reads: "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 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."

[3] *Supra* note 1 at 464.

[4] 47 U.S.C. § 151, *et.sec.,* June 19, 1934, c. 652, 48 Stat. 1105.

[5] 389 U.S. 347 (1967).

[6] *Id.* at 361 (Harlan, J. concurring).

[7] 388 U.S. 41 (1967).

[8] S. Rep No. 1097, 90th Cong., 2d Session; Title 18 U.S.C. § 2510-2520.

[9] Electronic Communications Privacy Act of 1986 (ECPA), S. Rep. No. 541, 99th Cong., 2nd Session.

[10] S. Rep. No. 402, 103rd Cong., 2d Session.

[11] The Federal legislation regarding electronic surveillance has preempted state legislation on the subject: *see, e.g., United States v. Feiste*, 792 F.Supp. 1153, *aff'd* 961 F.2d 1349 (1991). Consequently, state laws governing electronic surveillance must meet at least the minimum requirements for authorization in the federal statute. However, local officers should consult with their legal advisors to determine if state requirements are stricter than federal standards.

[12] Local officers should consult their legal advisors to determine if their local jurisdictions have adopted legislation regarding video surveillance.

[13] *United States v. Williams*, 124 F.3d 411 (3rd Cir. 1997).

[14] *United States v. New York Telephone*, 434 U.S. 159 (1977); *United States v. Mesa-Rincon*, 911 F.2d 1433 (10th Cir. 1990); *United States v. Falls*, 34 F.3d 6741 (8th Cir. 1994).

[15] *Katz v. United States*, *supra* note 5.

[16] *Oliver v. United States*, 466 U.S. 170 (1984); *United States v. Harvey*, 117 F.3d 1044 (7th Cir. 1997) (silent videotaping of activity in a marijuana plot in a national forest permissible).

[17] *United States v. Taketa*, 923 F.2d 665 (9th Cir. 1991). Officers should be alert, however, to the possible need to secure a warrant to install the monitoring equipment, if the installation is to be made in a area where there is an expectation of privacy.

[18] *United States v. McKinnon*, 985 F.2d 525 (11th Cir. 1993) *cert. denied,* 114 S. Ct. 130.

[19] *United States v. Van Poyck*, 77 F.3d 285 (9th Cir. 1996), *cert. denied,* 117 S. Ct. 276.

[20] *Manetta v. Macomb County Enforcement Team*, 141 F.3d 270 (6th Cir. 1998); *United States v. Gibson*, 170 F.3d 673 (7th Cir. 1999).

[21] Title 18 U.S.C. § 2511 (2)(c). Local officers should consult their legal advisors regarding consent exemptions under their state laws.

[22] *United States v. Tangeman*, 30 F.3d 950 (8th Cir. 1994), *cert. denied,* 115 S. Ct. 532; *United States v. McKneely*, 69 F.3d 1067 (10th Cir. 1995); *United States v. Gibson*, 170 F.3d 673 (7th Cir. 1999).

[23] *Supra* note 7 at 64.

[24] Federal courts have held the prerequisites for obtaining a warrant for silent video surveillance are the same as those established in Title III for a warrant authorizing the interception of wire or electronic communications: see *e.g. United States v. Koyomejian*, 970 F.2d 536, (9th Cir. 1992) opinion corrected, *cert. denied,* 113 S. Ct. 617. Local officers are again urged to consult with their legal advisors to determine if their state standards are more strict.

[25] Title 18 U.S.C. § 2518 1(b) and 3(a) and (b). Generally, courts have required that the government establish probable cause to believe a crime has been, is being, or is about to be committed; that the target of the investigation will use the instrument monitored or the area surveilled in furtherance of the crime; and that communications or activities regarding the crime will be captured. *United States v. Meling*, 47 F.3d 1546 (9th Cir. 1995), *cert. denied,* 116 S. Ct. 130.

[26] Title 18 U.S.C. § 2518 (1)(b)(i-iv). The officer is required to particularly describe the offense being investigated; the nature and location of the instrument to be tapped or the place to be surveilled; the types of communications or activities sought to be intercepted or recorded; and the people, if known, whose communications or activities will be intercepted or surveilled. These requirements form the basis for what is typically known as "minimization," the procedure whereby the government seeks to limit its monitoring or recording only to relevant communications or activities.

[27] Title 18 U.S.C. § 2516.

[28] Title 18 U.S.C. § 2518 (1)(e).

[29] Title 18 U.S.C. § 2518 (5).

[30] Title 18 U.S.C. § 2518 (1)(d), (4)(e), and (5). Generally, authorization may be given only for the length of time necessary to accomplish the objective of the request but in no event longer than 30 days.

[31] Title 18 U.S.C. § 2518 (1)(c) and (3)(c).

[32] Title 18 U.S.C. § 2518 (1)(c) and (3)(c); *United States v. Castillo-Garcia*, 117 F.3d 1179 (10th Cir. 1997), *cert. denied, United States v. Armendariz-Amaya*, 118 S. Ct. 395.

[33] *United States v. Kahn*, 415 U.S. 143, 153 n.12 (1974).

[34] Title 18 U.S.C. § 2518 (1)(c).

[35] Title 18 U.S.C. § 2518 (3)(c).

[36] *United States v. Falls*, 34 F.3d 674 (8th Cir. 1994); *United States v. Mesa-Rincon*, *supra* note 14.

[37] *United States v. Smith*, 31 F.3d 1294 (4th Cir. 1994), *cert. denied* 115 S. Ct. 1170.

[38] *United States v. McGlory*, 968 F.2d 309 (3rd Cir. 1992), *cert. denied, Cotton v. United States*, 113 S. Ct. 415; *United States v. Castillo-Garcia*, *supra* note 32.

[39] *United States v. Castillo-Garcia*, *supra* note 32 at 1188; *United States v. Mesa-Rincon, supra* note 14.

[40] *United States v. Commito*, 918 F.2d 95 (9th Cir. 1990).