INTRODUCTION

Within the arsenal of crime detection tools available to law enforcement is electronic surveillance. One of the best uses of electronic surveillance is to investigate and ultimately prosecute conspiracies, other organized criminal activity, or ongoing criminal activity.¹

Included among the common forms of electronic surveillance are wiretaps and implants ("bugs").² Such electronic surveillance can be very beneficial to law enforcement because of the extremely intrusive nature of the surveillance. However, because of this intrusiveness, significant statutory and judicial protections have resulted.

At the heart of the protections afforded the various communications upon which government intrusion is possible by means of electronic surveillance is the right to privacy.³ The government is held to a high standard of compliance under the law authorizing such intru-
The right to privacy and, hence, the protection afforded private communications intercepted by electronic surveillance, depends on the nature or means of the communication and the extent of government intrusion. For example, the installation and use of a pen register does not impinge upon an individual's expectation of privacy and, therefore, does not rise to the same level of protection as would a wiretap. This is because the pen register intercepts and registers only the electronic impulses that are communicated between telephones to establish the link through which the voice (aural) communication will travel. In comparison, a wiretap actually intercepts the aural communication between the parties.

The pen register (in addition to the trap and trace — or caller identification services) will inform the investigator of only the telephone numbers of the communicating telephones, the time of day of the call, and the length of the communication. A pen register will not identify the persons speaking over the wire or the conversation being communicated between the parties.

Abuses of the legitimate use of electronic surveillance are not only an unauthorized intrusion by government into the private affairs of people, but also a serious disservice to law enforcement and to the community as a whole regarding the community's continuing effort to be secure from crime. From a pragmatic standpoint, serious violations by law enforcement in their use of electronic surveillance beyond the legal limits on electronic surveillance can result in the

---


   We think that unfortunately the failure to seal the Levittown tapes here resulted from a disregard of the sensitive nature of the activities undertaken. The danger here is, of course, that today's dereliction becomes tomorrow's conscious avoidance of the requirements of law. The privacy and other interests affected by the electronic surveillance statutes are sufficiently important, we believe, to hold the Government to a reasonably high standard of at least acquaintance with the requirements of law.

Id. (citing United States v. Giordano, 416 U.S. 505, 527 (1974) (stating that "Congress intended to require suppression where there is [a] failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device").


suppression of key evidence.\textsuperscript{8}

The significance of the zone of privacy at issue and the legislative attempts at allowing, but limiting, electronic surveillance have led to the litigation of a number of challenges to the use of electronic surveillance. Most notably, these challenges have arisen in cases involving electronic surveillance as direct or derivative evidence. It is my purpose in this Article to address four of those areas of concern: (1) exhaustion of alternative methods of investigation, (2) achievement of the objectives of the electronic surveillance, (3) limiting ("minimizing") authorized electronic surveillance, and (4) maintaining the integrity of the product of the electronic surveillance ("sealing").

FEDERAL STATUTORY OVERVIEW

In 1986, by amending then-existing statutes, Congress enacted what is generally the present form of federal law governing the use of electronic surveillance.\textsuperscript{9} Included within electronic surveillance is the area of applied technology which intercepts only electronic impulses demonstrating and identifying the connection between sending and receiving devices (i.e., trap and trace devices, pen registers, and arguably similar devices or applications of technology).\textsuperscript{10} A separate federal statute governs the use of this "associated" technology.\textsuperscript{11}

The statute regulating electronic surveillance is organized around three types of communication: "wire communications," "oral communications," and "electronic communications."\textsuperscript{12} The main concern of "wire communications" is the "aural transfer" of communications.\textsuperscript{13} To constitute an "aural transfer" within the meaning of the statute, a transfer must: (1) contain the human voice at any point be-


\textsuperscript{10} The amendment of statutes does not always keep pace with the advance of technology. For example, caller identification service is presently available. Although it is arguably covered in the statute under § 3121, there is no express inclusion of the service in the statute. However, lack of express inclusion within the statute does not appear to preclude court authorized use of the technology. See 18 U.S.C. § 3127(4) (1988) (defining "trap and trace device"); 18 U.S.C. § 1851(a) (1988) (codification of the All Writs Act); Smith v. Maryland, 442 U.S. 735 (1979); United States v. New York Tel. Co., 434 U.S. 159 (1977); In re Application of the United States for an Order, 616 F.2d 1122 (9th Cir. 1980).


\textsuperscript{12} 18 U.S.C. §§ 2510-20.

\textsuperscript{13} Id. § 2510(1), (18).
between origin and reception; (2) be transferred by aid of wire, cable, or like connection; or (3) be engaged in providing or operating for interstate or foreign commerce. "Aural transfers" expressly include the electronic storage of such transfers. "Aural transfers" expressly exclude "the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit." The interception of aural transfers involves the use of a wiretap.

The second type of communication covered by the statute is "oral communication." Although somewhat circular in definition, the statute defines "oral transfer" to mean "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." "Oral communication" expressly excludes any electronic communication. The interception of "oral communication" involves the use of implants ("bugs").

The third type of communication covered by the statute is "electronic communication." The statute treats an electronic communication: (1) as any transfer of signs, signals, writing, images, sound, data, or intelligence of any nature; (2) which is transmitted in whole or part by wire, radio, or other specified means of transmittal; and (3) which affects interstate or foreign commerce. Electronic communication expressly excludes: (1) the radio portion of a cordless telephone, (2) any wire or oral communication, (3) any communication made through a tone-only paging device, and (4) any communication from a tracking device.

The statute defines "intercept" to include the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. The situation employing what is commonly known as "consensual monitoring" is exempted from the prohibitions covered by the statute.

The central intent of the statute is to declare it unlawful to in-
intercept the communications covered by the statute unless there is an express authorization or exception granted by the statute. The statute also expressly prohibits the use in evidence of communications intercepted in violation of the statute.

GENERAL CONSIDERATIONS

1. NATURE OF POSSIBLE CHALLENGES

Challenges to using the product of an intercept tend to be raised in one of three ways:

1. There was an error or omission regarding the application/affidavit for the intercept which is sufficient to require suppression of the results thereof (i.e., a Franks v. Delaware hearing);

2. Although not based on error or omission in the application/affidavit, the application/affidavit failed to satisfy the requirements of the statute, and the results of the intercept should, therefore, be suppressed (e.g., no probable cause, failure to exhaust alternative investigative techniques, no grounds for extension of the original order, or failure to identify target interceptees);

3. The order for the intercept was carried out in a manner contrary to the order/statute, and the results of the intercept should, therefore, be suppressed (a “section 3504 hearing”).

2. THE APPLICATION FOR ELECTRONIC SURVEILLANCE

The treatment of the application/affidavit in support of a wiretap or implant is much the same as the treatment of an application/affidavit.

23. See id. §§ 2511-13. See also 18 U.S.C. § 3121(a) (prohibiting pen register or trap and trace without a court order); United States v. Sedovic, 679 F.2d 1233, 1235 (8th. Cir. 1982).


25. Id. § 2515.

26. Id. § 2518(10)(a). Section 2518(10)(a) states in pertinent part:

Any aggrieved person may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that — (i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval.

27. Many of the references contained in the Article to the application for an order authorizing electronic surveillance also refer to the affidavit in support of the application because the application must be accompanied by an affidavit which should be incorporated into the application. Any consideration of the application should, therefore, be a consideration of the application/affidavit.


davit in support of a search warrant.\textsuperscript{31} The underlying rationale is the same: the authorization by an impartial judicial officer of the government’s invasion of an otherwise legitimate expectation of privacy by the person(s) subject to the government intrusion.\textsuperscript{32}

It is well established that the affidavit used to support the issuance of the wiretap order is presumed valid.\textsuperscript{33} The judge to whom the wiretap application is presented is entrusted with broad discretion, and the judge’s determination to grant the wiretap application is entitled to great deference.\textsuperscript{34}

An order authorizing the interception of aural/oral communications must be based on a finding of probable cause by the issuing judicial officer. This is comparable to the issuance of a search warrant.\textsuperscript{35} Of course, it is the application/affidavit which forms the basis of the judicial officer’s findings.

The tests for probable cause also are well established, and are based on a “totality of the circumstances” analysis.\textsuperscript{36} Applications/affidavits for electronic surveillance have generally been upheld against challenges based on lack of probable cause.\textsuperscript{37}

A court is to review the application/affidavit in a practical and common-sense manner, rather than in a hypertechnical manner.\textsuperscript{38} A significant part of the practical and common-sense analysis of the affidavit/application for a wiretap in many cases is that by its stated goals it pertains to the investigation of a conspiracy, other organized crime, or other continuing crime. The use of a wiretap has been found to be particularly appropriate in the investigation of a conspiracy.\textsuperscript{39}

3. \textbf{WHETHER TO SUPPRESS THE PRODUCT OF THE INTERCEPT}

As part of the court’s avoidance of a hypertechnical approach to

\begin{itemize}
  \item \textsuperscript{32} United States v. Leon, 468 U.S. 897, 919-923 (1984); United States v. Mims, 812 F.2d 1068, 1072-73 (8th Cir. 1987).
  \item \textsuperscript{33} \textit{Van Horn}, 579 F. Supp. at 811 (citing \textit{Franks}, 438 U.S. at 171).
  \item \textsuperscript{34} Id.
  \item \textsuperscript{35} 18 U.S.C. § 2518(3); Alderman v. United States, 394 U.S. 165, 175 (1969); \textit{Leisure}, 844 F.2d at 1354.
  \item \textsuperscript{36} Illinois v. Gates, 462 U.S. 213, 238 (1983); United States v. Ashley, 876 F.2d 1069, 1073 (1st Cir. 1989); \textit{Leisure}, 844 F.2d at 1354; United States v. Doty, 714 F.2d 761, 763 (8th Cir. 1983).
  \item \textsuperscript{37} \textit{Garcia}, 785 F.2d at 221-23; United States v. Kirk, 534 F.2d 1262, 1274 (8th Cir. 1976), \textsuperscript{cert} denied, 433 U.S. 907 (1977); United States v. Schaefer, 510 F.2d 1307, 1310 (8th Cir.), \textsuperscript{cert} denied, 421 U.S. 978 (1975); United States v. Brick, 502 F.2d 219, 224 (8th Cir. 1974); United States v. Kleve, 465 F.2d 187, 193 (8th Cir. 1972).
  \item \textsuperscript{38} \textit{Van Horn}, 579 F. Supp. at 810 n.4.
  \item \textsuperscript{39} Id. at 814.
\end{itemize}
reviewing an application/affidavit for electronic surveillance (i.e., wiretap or implant), a court need not suppress all evidence gathered as a result of a violation of the empowering statutes. The United States Supreme Court has held that "suppression is required only for a 'failure to satisfy . . . statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures.'"  

If a violation of the statute appears more technical than substantive and prejudice has not resulted to the persons aggrieved by the use of electronic surveillance in violation of statute, suppression of the fruits of the surveillance may be avoided. The United States Court of Appeals for the Eighth Circuit has adopted a three-part test to determine whether the product of an intercept must be suppressed:

1. Is the procedure that was employed by law enforcement to carry out the electronic surveillance a central or functional safeguard of the statute which was intended to prevent abuses?

2. If the procedure employed does pertain to a key safeguard of the statute, was the intended safeguard (i.e., avoidance of abuse) met despite the error in procedure at issue?

3. Did law enforcement deliberately ignore the requirements of the statute in employing the erroneous procedure and thereby gain some advantage in carrying out the intercept?

Examples of failure to comply with the statute which may not require suppression of the fruits of a wiretap or implant are a failure, under limited circumstances, to timely present interim reports to the supervising court, or a failure, not predicated on bad faith, to identify all of the interceptees of a wiretap regarding the requirement of serving an inventory (notice of interception) on all interceptees, with the failure later cured.

If a court determines that there was an unlawful act in the use of electronic surveillance to gather evidence, the evidence at issue may still be admissible if the government can demonstrate that the evidence did or clearly would have resulted from some source other than the intercept (i.e., that the taint of the unlawful act is somehow satisfactorily separated from the obtaining of the evidence).

As with a search warrant, in obtaining an order authorizing the

---

40. Donovan, 429 U.S. at 433-34; Giordano, 416 U.S. at 527; Chavez, 416 U.S. at 574-75.
42. Id. at 1400.
interception of aural/oral communications, it may be possible under appropriate circumstances to avoid suppression of the fruits of the intercept even if the order is later overturned because of a defect in the application/affidavit. The order will be upheld if the investigators have acted in good faith, placed reasonable reliance on the order, and done nothing to mislead the issuing judicial officer. The judicial officer also must have acted in good faith for that evidence to be determined nondefective, and the judicial officer may not abandon his or her objective neutrality in issuing the order.44

Furthermore, even if a court suppresses the fruits of electronic surveillance for purposes of the government's case-in-chief, it may be possible to use the fruits of the electronic surveillance for purposes of impeachment.45

4. STANDING

To have the necessary standing to challenge the interception of aural/oral communication by electronic surveillance, the challenging defendant must be an aggrieved person within the meaning of the statute and the Fourth Amendment.46 No special standing has been recognized for co-conspirators or co-defendants.47 The Eighth Circuit has followed the rationale used by the United States Supreme Court in establishing standing to seek the suppression of evidence under situations of claimed "derivative" or "vicarious" standing.48

44. Leon, 468 U.S. at 919-23 (1984); Mims, 812 F.2d at 1072.
46. See 18 U.S.C. § 2518(10)(a) (providing that "any aggrieved person" may bring a suppression challenge). See also 18 U.S.C. § 2510(11) (defining "aggrieved person" as "a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed").

In Civella, the Eighth Circuit stated:

Our review of the case law and the federal wiretap statute . . . indicates that a defendant may challenge evidence gathered pursuant to an interception order only if it is shown "that it was directed at him, that the Government intercepted his conversations or that the wiretap communications occurred at least partly on his premises."

Civella, 648 F.2d at 1171 (citations omitted). See also Alderman, 394 U.S. at 175-76 (explaining the correlation between standing under Fed. R. Crim. P. 41(e) and standing for a statutory challenge under Title III of the Omnibus Crime Control and Safe Streets Act).


48. See United States v. Wiley, 847 F.2d 480, 481 (8th Cir. 1988); United States v. Tate, 821 F.2d 1328, 1330 (8th Cir. 1987) (considering Fifth Amendment rights, rather than Fourth Amendment rights), cert. denied, 484 U.S. 1011 (1988); United States v.
5. Requirements in Challenging the Intercept

A Franks v. Delaware-type hearing is used to challenge the application as it appears on its face. In such a proceeding, it is well settled that the burden is on the defendant challenging the application/affidavit to make specific factual allegations of illegality with regard to the application/affidavit (i.e., that the application/affidavit is erroneous by an overt act or omission of the presenting agent/officer, either intentionally or recklessly, and that the agent/officer has misled the judicial officer issuing the order). The defendant must produce evidence and persuade the court that the evidence should be suppressed.49 The challenging party's burden is to prove his/her position by a preponderance of the evidence, whereafter the burden shifts to the government to prove the wiretap's legality.50

When a defendant challenges the admissibility of the evidence gathered by electronic surveillance by alleging that an unlawful act was involved in the gathering of the evidence, the defendant first must set forth a specific allegation of the unlawful act. It is then incumbent upon the prosecutor seeking admission of the evidence, acting within the facts and in good faith, to affirm or deny the occurrence of any such unlawful act in the gathering of the evidence. Thereafter, the risk should fall on the defendant as to whether the evidence should be admitted.61

---

51. See 18 U.S.C. § 3504. Section 3504 provides in pertinent part:
   (a) In any trial, hearing, or other proceeding in or before any court . . . (1) upon a claim by a party aggrieved that evidence is inadmissible because it is the primary product of an unlawful act or because it was obtained by the exploitation of an unlawful act, the opponent of the claim shall affirm or deny the occurrence of the alleged unlawful act; . . .
   (b) As used in this section "unlawful act" means any act the use of electronic, mechanical, or other device (as defined in section 2510(5) of this title) in violation of the Constitution or laws of the United States or any regulation or standard promulgated pursuant thereto.

Id.; see Phillips, 540 F.2d at 326 n.3.
EXHAUSTION OF ALTERNATIVE INVESTIGATIVE TECHNIQUES

One challenge to the use of electronic surveillance is the claim that the order authorizing the surveillance should never have been granted because the applicant failed to make the requisite showing that law enforcement had exhausted all alternative investigative techniques prior to the application for electronic surveillance. The argument would follow that if the order should never have been granted, the fruits of the exercise of the order should be suppressed.

Section 2518(1)(c), of Title 18, in the United States Code states in pertinent part, "Each application shall include the following information . . . 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." However, upon careful reading of this section, the requirement is not that the applicant must demonstrate that all other reasonable investigative techniques have actually been tried and failed. Entire categories of potential investigative techniques may be eliminated upon the reasonable expert opinion that such techniques are reasonably anticipated to be too dangerous or likely to fail, but always for an express reason.

Further, section 2518(1)(c) does not require that all investigative techniques must necessarily have been considered or exhausted before a wiretap or implant may be ordered. Congress has not intended that electronic surveillance necessarily be an investigative tool of last resort.

The standards to be applied with regard to section 2518(1)(c) in the Eighth Circuit are stated in United States v. Jackson:

The Supreme Court has stated that the language of §§ 2518(1)(c) and 2518(3)(c) "is simply designed to assure that wiretapping is not resorted to in situations where traditional investigative techniques would suffice to expose the

52. 18 U.S.C. § 2518(1)(c).
53. Garcia, 785 F.2d at 223; Leisure, 844 F.2d at 1356 (involving offenses regarding unauthorized creation of destructive devices); United States v. Daly, 535 F.2d 434, 439 (8th Cir. 1976) (involving a stolen credit card ring). In Daly, the Court stated:
This case is, we feel, a classic instance where electronic eavesdropping was reasonable and necessary. Daly's reliance on telephones, his distrust of confederates, and use of specialized jargon, rendered normal investigative techniques impractical. The broad scope and complexity of the operation compounded the investigative dilemma. Judge Regan properly concluded that alternative investigative means were inadequate.
54. 822 F.2d 1284, 1237 (2d Cir. 1987).
crime." . . . In enacting Title III, Congress did not require the exhaustion of "specific" or "all possible" investigative techniques before wiretap orders could issue. . . . Congress prohibited wiretapping only when normal investigative techniques were likely to succeed and not be too dangerous, . . . and "[m]erely because a normal investigative technique is theoretically possible, it does not follow that it is likely." . . . Thus, §§ 2518(1)(c) and 2518(3)(c) have been deemed to be designed only to ensure that wiretapping is not "routinely employed as the initial step in criminal investigation."

The issue of whether the provisions of §§ 2518(1)(c) and 2518(3)(c) have been complied with must be determined by viewing the facts contained in the Government's sworn applications and supporting affidavits. These applications and affidavits must be tested in a "practical and commonsense fashion." Moreover, as in other suppression matters, the judge to whom the wiretap application is made is entrusted with broad discretion.55

This issue also has been addressed by the United States District Court for the District of Nebraska, in the case of United States v. Van Horn,56 where the court stated:

The state and federal wiretap statutes allow a judge to enter an order authorizing interception of wire or oral communications if the judge determines on the basis of the facts submitted by the affiant 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." . . . The Court finds the affidavit/applications demonstrate sufficient prior use of conventional methods of investigation to justify the use of electronic surveillance in the Zookeeper investigations. In this regard, law enforcement officials are not required to exhaust "all possible" investigative techniques before wiretap orders may issue. . . . Sections 2518(1)(c) and 2518(3)(c) are meant to ensure that wiretapping is not "routinely employed as the initial step in criminal investigation." . . . The statutory requirements are designed to inform issuing magistrates and judges of the difficulties involved in the use of conventional techniques. . . . Law enforcement officers must provide the court with sufficient information by which the court may make an independent assessment of the necessity of the wiretaps . . . It is enough


that the affidavit explains the prospective and retrospective failure of several investigative techniques that reasonably suggest themselves.\textsuperscript{57}

There are certain standard types of investigative techniques to which reference might be made in the application/affidavit. Types of investigative techniques that might be considered include: telephone toll records, pen register, trap and trace (caller identification services), stationary surveillance, mobile surveillance, undercover agent, cooperating informant, garbage collection, interviews, grand jury testimony, administrative subpoenas, grants of immunity, search warrants, and, in limited cases, video surveillance (\textit{i.e.}, requiring court order, as opposed to what "the human eye can see").

**ACHIEVEMENT OF OBJECTIVES: DURATION OF THE INTERCEPT**

Another significant issue regarding interception of aural/oral communications is that after the first intercept that appears to indicate the existence of the target criminal offense, the intercept must terminate. The focus of the suppression argument is that after the occurrence of such event, the continuation of the intercept is in violation of the statute (and probably the authorizing order), and, therefore, all evidence obtained after that event must be suppressed.\textsuperscript{58}

If the objectives of the intercept are well stated in the application and the authorizing order, the law supports continuation of the intercept even after the first event that appears to indicate the targeted criminal offense.\textsuperscript{59} Again, it should be noted that the best use of electronic surveillance seems to be those instances in which the offense under investigation concerns a conspiracy or continuing criminal activity.\textsuperscript{60} As with all uses of electronic surveillance, the is-


\textsuperscript{58} 18 U.S.C. § 2518(5).

\textsuperscript{59} Id. Section 2518(5) provides in pertinent part:

(5) No order entered under this section may authorize or approve the interception of wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days ... and must terminate upon attainment of the authorized objective, or in any event in thirty days.

\textit{Id.}; see Van Horn, 579 F.2d at 815-16; Leisure, 844 F.2d at 1358-59.

\textsuperscript{60} United States v. Cox, 462 F.2d 1293, 1303-04 (8th Cir. 1972) (discussing Katz v.
suing judicial officer will review the original and any extension application/affidavit for probable cause regarding the necessity of continuing the intercept.

It appears to be advisable for the application/affidavit to refer at least categorically to known difficulties regarding achieving the stated objectives of the electronic surveillance. For example, the application/affidavit in a drug investigation might rely on the expert opinion of a qualified investigating agent to state that a standard form of communication by telephone is to speak cryptically or in code, thereby anticipating the necessity of a continued operation of the intercept to determine the actual meaning of the language used between suspected co-conspirators.\textsuperscript{61}

This also might be done with particularity regarding the instant investigation. For example, it may be known that the criminal endeavor under investigation centers on one person who deals with a large number of other persons. Moreover, it may be known that the telephone is used to accomplish communication between the key person and the network of persons with whom the key person works. However, it also may be known that ordinary surveillance for some specified reason has failed to reveal the identities of the other persons involved in the criminal enterprise. Therefore, it may be anticipated, if the stated objectives of the intercept include identification of all the persons involved in the criminal enterprise, that it will be necessary to continue the intercept beyond the first intercept that indicates that the target criminal offense has been verified.\textsuperscript{62}

There is a need to assess whether the electronic surveillance has achieved its stated objectives throughout the duration of the original period of interception, as well as any extension thereof. The statute provides for interim reports to be made to the judge supervising the surveillance to allow the judge to determine the need for continued surveillance.\textsuperscript{63}

\textsuperscript{61} E.g., Cox, 462 F.2d at 1300-01.

\textsuperscript{62} E.g., Daly, 535 F.2d at 438-39 (involving the investigation of a stolen credit card ring, as distinguished from many of the cases which deal with drugs or gambling). In Daly, the court upheld an extension of the wiretap, not only to identify the persons providing Daly with the stolen credit cards, but also to identify the businesses other than service stations that Daly's operation had infiltrated (arguably identifying not only the extent of the operation, but also its victims).

\textsuperscript{63} 18 U.S.C. § 2518(6). Section 2518(6) provides:

Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.
MINIMIZATION

Minimization concerns the limitation placed on the intrusion of the electronic surveillance by the statute or by the order authorizing the surveillance. Minimization has both a "horizontal view" and a "vertical view." The horizontal view assesses the entire span of the electronic surveillance. This view requires an examination as to whether the monitors (persons conducting the surveillance) have limited the conversations to which they listened to comply with the statute and the authorizing order.

The vertical view assesses one specific intercept or one small group of intercepts. Under this view, the question is whether the monitor has limited his or her intrusion into this conversation in compliance with the statute and the authorizing order.

Whether addressing the horizontal or vertical view of minimization, the central thrust of minimization is that the investigators monitoring aural/oral communications over the target telephone number, or at the target location, should monitor only those conversations and parts of conversations that are authorized by the statute and by the order (i.e., relating to the target offenses or the manner of carrying out those offenses). Although not exclusively limited thereby, the stated objectives of the intercept are important in measuring the latitude of monitoring permitted. The target offenses and target interceptees also are important for this purpose.

It may not be unusual for persons using the telephone in furtherance of some ongoing criminal activity to speak cryptically, in specific codes, or to bury criminal conversation sporadically within some tedious, personal conversation. The problem may be even more acute.

Id. 64. See id. § 2518(5). Section 2518(5) provides: "Every order and extension thereof . . . shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." Id. 65. Cox, 462 F.2d at 1300-01 (distinguishing between minimization and discreetness in monitoring interceptions during electronic surveillance).

An attempt is made in this Article to use the term "monitor" when referring to the actual intercept of aural/oral communication in an effort to stress that, under practical circumstances, intercept includes listening and/or recording the communication.


68. This does not mean that the monitors are prohibited from listening to conversation regarding crimes other than the "target crimes" (i.e., those contained in the authorizing order). Neither does this mean that only conversations between "target interceptees" (i.e., persons whose communications are authorized to be monitored in the order) may be monitored. See 18 U.S.C. § 2517(5).

69. See United States v. O'Connell, 841 F.2d 1408, 1417 (8th Cir.), cert. denied, 488 U.S. 1011 (1989); United States v. Losing, 539 F.2d 1174, 1180 (8th Cir. 1976), cert. de-
when monitoring oral communication by means of an implant.\textsuperscript{70} Reliance on the interim report suggested in the statute\textsuperscript{71} and ordinarily ordered by the supervising court might be appropriate with regard to such conversations hidden within conversations.

In applying the minimization requirements of the statute,\textsuperscript{72} courts have determined that, although the state of mind of an agent or officer (i.e., good faith effort to comply with the statute and the authorizing order) regarding minimization may, in some regards, be instructive, it is not initially determinative of whether a violation of the minimization requirements has occurred. Rather, a court reviewing compliance with minimization requirements, on a case-by-case basis, first must undertake an objective analysis of the actions of the monitors of the communications at issue. The standard of review is reasonable compliance under the facts unique to the case under review.\textsuperscript{73}

The United States Supreme Court has indicated various factors to be used in evaluating whether the monitors of an intercept have complied with the minimization requirements. Among these factors are:

1. That "the statute does not forbid the interception of all nonrelevant conversations;"\textsuperscript{74}

2. That, although a computation of the percentage of nonpertinent calls intercepted may, under some circumstances, assist in analysis, generally this is not determinative of the issue;\textsuperscript{75}

3. That the circumstances of the intercept must be considered;\textsuperscript{76}

\textsuperscript{70} United States v. Costello, 610 F. Supp. 1450, 1474 (N.D. Ill. 1985), aff'd sub nom., United States v. Olson, 830 F.2d 195 (7th Cir. 1987), and cert. denied, 484 U.S. 1010 (1988).
\textsuperscript{71} 18 U.S.C. § 2518(6).

Previous reference has been made to United States v. Cox, 462 F.2d 1293 (8th Cir. 1972). The decision in Cox should be read as being correct in historical context and in its general description of the two types of minimization (i.e., term of the intercept and discreetness of the intercept). However, it would be error to find any suggestion in Cox that a violation of the statute or the authorizing order with regard to minimization is never sufficient to result in the suppression of evidence obtained as a result of the breach of minimization requirements. As suggested in the preliminary case history in Scott, suppression could result under certain circumstances. See Scott, 436 U.S. at 131-35.

\textsuperscript{74} Id. at 140.
\textsuperscript{75} Id.
\textsuperscript{76} Id.; Garcia, 785 F.2d at 224. This could include such factors as: (1) the reason-
4. That a pattern of innocent communications cannot be established.\(^77\)

The last point regarding patterns of communication may prove especially important. The monitors of the intercept should be alert to the development of a pattern of innocent conversation between certain persons involved in repetitive communication. If such a pattern is or should be discerned by the monitors acting reasonably and in good faith under the minimization instructions, then, depending on the circumstances, conversations between those persons should either stop being monitored or should be minimized to a greater extent than others.

Of course, it is key to this function that the monitors may exercise a reasonable time or number of communications between these persons to determine whether a pattern of innocent communication exists. This necessarily implies that there is more ability to monitor communications earlier in the term of the intercept than later in the intercept.\(^78\) The issue of a pattern of innocent communications further demonstrates the importance of the interim report required by the statute and ordered by a court.\(^79\)

Central to the concept of minimization is the function of “spot checking.” At the beginning of an intercept, greater latitude is afforded the monitors in monitoring entire communications. However, as the intercept develops, especially with regard to persons whose voices are recognized as having been intercepted previously during the term of this intercept, there is an increased expectation that the monitors will limit their monitoring away from purely personal communications.

However, this does not mean that the monitors cannot monitor to any extent some communications in circumstances where the monitors think that the communications may not be within the express categories of crimes authorized to be intercepted. Monitors may “spot monitor” such communications briefly at certain intervals of time to be relatively certain that no criminal communication is a part

\(^77\) Scott, 436 U.S. at 141-42.
\(^79\) 18 U.S.C. § 2518(6); see supra note 67.
of the communication in progress.\textsuperscript{80}

The minimization expectations include concerns regarding: new subjects/unknown persons, privileged communications\textsuperscript{81} (e.g., attorney-client,\textsuperscript{82} clergyperson-penitent/parishioner, doctor-patient, husband-wife,\textsuperscript{83} and other interpersonal relationships), evidence of crimes other than target crimes,\textsuperscript{84} communications not involving target interceptees,\textsuperscript{85} patterns of innocence, patterns of involvement, and exigent circumstances.\textsuperscript{86}

A special situation involving minimization is the circumstance in which all or a portion of the communication being intercepted is in a foreign language or in a "true" code. In such cases, the statute provides that the communication may be monitored in its entirety. However, this exception applies only so long as the recorded product of the intercept is minimized as soon as practicable after the intercept is completed.\textsuperscript{87}

If there is an attempt to suppress the product of an intercept for failure to minimize the intercept, the demonstrated attempt by monitors to comply with accepted minimization standards could prove determinative of the issue.\textsuperscript{88} It also should be noted that an

\textsuperscript{80} \textit{Losing}, 560 F.2d at 909 n.1. (approving "spot monitoring" in which the monitoring function is engaged for up to two (2) minutes).

\textsuperscript{81} If a failure to minimize is claimed on the basis of a privileged communication, the burden is on the party claiming the privilege to prove the existence of the privilege and that the communication is within the protection of the privilege.


\textsuperscript{83} Special attention may be paid to husband-wife confidential communications in criminal enterprises in which both are involved in the crime. In general, it may be argued that communications between a husband and wife are not privileged if they are strictly in the nature of a business communication (i.e., the business of the crime). See \textit{United States v. Malekzadeh}, 855 F.2d 1492, 1496 (11th Cir. 1988), \textit{cert. denied}, 489 U.S. 1029 (1989); \textit{United States v. Kapnison}, 743 F.2d 1450, 1454 (10th Cir. 1984), \textit{cert. denied}, 471 U.S. 1015 (1985); \textit{Fowler v. United States}, 352 F.2d 100, 113 (8th Cir. 1965), \textit{cert. denied}, 383 U.S. 907 (1966). Of course, the only concern at issue is the confidential communication. Nothing herein deals with the "anti-spousal testimony privilege."

\textsuperscript{84} It is appropriate to intercept communications regarding crimes for which interception is not authorized in the order. However, should this occur, for use of the "other crime" intercept to be made in evidence, there must be compliance with 18 U.S.C. § 2517(5).

\textsuperscript{85} See supra note 74.

\textsuperscript{86} For example, what must be done to preserve the integrity of the electronic surveillance in a wiretap if the recorder fails to function?

\textsuperscript{87} 18 U.S.C. § 2518(5). Section 2518(5) provides in pertinent part: "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." \textit{Id.} (emphasis added).

isolated error, or even a few isolated errors, regarding minimization will not necessarily require suppression of the entire intercept or even of the entire communication in which the error occurred. The degree of supervision of the intercept also may impact on the demonstration of good faith compliance with minimization requirements. This suggests the importance of timely compliance with the interim report requirements established by the order authorizing the intercept or any extensions thereof.

SEALING THE PRODUCT OF THE INTERCEPT

A significant suppression issue that was recently in issue concerned the sealing of the tapes of intercepted communications. Sealing is one of the elements of a court's supervision of the intercept. It involves the court taking physical custody of, or directing the physical custody of, the recorded product of the intercept, and providing that such recorded product be maintained in a condition and situation which guarantees the authenticity of the recorded product of the intercept from the time the court takes custody.

The seal of the court on the product of the intercept is a prerequisite for admission of the product into evidence. The timeliness of the placement of the court's seal, and hence the receipt of the product of the intercept by the court, is important and was the ultimate issue in United States v. Ojeda Rios.

The statute requires the product of the intercept to be sealed immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation of the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

90. 18 U.S.C. § 2518(6); see supra notes 66, 74.
91. 18 U.S.C. § 2518(8)(a). Section 2518(8)(a) provides:

The contents of any wire, oral or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation of the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517.

92. Ojeda Rios, 495 U.S. at 262-63.
93. 18 U.S.C. § 2518(8)(a); Ojeda Rios, 495 U.S. at 262-63.
mediately upon termination of the authorizing order. The order terminates automatically upon its expiration date if not extended, or earlier upon the decision of investigators that optimum benefits have been achieved by the intercept and that the monitoring cease.

Although the full parameters of "immediately" may not have been definitively determined, it certainly does not mean 82 days or 118 days after the termination of an intercept. However, the Supreme Court in Ojeda Rios did not comment on the failure of the United States Court of Appeals for the Second Circuit to overturn a district court order admitting into evidence tapes from wiretaps in which twenty days and sixteen days, respectively, had passed between the termination of the authorizing order and the sealing of the tapes with the court. One circuit court of appeals has found that sealing the product of the intercept within one or two days of the termination of the intercept is timely compliance with the mandate that such product be sealed immediately.

The Supreme Court in Ojeda Rios made it clear, however, that

96. See Ojeda Rios, 495 U.S. at 262-63. The Ojeda Rios case dealt with a series of wire taps in Puerto Rico. As noted by Justice Stevens in the dissent, the case involved 1011 tapes, gathered under 8 authorizing orders and 17 extension orders. See id. at 289-70 (Stevens, J., dissenting).

The general facts of the case are set forth in the majority opinion. Id. at 260-62. The case dealt with at least four separate wire taps: (1) Levittown, (2) El Cortijo, (3) Vega Baja-private, and (4) Vega Baja-public. For investigative purposes, the wire taps were grouped: Levittown and El Cortijo together and the "two" Vega Baja intercepts together.

The Levittown order was originally entered April 27, 1984, and with two extensions expired July 23, 1984. The El Cortijo order was originally entered July 27, 1984, and with extensions expired September 24, 1984. The tapes from these two intercepts were sealed October 13, 1984 — 82 days after the Levittown termination and 20 days after the El Cortijo termination.

The Vega Baja-private order was entered November 1, 1984, and with extensions expired May 30, 1985. The Vega Baja-public order was entered January 18, 1985, and expired February 17, 1985. A second Vega Baja-public order was entered March 1, 1985, and with extensions expired May 30, 1985. Both Vega Baja-public authorizing orders were on the same telephone number. The tapes from these two intercepts (i.e., Vega Baja-private and the two Vega Baja-public) were sealed June 15, 1985 — 118 days after the termination of the first Vega Baja-public order and 16 days after the termination of the second Vega Baja-public order and the Vega Baja-private order. There was, as shown, a 12-day lapse between the termination of the first Vega Baja-public order and the issuing of the second Vega Baja-public order.

The district court suppressed all of the tapes of intercept from the Levittown intercept and from the first Vega Baja-public intercept. The court did not suppress the tapes of intercept from the El Cortijo intercept, from the second Vega Baja-public intercept and from the Vega Baja-private intercept. The Second Circuit affirmed the district court on the government's appeal. From this decision, the government sought review by certiorari to the Supreme Court in the instant case.

97. Ojeda Rios, 495 U.S. at 262-63.
“timeliness is of the essence” in sealing the product of intercepts. Although it may be unnecessarily early, it is not inordinately cautious to seek the sealing of the product of the intercept at the time of the presentation of interim reports to the court, or at least at the time of the presentation of an application/affidavit seeking an extension of the authorizing order.

If the government does not seal the product of the interception immediately, the government must make a satisfactory showing regarding the delay. Such satisfactory showing cannot simply be a recitation of the reason for the delay, in addition to a showing that the product of the interception is, in fact, authentic.

To constitute the showing of a satisfactory reason for delay in sealing the product of an intercept, the government must make a two-fold showing. First, the government must show that the reason for delay was objectively reasonable at the time of the delay. Second, the government must show that the excuse for delay was, in fact, the actual reason for the delay at the time of the delay. The government should raise this actual reason at the time of the suppression hearing, not later.

99. Ojeda Rios, 495 U.S. at 263.
100. The sealing requirement is effective immediately upon the termination of the authorizing order. However, this includes extensions thereof. Part of the issue in Ojeda Rios was the prosecutor’s reliance on two Second Circuit cases which were interpreted to mean that the 12-day gap in time between the expiration of the first Vega Baja-public order for intercept and issuing of the second Vega Baja-public order for intercept did not cause a lapse of the first order; but, rather, the second order was merely an extension of the first order. See supra note 81. The Supreme Court in Ojeda Rios determined that although this was a mistaken interpretation of the law, it was objectively reasonable at the time, and, if this was the actual reason for not sealing the tapes of the intercept (i.e., in this case, if this reason had been argued to the district court in the course of the suppression hearing), this could constitute a satisfactory excuse for not timely sealing the product of the intercept under 18 U.S.C. § 2518(8)(a).

101. 18 U.S.C. § 2518(8)(a); Ojeda Rios, 495 U.S. at 263-64.
102. Ojeda Rios, 495 U.S. at 263-64. This portion of the decision expressly overruled the prior Eighth Circuit decision to the contrary regarding this issue. See Ojeda Rios, 495 U.S. at 265 n.5 (overruling McMillan v. United States, 558 F.2d 877, 878-79 (8th Cir. 1977)).
103. Compare Feiste, 961 F.2d at 1350-51 (8th Cir. 1992) (applying a subjective standard to analyzing the reason for delay) with United States v. Sawyers, 963 F.2d 157, 160-61 (8th Cir.) (applying the “objectively reasonable” standard when analyzing the reason for delaying in sealing), cert. denied, 113 S. Ct. 619 (1992).
104. In Ojeda Rios, the Supreme Court remanded the case for the sole purpose of making a factual determination concerning whether the reason for delay advanced by the Government was the actual reason at the time of the delay in sealing (i.e., was this reason argued at the district court suppression hearing?).
Of course, it is inherent within the statute and *Ojeda Rios* that once the product of the intercept is sealed, it must remain sealed until a court directs its unsealing. Should access to the sealed product of the intercept be needed, a court order for the temporary unsealing of the product of the intercept should be obtained.

CONCLUSION

The use of electronic surveillance is an important tool for the enforcement of criminal laws, especially with regard to conspiracies, other organized criminal activity, or continuing criminal activity. However, because of its intrusive nature, electronic surveillance is strongly regulated by federal statute and court decisions. Although absolute compliance with the requirements of the statute and the order authorizing the use of electronic surveillance may not be required, virtual compliance, especially with portions of the statute directly affecting substantive individual rights, is necessary.

Failure to abide by the requirements of the statute and the supervising court's orders may result in the suppression of key evidence otherwise available against persons aggrieved by inappropriate uses of electronic surveillance. Monitors of aural and oral communications will be held to an objective standard in obtaining and employing electronic surveillance. However, maintaining good faith compliance with the requirements for employing electronic surveillance may, in some circumstances, where evidence might otherwise be suppressed, allow the use of evidence recovered thereby.

Four areas of significant concern in determining compliance with such requirements include: (1) exhaustion of alternative investigative techniques, (2) achievement of the objectives of the use of electronic surveillance, (3) minimization of the use of electronic surveillance, and (4) sealing of the product of the intercept immediately after termination of the electronic surveillance.

---

105. Many states also have adopted electronic surveillance statutes. However, consideration of such statutes and of the relationship between state statutes and federal prosecutions employing the product of a "state electronic surveillance" are topics beyond the scope of this Article.