# FINANCIAL FRAUD LAW REPORT

VOLUME 2 NUMBER 9 OCTOBER 2010

The FINANCIAL FRAUD LAW REPORT is published 10 times per year by A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207, 
POSTMASTER: Send address changes to the Financial Fraud Law Report, A.S. Pratt & Sons, 805 Fifteenth Street, NW., Third Floor, Washington, DC 20005-2207. *ISSN 1936-5586*

# Wiretaps and Undercover Sting Operations: Are White Collar Defendants Ready?

MARK B. SHEPPARD AND RYAN ANDERSON

*"Out are the days of resting easy in the belief that only self-reporting or tipsters will bring criminality to light. In are the days of proactive and innovative white collar enforcement."*

– Lanny Breur, February 25, 2010, at the 24th annual National Institute on White Collar Crime.

The U.S. Department of Justice has aggressively used proactive enforcement techniques such as undercover sting operations and enhanced use of electronic surveillance in white collar cases. The recent Foreign Corrupt Practices Act ("FCPA") arrests at a Las Vegas gun show following a two-year long sting investigation and the *Galleon* case in New York are but two of the more prominent examples. These techniques, once reserved for drug and organized crime conspiracies are now becoming part of garden variety health care and financial fraud investigations. As a result, white collar practitioners can no longer afford to be in the dark regarding these techniques and the law that surrounds them.

---

Mark B. Sheppard is a partner in the Litigation Department at Montgomery, McCracken, Walker & Rhoads, LLP. His practice focuses on white collar criminal defense, SEC Enforcement, complex commercial litigation. Ryan Anderson is an associate in the firm's Litigation Department. The authors can be reached at msheppard@mmwr.com and randerson@mmwr.com, respectively.



Published in the October 2010 issue of *The Financial Fraud Law Report*.

Consider, that, in a recent FCPA sting case, there were 22 defendants, 16 unsealed indictments that "represent the largest single investigation and prosecution against individuals in the history of DOJ's enforcement of the FCPA," according to a DOJ release. The indictments, following over two and a half years of sting operations, allege that the 22 defendants allegedly agreed to pay a 20 percent bribe to sales agents supposedly representing the foreign defense minister in return for a $15 million contract. In reality, the sales agent was an undercover FBI agent.

And consider this, in the *Galleon* case: There were over 18,000 intercepted recordings through use of informant wearing a wire — thousands of wiretaps were made in the criminal investigation between 2003 and 2009. David Slaine, a former hedge fund manager was identified as a government "mole" in an undercover sting operation targeting the fallen Galleon Group. Slaine agreed to secretly record conversations used against Galleon after federal authorities caught him trading on inside tips supplied by UBS in a separate case. On March 10, 2010, it was reported that federal prosecutors wired several cooperating witnesses in the Galleon Group insider trading case in order to obtain information on other targets of the investigation.

The wiretapping law jurisprudence that developed in the 1970s has been well settled for decades and practitioners in drug and gang cases are very familiar with this area of the law. White collar practitioners are now confronted with these old tactics in a new forum. White collar defendants are being caught on tape and their attorneys must be prepared to defend against the tapes. The applicability of the wiretapping laws to white collar cases is new, relatively uncharted and as such, presents both concern and opportunity.[1]

## DEFENDING AGAINST TITLE III EVIDENCE — FEDERAL WIRETAP LAW

Congress enacted the Federal Wiretap Act as part of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III") in an effort to balance the privacy rights of individuals and the legitimate needs of law enforcement.[2] The Act seeks to safeguard privacy in oral and wire communications while simultaneously articulating when law enforcement officials may intercept

such communications.[3] Title III prohibits the intentional interception of wire, oral or electronic communications, unless specifically provided for in the statute.[4]

The strict procedural and evidentiary requirements of the Act, provide plenty of room for creative lawyering. Although courts have been less and less likely to enforce the strict requirements of sealing or having the proper official sign the application, rather than just authorize the wiretap, there is still plenty to fight when confronted with wiretap evidence.

## Challenges to a Title III Electronic Interception

### *Challenge Each Wiretap Application, Supporting Affidavit and Order Independently, On Its Face*

A defendant should analyze and challenge each separate application.[5] In addition, when defending the wiretap applications and orders, the government is limited to the information contained only within the application and affidavits as presented to the authorizing court.[6] Note that the government can use testimony or affidavits incorporated by reference in the application (as long as these documents are also presented to the authorizing court).

### *DOJ Official Authorization*

Title III requires that the Attorney General of the Department of Justice or a subordinate designated by the Attorney General authorize an AUSA's wiretap application. The DOJ official authorizing the wiretap application must be specifically identified.[7] The wiretap order must also identify the DOJ official who authorized the application.[8]

The Title III provisions concerning official authorization are as follow:

- Section 2518(10)(a)(iii): Gives authority to challenge wiretap orders;
- Section 2518(4)(d): Requires orders to reflect the identity of the authorizing official;
- Section 2516(1): Provides which DOJ officials are empowered to authorize an application.

There are many cases where the government fails in this step and the result is mixed between suppression of the wiretap and upholding the wiretap.[9]

### *Sealing*

Sealing is another procedural requirement that can be challenged, although the results are again, mixed. Title III states that "[i]mmediately upon the expiration of the period of the order [authorizing wiretapping], or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions."[10] "The government must follow these procedures or it cannot use the intercepted communications against the surveilled individual in a criminal trial. To use wiretap evidence, the government must (1) seal the tapes immediately or (2) provide a 'satisfactory explanation' for the delay in obtaining a seal."[11]

Therefore, at the beginning of any wiretap litigation it is essential to visit the facility housing the original tapes or data, and examine the sealing orders and logs for the data.

### *Minimization Challenges*

Title III demands minimization of the eavesdropping on calls:

> .... Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception.[12]

The Third Circuit has advised that "[o]ur inquiry is on the 'reasonableness' of minimization efforts, under the totality of the circumstances."[13]

In *Scott*, the court found that such circumstances included "the purpose of the wiretap and the information available to the agents at the time of interception."[14] Thus, minimization requirements are less stringent where, because of coded language and one-time only calls, "agents can hardly be expected to know that calls are not pertinent prior to their termination."[15]

The Third Circuit further instructs that "[t]he mere number of intercepted, but nonpertinent calls, is not dispositive."[16] In *Armocida,* where agents intercepted 77 "personal" calls, most of which lasted less than two minutes, the court stated that under the circumstances it would not find "that a full interception of a one-and-one-half minute to two minute conversation violates the minimization requirements."[17]

The Third Circuit has articulated three "crucial" factors for the minimization analysis.[18] First, a court reviewing minimization efforts should consider "the nature and scope of the criminal enterprise under investigation."[19] "[S]omewhat greater latitude may be allowed where conspirators converse in a colloquial code, thereby creating superficially innocent conversations that are actually relevant to the investigation."[20] Moreover, large-scale investigations of criminal conspiracies may need to intercept a greater number of conversations, especially when "the judicially approved wiretap is designed to identify other participants in the conspiracy and to determine the scope of the conspiracy."[21] More recently, the *Hull* court reiterated that "when investigating a wide-ranging conspiracy between parties known for their penchant for secrecy, broader interceptions may be warranted."[22]

Second, courts should consider "the government's reasonable expectation as to the character of, and the parties to, the conversations."[23] By way of example, "if the government knows during what time of the day the telephone will be used for criminal activity, it can avoid intercepting calls at other times."[24] The Supreme Court in *Scott* explained that while agents should not listen to every call over a wiretap on a public telephone where one person is suspected of placing illegal bets, "if the phone is located in the residence of a person who is thought to be the head of a major drug ring, a contrary conclusion may be indicated."[25]

Third, "the degree of judicial supervision by the authorizing judge" must be considered.[26] Section 2518(6) of Title III "permits a district judge,

once he has authorized a wiretap, to continue supervising the operation of the interception by requiring reports from the government." *Id.* Such supervision should be taken into consideration when determining the adequacy of the government's minimization efforts.[27]

The minimization argument, however, is a tedious one that is of limited benefit. In *United States v. Cox*,[28] the court allowed for the only remedy for failure to minimize wiretapping to be a civil suit for the disclosure of the information under § 2520. In *United States v. LaGorga*,[29] the court decided that suppression only applies to the specific interception which is determined to be unlawful, rather than a blanket order which would affect all the evidence, including that obtained by procedures sanctioned by statute and court order.

## "Necessity" Shortcomings as a Challenge to Electronic Interceptions

### *Necessity and Normal Investigative Techniques*

Title III demands that each wiretap application 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."[30]

Similarly, a wiretap order must show the judge's determination that the procedure is necessary: "Upon such application the judge may enter an ex parte order … authorizing … interception of … electronic communications … if the judge determines on the basis of the facts submitted by the applicant that … normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[31]

"The statutory language suggests that before finding that a wiretap is necessary, the court must find that alternative methods have been tried or would not have succeeded."[32] Electronic interceptions should not be permitted if "traditional investigative techniques would suffice to expose the crime."[33] In order to satisfy this requirement, however, the government need only lay a "factual predicate" sufficient to inform the judge why other methods of investigation are not sufficient.[34]

Although the application for a wiretap is likely to follow the guidance of the courts and reflect that alternative methods have been tried and failed, it is possible through a Franks hearing to show that those methods were exaggerated.[35] After the Franks analysis, it was determined that, given an informant who was willing to testify, the necessity requirement was not met.

Many of the normal investigative techniques that must be exhausted before the government resorts to a wiretap are listed below:

- Search warrants
- Witness interviews
- Grand jury testimony/subpoena
- Cooperating witnesses/informants
- Infiltration by undercover agents
- Surveillance
- Video surveillance
- Trash covers
- Mail covers
- Financial investigations
- Pen registers
- Toll registers (phone records)
- Trap and trace[36]

### *Specificity and Boilerplate*

Circuit courts have rejected the use of boilerplate language in support of a necessity showing. The government, "[M]ust allege specific circumstances that render normal investigative techniques particularly ineffective or the application must be denied...."[37]

The government cannot use the investigating agents' conclusions regarding whether or not traditional investigative techniques will theoretically work or not work. The required necessity cannot be shown by "bare conclusory statements that normal techniques would be unproductive."[38]

### *Previous Investigations or Applications cannot be Used as the Proof of Necessity*

The necessity rule requires that each wiretap application stand on its own. The government cannot aggregate necessity from other wiretap applications to show necessity for a subsequent application.[39]

The need for individualized necessity and probable cause showings often is at issue in extension applications. Extension applications are not merely formalities that automatically extend an original wiretap. Section 2518(5) of Title 18 requires that each application for an extension of a wiretap must include a full statement of facts regarding necessity, as is required for original applications under Section 2518(l)(c). There is, however, an additional statutory requirement in Title III for extension applications. Section 2518(l)(f) specifically requires an extension affidavit to provide "a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results."[40] Failure to provide adequate necessity for an application means that probable cause is not shown and the wiretap will be suppressed.[41]

The Supreme Court has acknowledged these separate requirements for extension applications. In *Giordano*, the Court observed that "extension orders do not stand on the same footing as original authorizations … but are provided for separately."[42] It then emphasized the additional showing required by Section 2518(l)(f).[43] The Court found a common sense rationale for this greater showing: Plainly the function of § 2518(l)(f) is to permit the court realistically to appraise the probability that relevant conversations will be overheard in the future. If during the initial period, no communications of the kind that had been anticipated had been overheard, the Act requires an adequate explanation for the failure before the necessary findings can be made as a predicate to an extension order.[44]

## Probable Cause Shortcomings in Wiretap Applications and Orders

### *The Three Probable Cause Requirements of Title III*

A wiretap application (and the resulting order) must establish probable cause in relation to three facts: i) that an individual is committing crime, ii)

that communications about that crime will be intercepted, and iii) that the phone line tapped is being used to communicate about the crime.[45]

As with a traditional search warrant affidavit, a wiretap application must establish that the target has committed or is committing a crime.[46] There are limits as to which crimes are permissible bases for a wiretap (albeit, very broad limits). The statute permits wiretaps for crimes enumerated in 18 U.S.C. § 2516. That statute, in turn, provides a laundry list of federal offenses ranging from assassination of the President to obscenity. The classic wiretapping subjects — drugs and guns clearly fall within the statute, as do all acts of fraud, wire fraud, and bank fraud, as well as computer fraud and nearly one-hundred other enumerated offenses. If the wiretap produces unusual charges, it is worth it to check Section 2516 to make sure the crime is enumerated.

Before obtaining a wiretap, the government must show probable cause that communications about the crime will be intercepted.[47]

The final probable cause requirement is whether the specific target line (a specific phone number) is being used for criminal conversations.[48] This is closely related to the second requirement, that "particular communications" regarding crimes will be intercepted (Section 2518(3)(b)).

Both (b) and (c) appear to be areas ripe for defending in white collar cases. The chances that white collar defendants will be communicating at any particular time about a criminal enterprise, or that a particular line may be fruitful for the investigation would seem hard to prove given the likelihood that any tapped line would be used, in the vast majority of calls, for legitimate business purposes.

Staleness is another area where an argument can be made against the wiretap. Staleness, however, is unlikely to work. The Third Circuit Court of Appeals has explained that "where the facts adduced to support probable cause describe a course or pattern of ongoing and continuous criminality, the passage of time between the occurrence of the facts set forth in the affidavit and the submission of the affidavit itself loses significance."[49] The court has further specified that "[t]he liberal examination given staleness in a protracted criminal conduct case 'is even more defensible in wiretap cases than in ordinary warrant cases, since no tangible objects which can be quickly carried off are sought.'"[50]

## Franks Challenges to Electronic Interceptions

### *Franks and Title III Challenges*

Under the Fourth Amendment, a defendant may challenge a search conducted pursuant to a warrant on the grounds that the warrant affidavit, even though facially adequate to support probable cause, contained factual misstatements or omissions that influenced the issuing magistrate.[51] If the reviewing court determines that an affiant has knowingly or recklessly included false information that is material to the determination of probable cause, evidence seized pursuant to that warrant must be suppressed.[52]

This reasoning applies with equal force to wiretap affidavits.[53] The Franks legal analysis in the context of a wiretap motion is similar to the Franks approach to a search warrant. One significant difference is the impact of the omissions or misstatements upon the government's application; in a wire motion, a Franks error may jeopardize not only probable cause, but also necessity for the wiretap.[54]

A defendant seeking a Franks hearing must make a "substantial preliminary showing"[55] that (1) the affidavit contains a material misrepresentation, (2) the affiant made the misrepresentation knowingly and intentionally, or with reckless disregard for the truth, and (3) the allegedly false statement was material to the finding of probable cause.[56] Where the defendant asserts that the affiant omitted facts with a reckless disregard for the truth, the defendant can satisfy the substantial preliminary showing standard by demonstrating that "an officer recklessly omit[ed] facts that any reasonable person would want to know."[57] If the defendant makes this preliminary showing, but "there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required."[58] If "the remaining content is insufficient," then the defendant is entitled to a hearing.[59]

### *Taint from Previous Wiretaps*

If an original wiretap was improvidently granted, the government cannot use the fruits of that wiretap to obtain authorization for later interceptions.[60]

## Practical Considerations

### *Early Disclosure of Wiretap Applications and Ten-Day Reports*

Title III requires that wiretap applications and orders be disclosed ten days before wiretap proceeds are used in any trial, hearing, or other proceeding in a federal or state court.[61] Although this was presumably intended for evidentiary hearings and trial, this disclosure provision has also been held to apply to detention hearings.[62] Early and aggressive invocation of this right can help back government counsel off of relying on wiretap proceeds in bail hearings (as an AUSA rarely has disclosure ready that early in the case).

### *Early Identification of Cooperating Informants*

Wiretaps are expensive and time-consuming, and are typically only used in fairly serious cases. With high federal sentencing exposures, the likelihood that co-defendants will become cooperating witnesses is increased. Once co-defendants cooperate, their names will likely be omitted from any subsequent wiretap application and instead they will be given code names so that their identities will not be disclosed. Every cooperative co-defendant represents a lost opportunity to identify wire informants.

Therefore, in a defense against wiretap evidence, counsel should review the wiretap applications for any references to cooperating witnesses and informants, and develop outlines of their characteristics such that all defendants, co-defendants and counsel can attempt to identify the informants before they are lost to a §5K1.1 deal.

### *View Hard Copy Originals of All Documents*

In a wiretap in the Northern District of California, the government completely failed to attach a referenced affidavit to a wiretap extension application. The application was nonetheless approved.[63] That omission would have never been detected if someone hadn't gone through all of the hard copy applications and affidavits in the district court clerk's office.

Very close review of the materials actually on file can reveal missing (and essential) attachments, applications that were authorized by the DOJ

official after the district court issued the wiretap order, and DOJ authorizations that are missing altogether.

### *Fight the Recordings Themselves*

The transcripts and the recordings themselves are wide open to interpretation. Nobody, especially those who are being surreptitiously recorded, speaks clearly and precisely when speaking in everyday life. They use jargon, and with people whom they have known for years, or possibly decades, they use plenty of inside references. They think out loud. They ask questions. They brainstorm. They joke. When taken out of context, a statement may sound incriminating, while in the context of the relationship with the other party on the line it is perfectly innocent. Any defense counsel defending against wiretaps must listen to every intercept. The defense should learn the context of each conversation in order to understand and explain what the words spoken truly mean. Any help from the client in shedding light on the actual meaning of a potentially incriminating conversation is invaluable.

Most people speak, especially when in private conversation, in a less formal manner than when they speak publicly or with strangers. They do not enunciate as well. They speak in a lazier, or gruffer, or more accented fashion. Their speech becomes casual. Prosecutors, on the other hand, are listening for evidence of crime and can hear things in a speech pattern that does not exist. They are accustomed to interpreting malfeasance, not innocence. If there is doubt as to the clarity of the words recorded, have an inaudibility hearing and get the recording deemed inadmissible.

## PRACTICAL ADVICE TO OBTAIN A FRANKS HEARING:

- Get a copy of the warrant, the application for a warrant and affidavits and the inventory.
- Get copies of any police reports regarding the warrant.
- Verify all statements in the affidavits and application for warrant.
- Analyze the application and affidavits for omissions.

- Investigate the affidavit and application allegations.
- Review all documentation with the client.
- File a motion to suppress with a request for Franks hearing.
- Look to prove material, deliberate falsehoods or statements made in reckless disregard for the truth, or omissions of material facts, which affect probable cause.
- Submit a revised affidavit without misstatements and include any omitted material information and argue that the revised affidavit fails to support a probable cause finding.
- Informants -
  - obtain their identities
  - get all police reports of statements
  - get prior jail and criminal records
  - discuss informant with client
- Obtain prior affidavits and applications in other search warrant cases of the officers.
- Obtain copies of prior convictions of persons named in the application.

## EXAMPLES OF SUCCESSFUL FRANKS WIRETAP MOTIONS

- *United States v. Novaton* — Affidavit for wiretap falsely stated that four informants had been reliable in the past and failed to include statements about the animosity between informants and target.[64]
- *United States v. Rice* — Suppressing wiretap because of reckless statements in affidavit.[65]

## THE FUTURE — FCPA APPLIED TO PHARMACEUTICALS

The possibilities of fake doctors or fake sales representatives conducting sting operations in order to ensnare one another are not so unrealistic.

Given state run health care systems, the range of foreign officials covered by the FCPA are substantial. In some countries the entire health care system may involve "foreign official[s]" under the FCPA.

In Assistant Attorney General Lanny A. Breuer's November 12, 2009 address to Pharmaceutical Regulatory and Compliance Congress and Best Practices Forum he stated that the DOJ is meshing resources in the fraud section's health care and FCPA silos, and department officials said they have met with overseas counterparts to coordinate for their cooperation in the effort.

Said Breuer:

> In the pharmaceutical context, we have additional expertise that significantly enhances our ability to proactively investigate and prosecute these often complex cases. That additional expertise is located in our health care fraud group, where we have prosecutors and analysts with the industry knowledge necessary to quickly identify corrupt practices. These two groups — our FCPA unit and our health care fraud unit — are already beginning to work together to investigate FCPA violations in the pharmaceutical and device industries in an effort to maximize our ability to effectively enforce the law in this area.

## CONCLUSION

The expansion of surveillance and sting operations into new areas of criminality reflects a shift in resources and attitudes toward white collar crime. As the DOJ melds the expertise it has in prosecution of these cases, the defense bar must step up its game to properly defend these types of cases. By melding expertise in handling government investigations into corporate practices with experience in defending against overbroad and illegal wiretaps we can provide the best defenses available for our clients.

## NOTES

[1] Various resources were used to develop many of the strategies contained herein including, "Uncle Sam is on the Line" by Steven Kalar and Josh

Cohen," "The Criminal Lawyer" blog, and various materials developed by and available through the Office of Defender Services — Training Branch.

[2] *See United States v. Dalia*, 441 U.S. 238, 250 n.9, 252 (1979).

[3] *See Gelbard v. United States*, 408 U.S. 41, 48 (1972).

[4] 18 U.S.C. § 2511(1).

[5] *See, e.g., United States v. Carneiro*, 861 F.2d 1171, 1176 (9th Cir. 1988) ("The district court erred in failing to examine each wiretap application separately. Each wiretap application, standing alone, must satisfy the necessity requirement."); *U.S. v. Majeed*, 2009 WL 2393439, 13 (E.D.Pa. 2009)(showing a thorough wiretap by wiretap analysis).

[6] *See, e.g., United States v. Meling*, 47 F.3d 1546, 1551-52 (9th Cir. 1995) ("Looking only to the four corners of the wiretap application, we will uphold the wiretap if there is a substantial basis for these findings of probable cause.").

[7] 18 U.S.C. § 2518(1).

[8] 18 U.S.C. § 2518(4).

[9] *See, e.g.*, *United States v. Giordano*, 416 U.S. 505, 525-26 (1974) (upholding suppression when wiretap application was not approved by designated official, but by Attorney General's Executive Assistant); *United States v. Chavez*, 416 U.S. 562 (1974) (suppressing wiretap proceeds when application had not been approved by Attorney General or designated Assistant Attorney General); *United States v. Traitz*, 871 F.3d 368, 379-80 (3rd Cir. 1989) (upholding wiretaps when contested application and order identified the authorizing official by title, but not by name); *United States v. Camp*, 723 F.2d 741, 744 (9th Cir. 1984) (permitting the Attorney General to designate the Assistant Attorney General by job title rather than name); *United States v. Citro*, 938 F.2d 1431, 1435 (1st Cir. 1991) (permitting the Attorney General to designate Assistant A.G.'s by title, rather than by name).

[10] 18 U.S.C. § 2518(8)(a).

[11] *United States v. McGuire*, 307 F.3d 1192, 1202-03 (9th Cir. 2002) (*citing United States v. Pedroni*, 958 F.2d 262, 265 (9th Cir. 1992)); *see also U.S. v. Quintero*, 38 F.3d 1317 (3d Cir. 1994) (hectic trial schedule is the norm for federal prosecutors and is not a satisfactory explanation for failure to seal wiretap tapes immediately).

[12] 18 U.S.C. § 2518(5).

[13] *United States v. Hull*, 456 F.3d 133, 142 (3d Cir. 2006) (*citing Scott v. United States*, 436 U.S. 128, 140 (1978)).

[14] *Scott*, 436 U.S. at 132-33. *See also*, *United States v. Vento*, 533 F.2d 838,

854 (3d Cir. 1976) ("Minimization is not to be judged by a rigid hindsight that ignores the problems confronting the officers at the time of the investigation.").
[15] *Scott*, 436 U.S. at 140.
[16] *Hull*, 456 F.3d at 143 (*citing* to *United States v. Adams*, 759 F.2d 1099, 1115 (3d Cir. 1985)).
[17] *United States v. Armocida*, 515 F.2d 49, 52 (3d Cir. 1975).
[18] *Id*. at 52-53.
[19] *Id*.
[20] *Id*.
[21] *Id.*
[22] *Hull*, 456 F.3d at 142.
[23] *Armocida*, 515 F.2d at 44.
[24] *Id*.
[25] *Scott*, 436 U.S. at 140.
[26] *Armocida*, 515 F.2d at 44.
[27] *Id*. at 44-45.
[28] 462 F.2d 1293, 1302 (8th Cir. 1972), *cert. denied*, 417 U.S. 918, 94 S.Ct. 2623, 41 L.Ed.2d 223 (1974).
[29] 336 F. Supp. 190, 196 (W.D.Pa. 1971).
[30] 18 U.S.C. § 2518(l)(c).
[31] 18 U.S.C. § 2518(3)(c)(3).
[32] *United States v. Ippolito*, 774 F.2d 1482, 1485 (9th Cir. 1985).
[33] *United States v. Kahn*, 415 U.S. 143, 153 & n.12 (1974); *see also United States v. Williams*, 124 F.3d 411, 418 (3d Cir. 1997) and *United States v. Armocida*, 515 F.2d 29, 38 (3d Cir. 1975).
[34] *United States v. McGlory*, 968 F.2d 309, 345 (3d Cir. 1992).
[35] *See United States v. Ippolito*, 774 F.2d 1482, 1485 (9th Cir. 1985), wherein the officer did not include that the confidential informant was cooperating in the investigation and willing to testify.
[36] *See generally* S. REP. 90-1097, 1968 U.S.C.C.A.N. 2112, 2190 ("The judgment would involve a consideration of all the facts and circumstances. Normal investigative procedure would include, for example, standard visual or aural surveillance techniques by law enforcement officers, general questioning or interrogation under an immunity grant, use of regular search warrants, and the infiltration of conspiratorial groups by undercover agents or informants.").
[37] *Ippolito*, F.2d at 1486; *see also U.S. v. Teagle*, 2007 WL 2972554 (E.D.Pa.

2007).
[38] *United States v. Ashley*, 876 F.2d 1069, 1072 (1st Cir. 1989). *See also U.S. v. Teagle*, 2007 WL 2972554 (E.D.Pa. 2007) at *4 explaining the specificity of an application.
[39] *See U.S. v. Majeed*, 2009 WL 2393439, at *11 (E.D.Pa. 2009).
[40] 18 U.S.C. § 2518(f).
[41] *U.S. v. Majeed*, 2009 WL 2393439, at *11 (E.D.Pa. 2009).
[42] *Giordano*, 416 U.S. at 530.
[43] *Id*.
[44] *Id.*
[45] 18 U.S.C. § 2518(3)(a)(b) & (d).
[46] 18 U.S.C. § 2518(3)(a).
[47] 18 U.S.C. § 2518(3)(b).
[48] 18 U.S.C. § 2518(3)(d).
[49] *United States v. Urban*, 404 F.3d 754, 774 (3d Cir. 2005).
[50] *Id*. at 775.
[51] *See Franks v. Delaware*, 438 U.S. 154 (1978).
[52] *See U.S. v. Majeed*, 2009 WL 2393439, at *13 (E.D.Pa. 2009).
[53] *United States v. Ippolito*, 774 F.2d 1482, 1485 (9th Cir. 1985); *Majeed*, 2009 WL 2393439, 13 (E.D.Pa. 2009).
[54] *See, e.g*., *Ippolito*, 774 F.2d at 1485 ("The necessity showing and finding are therefore material to the issuance of a wiretap order and are subject to Franks.").
[55] *Franks*, 438 U.S. at 170.
[56] *See id*. at 155-56, 171; *see also United States v. Brown*, 3 F.3d 673, 676 (3d Cir. 1993).
[57] *United States v. Yusuf*, 461 F.3d 374, 383 (3d Cir. 2006) (citing *Wilson v. Russo*, 212 F.3d 781, 783 (3d Cir. 2000)).
[58] *Id*. at 171–172.
[59] *Id*. at 172.
[60] *See, e.g*., *United States v. Giordano*, 416 U.S. 505, 529-30 (1974) ("Even though suppression of the wire communications intercepted under the October 16, 1970, order is required, the Government nevertheless contends that communications intercepted under the November 6 extension order are admissible because they are not 'evidence derived' from the contents of communications intercepted under the October 16 order within the meaning of § § and 2518(10)(a). This position is untenable."); *United States v. Vento*, 533

F.2d 838, 847 (3d Cir. 1976) ("If the government's application did not present probable cause for the authorization of the interception, then the authorization and any surveillance pursuant to it were improper. And, if the surveillance was improper, the government could not use the fruits of that surveillance at trial or to further its investigation.").

[61] *See* 18 U.S.C. § 2518(9).

[62] *See United States v. Salerno*, 794 F.2d 64 (2d Cir. 1986), rev'd on other grounds, 107 S. Ct. 2095 (1987) ("We think it clear that Congress intended § 2518(9) to apply to detention hearings.").

[63] See *U.S. v. Callum*, 410 F.3d 571 (9th Cir. 2005) (showing the difficulty in challenging a wiretap that is is flawed on its face, "Under the force of precedent, we uphold the challenged wiretap applications and orders. Still, we note that the Department of Justice and its officers did not cover themselves with glory in obtaining the wiretap orders at issue in this case."). *Id* at 577.

[64] 271 F.3d 968 (11th Cir. 2001).

[65] 478 F3d 704 (6th Cir. 2007).