1979

A Diagnosis, Dissection, and Prognosis of Maryland's New Wiretap and Electronic Surveillance Law

Richard P. Gilbert
Former Judge, Maryland Court of Appeals

Follow this and additional works at: http://scholarworks.law.ubalt.edu/ublr

Part of the Law Commons

Recommended Citation
Available at: http://scholarworks.law.ubalt.edu/ublr/vol8/iss2/2

This Article is brought to you for free and open access by ScholarWorks@University of Baltimore School of Law. It has been accepted for inclusion in University of Baltimore Law Review by an authorized administrator of ScholarWorks@University of Baltimore School of Law. For more information, please contact snolan@ubalt.edu.
A DIAGNOSIS, DISSECTION, AND PROGNOSIS OF MARYLAND'S NEW WIRETAP AND ELECTRONIC SURVEILLANCE LAW

Richard P. Gilbert†

This article examines the Maryland Wiretapping and Electronic Surveillance Act. After comparing the Maryland act with corresponding federal law dealing with the interception of oral communications, the author concludes that the Maryland act guarantees greater protection from surreptitious eavesdropping and wiretapping than that afforded by its federal counterpart.

I. INTRODUCTION

History does not record the first occurrence of eavesdropping,¹ but it may well have been soon after Eve gave birth to Cain and there were thus three persons in existence. Whatever its origin, the odious practice continues today, but man no longer has to rely upon his ear alone. Modern technology has turned persons, rooms, and open areas into radio broadcasting stations by the simple placing of a microphone — or “bug” — therein or by directing a highly sensitive listening apparatus toward the place where the conversation is being held.²

† A.A., J.D., LL.M., University of Baltimore; Chief Judge Court of Special Appeals of Maryland.

The author acknowledges with thanks the aid of Patrick Casey Duncan, Esq., of the Montgomery County Bar and Shelly Mintz, Esq., of the Baltimore City Bar, both of whom served as judicial clerks to the author during the term of Court, September 1977.

1. An examination of the etymology of the term “eavesdropper” inevitably leads to Sir William Blackstone, who, in 4 W. BLACKSTONE, COMMENTARIES (1st ed. 1803) 168, refers to “Eaves-droppers,” as such as listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, [and] are a common nuisance, and presentable at the court-leet, or are indictable at the sessions, and punishable by fine and finding sureties for their good behavior. (footnotes omitted).

2. Developments in electronics and miniaturization allow virtually indetectable snooping to be carried out via such diverse technological wonders as transistors, microcircuits, and lasers. Radio transmitters made out of integrated microcircuits can be constructed on a piece of material smaller and thinner than a postage stamp. The transmitter can be readily concealed in such unobtrusive places as behind wallpaper or in a playing card. See generally E. LONG, THE INTRUDERS 5-20 (1967); Scoular, Wiretapping and Eavesdropping Constitutional Development from Olmstead to Katz, 12 St. Louis U.L.J. 513, 514 (1968). “Nor is an individual even safe in the shower — microphones have been developed which segregate man’s voice from the sound of running water.” Id. at 514 (footnote omitted). See also Kamisar, The Wiretapping-Eavesdropping Problem: A Professor’s View, 44 MINN. L. REV. 891, 892-93 (1960).

Out of the pages of science fiction and into the every-day world emerges the latest in the arsenal of electronic eavesdropping mechanisms — the laser beam. One available portable laser microphone sends out an invisible infra-red beam only a quarter of an inch in thickness. The power of a laser beam
The "wiretap" originated over a hundred years ago when man learned that he could tap into telegraph lines and overhear Morse Code messages being sent from one point to another.\textsuperscript{3} Telegraph taps were used during the Civil War as a means of intercepting military communications\textsuperscript{4} and were later a highly remunerative source of private gain.\textsuperscript{5}

On March 10, 1876, in Boston, Massachusetts, Alexander Graham Bell uttered what are now the historical words, "Mr. Watson, come here. I want you."\textsuperscript{6} Those seven words, the first ever spoken over a telephone, established a series of new industries. One of them is the manufacture of equipment to intercept the electronic impulses that traverse telephone wires — the "wiretap."\textsuperscript{7}

to remain focused over long distances allows it to go for miles from the point of transmission to a target room. There it strikes a two-inch mirrored modulator planted in the room by the investigator, which sends the laser beam back to its original source miles away. Since the returning beam has been modulated by the sound waves produced by speech in the room under surveillance, a photo amplifier at the listening post allows the investigator to transform the returning light into sound. (footnote omitted).


5. Gamblers made a practice of intercepting the news of racetrack results in order to get last-minute bets placed before bookmakers could know which horse had won. Stock-market operators got inside information and market prices in time for some fast finagling on the exchanges. Newspapers pirated each other's exclusive stories before publication. Blackmailers winnowed some remunerative wheat from the chaff of telephonic confidences.


7. By 1895, the government had replaced the individual profiteer as the primary user of newly developed eavesdropping techniques. The "New York police were actively using wiretapping in criminal investigations in 1895. A loose arrangement existed between the New York police and the telephone company whereby the telephone company cooperated with the wiretapping practices of the police department, [and this despite the fact that] there were [only] 339,500 telephones in the country ...." S. Dash, R. Schwartz, & R. Knowlton, The Eavesdroppers 25 (1959) (footnote omitted).
II. ORIGINS OF THE MARYLAND WIERTAPPING AND ELECTRONIC SURVEILLANCE STATUTE

Prior to the 1971 decision of the Court of Special Appeals in State v. Siegel, Maryland had two statutes dealing with the interception of oral communications. Maryland Annotated Code, article 35, sections 92-99 applied to the interception of wire communications, telephonic and telegraphic, while Maryland Annotated Code, article 27, sections 125A-C pertained to electronic devices used in the interception of oral communications.

The provisions of Maryland Annotated Code, article 35, sections 92-99 (interceptions) were discussed in Manger v. State by the Court of Appeals, but were not applied because Manger lacked "standing to object to the introduction against him of evidence seized in the raid made under the authority of the search warrant, on the ground that the warrant was based on evidence forbidden to be introduced by Sec. 105 of the Act, or to be divulged to any person." The court bottomed its decision on the fact that neither of the two tapped phones was listed to Manger and the complainants were not participants in the overheard conversations.

Subsequently, in Robert v. State, the Court of Appeals implicitly sanctioned the validity of the wiretap sections of Maryland Annotated Code, article 35, sections 92-99. Nevertheless, the court overturned convictions for sexual offenses because the police listened via a "headset" to a telephone conversation, and all the participants to the communication had not consented thereto.

Article 27, sections 125A-C (devices) were not construed until the Court of Special Appeals decided Pennington v. State, although they have been peripherally addressed in a series of cases.

11. 214 Md. 71, 133 A.2d 78 (1957).
12. Id. at 77, 133 A.2d at 81.
13. Manger's situation was comparable to that of persons who, for lack of a proprietary interest in particular premises, had no standing to complain of a search and seizure made on those premises. "[O]ne cannot complain of an illegal search and seizure of premises or property which he neither owns, nor leases, nor controls, nor lawfully occupies, nor rightfully possesses, or in which he has no interest." Baum v. State, 163 Md. 153, 157, 161 A. 244, 245 (1932). See also United States v. Jeffers, 342 U.S. 48 (1951).
16. E.g., Hopkins v. State, 19 Md. App. 414, 426, 311 A.2d 483, 490 (1973) (illegal electronic interception of conversations between a state witness and the accused, suppressed by the trial judge, did not taint indictment); State v. Graziano, 17 Md. App. 276, 301 A.2d 36 (1973) (information furnished by informant was insufficient to support order for wiretap); State v. Lee, 16 Md. App. 296, 295 A.2d
Pennington made clear that while it was a misdemeanor to overhear or record, through the use of electronic devices, any conversation without the consent of all the parties to that conversation, the statute did not provide any other sanction, such as exclusion of the evidence.\(^\text{17}\)

With the Court of Special Appeals' opinion in State v. Siegel,\(^\text{18}\) a third statute, the federal electronic wiretap and eavesdrop provisions of the Omnibus Crime Control and Safe Streets Act of 1968,\(^\text{19}\) became an integral part of the criminal law of Maryland. Siegel pronounced that pursuant to 18 United States Code, section 2516(2), if the "principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, . . . is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order"\(^\text{20}\) permitting the electronic interception of wire or oral communications, then the judge to whom the application is made may grant the order in accordance with 18 United States Code, section 2518. Absent a state statute authorizing such an application by the principal attorney, the judge could not issue the order.\(^\text{21}\) Siegel also pointed out that the several states are at liberty to adopt more restrictive provisions than those contained in the federal act. The states, however, may not enact wiretap or electronic interception statutes that are less restrictive than those of the federal act inasmuch as Congress has preempted the field, and the federal statutes prevail over repugnant state statutes.\(^\text{22}\)

On certiorari, the Maryland Court of Appeals, in State v. Siegel,\(^\text{23}\) trod much the same path as that traveled by Judge Charles E. Orth, Jr., in the Court of Special Appeals, except that the state’s highest court declared flatly that "[t]he statute [18 United States Code, sections 2510–2520] sets up a strict procedure that must be followed and we will not abide any deviation, no matter how slight, from the prescribed path."\(^\text{24}\) The Siegel wiretap was therefore

---

812 (1972) (court found that the Federal Wiretapping Act was properly implemented by Md. ANN. CODE art. 27, § 125A, et seq. and art. 35, § 94); Avery v. State, 15 Md. App. 520, 539, 292 A.2d 720, 742, cert. denied, 266 Md. 733, cert. denied, 410 U.S. 977 (1972) (electronic interception and video transmission which was transmitted to the police with the cooperation and consent of the victim of the crime held valid). Cf. Johnson v. State, 2 Md. App. 300, 234 A.2d 464 (1967) (police observations made by means of binoculars held proper to show probable cause for issuance of search warrant).

17. 19 Md. App. at 278, 310 A.2d at 830.
20. Id. at § 2516(2).
22. Id. at 613.
23. 266 Md. 256, 292 A.2d 86 (1972).
24. Id. at 274, 292 A.2d at 95 (emphasis in original).
invalid, as the authorization failed to provide for termination of the
tap as required by the federal statute.

Strict statutory compliance was likewise required in *Calhoun v. State*,25
where the State was precluded from curing a "defective
present affidavit in support of an application for a court order
authorizing an electronic listening device, by incorporating by
reference into the present affidavit a prior valid affidavit used in
another application."26 The court refused to permit a deviation from
the prescribed path of the statute.27

In *Spease v. State*,28 the Court of Special Appeals elected to
follow a line of cases holding that violation of post-intercept orders
would not be grounds to suppress evidence unless the accused could
show prejudice.29 The Court of Appeals, on *certiorari*, affirmed,30 and

 A.2d 103 (1978), cert. denied, ___ Md. ___, A.2d ___ (May 19, 1978)*
 (conviction upheld despite certain minimal departures from the judicial order
 after interception occurred).


27. Emphasizing the attitude toward strict compliance, the court said that
 frequently a police officer, in a reflective mood, will say, "Judge, you
 know this . . . [wiretap law] makes my job a lot tougher and more
difficult." What does one respond, except to say:

"Officer, that's precisely what . . . [it] is for. Even in our service, you
are not permitted the efficiency permitted a counterpart in a Gestapo or
an NKVD. From day to day, that is your burden; but from decade to
decade and century to century, that is your glory. When you look at your
wife and children at home at night, you yourself would not have it
otherwise. Yes, officer, it makes your job a lot more difficult. It's
supposed to."

*Id.* at 377, 367 A.2d at 46 (quoting J. MOYLAN, *THE RIGHT OF THE PEOPLE TO BE
SECURE, AN EXAMINATION OF THE FOURTH AMENDMENT* (1976)).


29. United States v. Wolk, 466 F.2d 1143 (8th Cir. 1972) (failure timely to serve
formal inventories of wiretap interceptions, as required by 18 U.S.C. § 2518(8)(d)
(1976), did not justify suppression of the evidence derived from a wiretap when
the complainants had actual notice of the interception and were not prejudiced);
United States v. Smith, 463 F.2d 710 (10th Cir. 1972) (failure to serve notice or
inventory of wiretap within the required 90 day period, 18 U.S.C. § 2518(8)(d)
(1976), did not justify suppression of evidence); United States v. Ripka, 349 F.
Supp. 539 (E.D. Pa. 1972), aff'd, 480 F.2d 919 (3d Cir. 1973) (failure to provide an
inventory or to specify the period of time during which the interception is
authorized did not constitute grounds for suppression); United States v. Iannelli,
intent did not include voiding an interception *ab initio* because of unauthorized
disclosure after successfully acquiring evidence pursuant to a lawful wiretap
order); United States v. LaGorga, 336 F. Supp. 190 (W.D. Pa. 1971) (where
unlawful interception of some telephone calls pursuant to court order occurs, only
the unlawful interceptions need be suppressed, and evidence obtained by
procedures sanctioned by statute and court order will not be suppressed); United
days beyond the time permitted for filing did not require that wiretap evidence be
suppressed absent an allegation of prejudice). *But see* United States v. Eastman,
failure to serve an inventory vitiated the wiretap and precluded use of evidence
derived therefrom).

30. 275 Md. 88, 338 A.2d 284 (1975). The opinion was written by Chief Judge Robert
C. Murphy. Judge John C. Eldridge dissented on the ground that the police failed
in so doing stated that "[n]othing in our opinion in this case is intended to depart in any way from our holding in Siegel."\textsuperscript{31}

It was not until thirty-four months later, in \textit{Poore v. State},\textsuperscript{32} that the question of pre-order compliance \textit{vis a vis} post-order compliance reached the Court of Special Appeals. The \textit{Poore} court determined that any variance with pre-intercept orders will not be tolerated, and any evidence derived from such illegal acts will be suppressed. On the other hand, substantial compliance with post-intercept orders will suffice if the defendant has not been prejudiced.\textsuperscript{33}

Not long after \textit{Spease}, the Court of Special Appeals, in \textit{Shingleton v. State},\textsuperscript{34} observed that except for two narrow exceptions, specified in the federal act, and even then subject to rigid requirements, applications for wiretap or other electronic interceptions of communications must be made in writing. These two exceptions involve emergency matters relating to national security or organized crime.\textsuperscript{35}

In apparent response to \textit{Siegel}'s implicit invalidation of Maryland's time framework for communication interception\textsuperscript{36} on the

\textsuperscript{31} 275 Md. 88, 108 n.3, 338 A.2d 284, 295 n.3.
\textsuperscript{33} \textit{Id.} at 53, 384 A.2d at 110. \textit{See also} text at notes 136-39 \textit{infra}.
\textsuperscript{34} 39 Md. App. 527, 387 A.2d 1134 (1978).

\begin{enumerate}
\item Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—
\begin{enumerate}
\item an emergency situation exists with respect to conspiratorial activities threatening the national security interest or to conspiratorial activities characteristic of organized crime that requires a wire or oral communication to be intercepted before an order authorizing such interception can with due diligence be obtained, and
\item there are grounds upon which an order could be entered under this chapter to authorize such interception,
\end{enumerate}
\end{enumerate}

may intercept such wire or oral communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

\textsuperscript{36} \textbf{MD. ANN. CODE} art. 35, § 94(f) (1957). \textit{Siegel} did not expressly declare the section to be unconstitutional, but in light of the court's language that "under no
ground that it was less restrictive than its federal counterpart and hence illegal, the 1973 Maryland General Assembly passed and sent to Governor Marvin Mandel, House Bill No. 962. That bill sought to repeal Maryland Annotated Code, article 35, sections 92–99 and reenact them in such a way as to avoid federal constitutional pitfalls. With characteristic paternal benevolence, Governor Mandel vetoed House Bill No. 962, however, and in his message to the Speaker of the House of Delegates noted,

I cannot believe that the Legislature fully realized the scope of the provisions, or that Congress realized their scope when enacting the federal law. In any event, I will not be a party to making such unlicensed intrusions on private communications a matter of State policy.

circumstances is [a state] law enforceable if it is less restrictive than the federal statute...” 266 Md. at 271, 292 A.2d at 94, it is clear that § 94(f) was unconstitutional. This is so because the federal act provides that an order allowing “interception of any wire or oral communication” shall not be “for any period longer than necessary, nor in any event longer than thirty days.” 18 U.S.C. § 2518(5) (1976). Extensions of the order, however, may be granted upon certain specified conditions. Id. The Maryland statute, article 35, § 94(f), limited the order to a period of not “longer than thirty (30) days,” after which it could be renewed upon application, and subject to the discretion of the court, “for an additional period not to exceed thirty (30) days.” The Maryland statute failed to embody the “no longer than is necessary to achieve the objective of the authorization” limitation, embodied in 18 U.S.C. § 2518(5) (1976), upon the police. Thus, if the interceptors accomplished their mission on the first day of the order, they could continue to intercept oral or wire communication for such additional time as the order was viable, so as to “gild the lily.”

37. House Bill No. 962 was introduced as

AN ACT to repeal Sections 125A through 125D of Article 27 of the Annotated Code of Maryland (1971 Replacement Volume), titled and subtitle “Crimes and Punishments,” [subtitle] subheading “Electronic Devices”; to repeal Section 585 of Article 27 of the Annotated Code of Maryland (1971 Replacement Volume), title and subtitle “Crimes and Punishments,” [subtitle] subheading “Wire Tapping”; and to repeal Sections 92 through 99 of Article 35 of the Annotated Code of Maryland (1971 Replacement Volume), title “Evidence,” subtitle “Wire Tapping,” and to enact in lieu thereof new Sections 92 through [[99]] 99A, to be under the new subtitle “Wire Interception and Interception of Oral Communications,” to define the terms used in the new subtitle, to prohibit the unauthorized interception of wire and oral communications and to prohibit their use as evidence, to authorize the Attorney General in certain cases and the State’s Attorneys to seek judicial authority for appropriate law enforcement officials to intercept wire or oral communications which may provide evidence of certain crimes, to set forth the procedures to be followed for obtaining authorization to lawfully intercept wire or oral communications, to set forth the circumstances under which intercepted communications can be disclosed or used, to require reports concerning intercepted wire and oral communications and to provide for recovery of civil damages for persons whose wire or oral communication has been unlawfully intercepted and to provide for the registration of certain devices by certain persons.

39. The speaker at that time was the Honorable Thomas Hunter Lowe, presently an associate judge of the Court of Special Appeals.
When Senate Bill No. 1 was introduced at the 1973 First Special Session of the Maryland General Assembly, the Code Revision Commission drafted what became Maryland Courts and Judicial Proceedings Code Annotated, section 10-403(f) and (g) to reflect the Siegel holding. The Senate Judicial Proceedings Committee and the House Judiciary Committee regarded the Commission's attempt to satisfy the requirements of Siegel as no more than a "band-aid" approach. Maryland Annotated Code, article 35, section 94(f) was added by amendment to Maryland Courts and Judicial Proceedings Code Annotated, section 10-403 as subsection (f), and in substantially the same language that Siegel implicitly found wanting.

Three years after the rejection of the "band-aid" approach to solving the Siegel problem, and in the interim allowing unchecked "bleeding" by bench and bar, a "tourniquet" was applied in the form of a comprehensive "Wiretapping and Electronic Surveillance" law, which was enacted and codified as Maryland Courts and Judicial Proceedings Code Annotated, sections 10-401 through 10-412.

44. Law of May 26, 1977, ch. 692, § 3, 1977 Md. Laws 2798, 2805. The avowed purpose of the act was stated as follows:

AN ACT concerning
Wiretapping and Electronic Surveillance

FOR the purpose of repealing existing provisions of law relating to wiretapping and electronic surveillance and enacting new provisions relating to the same matters; defining various terms; prohibiting, with certain exceptions, the interception and disclosure of oral and wire communications and prescribing a criminal penalty; prohibiting, with certain exceptions, the manufacture, possession and sale of devices for surreptitiously intercepting oral and wire communications, and providing for the forfeiture of such devices; prohibiting, in certain circumstances, the use of intercepted communications in various proceedings; providing for the interception, under certain circumstances and with prior judicial authorization, of oral and wire communications by law-enforcement personnel; providing for the protection, disclosure, and suppression of such communications; requiring certain reports relating to the interception of such communications; creating certain civil liabilities and criminal offenses; requiring law-enforcement agencies to register devices for the interception of oral and wire communications; and generally relating to the interception of oral and wire communications.

BY repealing

Article 27 — Crimes and Punishments
Section 125A through 125D and the subheading "Electronic Devices"
the date of this writing, no reported opinion of the Court of Appeals or the Court of Special Appeals has directly construed the current Maryland act.

Having mapped out the historical background for Maryland's current wiretap and electronic surveillance law, we shall now tread our way through that labyrinthine legislation.

III. DIAGNOSIS, DISSECTION, AND PROGNOSTICATION

An examination of the Maryland act regulating electronic interception of oral or wire communications discloses many similarities to the federal statute. Indeed, it is unmistakable that the federal law served as the guiding light for the Maryland act. 45 Where

and 585
Annotated Code of Maryland
(1976 Replacement Volume and 1976 Supplement)

BY repealing
Article — Courts and Judicial Proceedings
Section 10-401 through 10-408
Annotated Code of Maryland

BY adding to
Article — Courts and Judicial Proceedings
Section 10-401 through 10-412
Annotated Code of Maryland

Senate Bill No. 175, enacted as Law of May 26, 1977, ch. 692, 1977 Md. Laws 2798, was introduced by the chairman of the committee on constitutional and public law, Senator Edward T. Conroy from Prince George's County, Maryland.

the state legislation is identical to that of the Congress or relatively minor stylistic changes have been made so as to narrow the effect of the law to the geographical confines of Maryland, this discussion shall do no more than note that fact and then proceed to what the author perceives to be significant substantive departures from the federal act.

Section 10-401: Definitions

Subsections (1), (3), (4), (5), (6), (7), and (10) are, except for minor stylistic modifications, and the narrowing of their scope to Maryland, the same as their federal models.46

Subsection (2) of the federal act defines an oral communication as one "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation . . . ."47 Maryland's section 10-401(2) is considerably more inclusive; it defines "oral communication" to mean "any conversation or words spoken to or by any person in private conversation . . . ." While there have not, as yet, been any appellate court decisions interpreting section 10-401(2), it is relatively safe to speculate that inasmuch as the Maryland definition includes a broader class of communications than that employed by the Congress, it will pass constitutional muster.

Subsection (8) of section 10-401 defines the phrase "Judge of competent jurisdiction" as "a judge of a circuit court or the Supreme Bench of Baltimore City," which may be translated to mean a trial judge of the circuit court, the second level of the Maryland four-tier judicial system.48 Maryland District Court judges and the judges of the appellate courts are without jurisdiction to authorize electronic interceptions.

The Maryland act has no provision corresponding to subsection (3) of section 2510. The reason for the absence is that the federal act defines "State" in subsection (3). Inasmuch as the Maryland statute is confined to the State of Maryland and does not involve any extra-territorial enforcement or uses, the drafters of the Maryland law properly deemed it unnecessary to include a definition of what is meant by the noun, "State."

Subsection (9) of section 10-401 of the Maryland statute narrows the definition of "communications common carrier" as that term is

46. 18 U.S.C. §§ 2510(1), (4), (5), (6), (7), (8), and (11) (1976) respectively.
47. Id. § 2510(2) (1976).
48. The Maryland judicial system consists of the Court of Appeals, the highest court of the State, the Court of Special Appeals, an intermediate court of appeal, the circuit courts, the highest common law and equity courts of record exercising original jurisdiction within the State, and the district court, a court of record with limited jurisdiction. See Md. CTS. & JUD. PROC. CODE ANN. §§ 1-301, 1-401, 1-501, and 1-601 (1973).
defined in section 2510(10) of the federal act. The federal statute uses the definition of "common carrier" found in 47 United States Code, section 153(h), while Maryland limits the definition to include only "telegraph company," "telephone company," and "radio common carrier" as defined in Maryland Annotated Code article 78, sections 2(x), 2(z), and 2(ii), respectively.

Section 10-402: Interception of [Oral or Wire] Communications Generally

Both section 10-402 of the state law and section 2511 of 18 United States Code proscribe the willful endeavor to intercept or to procure any other person to intercept or endeavor to intercept a wire or oral communication. Furthermore, each imposes a penalty of imprisonment of "not more than five years" or a "fine of not more than $10,000." Both the federal and state statutes apparently prohibit the use of the interception for any purpose by any person who knows or has reason to know that the interception was obtained in violation of the respective statutory enactments.

Both acts, however, exempt from their purview switchboard operators or employees or agents of any communication common carrier who intercept wire communications in the course of their normal duties incident to the service provided by the common carrier or for the protection of the "rights or property of the carrier." The state statute carves out a further exception for which there is no federal counterpart. Subsection (c)(ii) of section 10-402 provides that it is permissible for the carrier's employee to provide information, facilities, or technical assistance to an investigative or law enforcement officer who is authorized by the statute, either directly or by order of a judge of a court of competent jurisdiction, to intercept a wire or oral communication. Subsection (c)(ii) appears to permit local police to gain technical aid from the communication common carrier's personnel. Whether that feature of the state act will be construed as being less restrictive than the federal law remains to be determined, but on the surface the subsection does no more than recognize that which is implicit in the federal act. Certainly, federal agents must of necessity, from time to time, obtain information from a common carrier and its employees, as well as occasionally utilize the carrier's facilities and rely on the technical knowledge of the carrier's personnel.

One significant feature that distinguishes the federal law from that of Maryland is that under the former a party to an oral or wire communication may give prior consent to a law-enforcement official to intercept or record the communication without the consent or knowledge of the other party or parties to the communication. In such a case, no judicially authorized interception order is required. The federal statute imposes no limitation on that procedure with respect to the nature of the crime. Furthermore, subsection (d) of section 2511 allows one of the parties to a conversation to record it, or to permit another, not a police or investigative officer, to do so without the knowledge or consent of the other party or parties to the communication, provided the interception is not for the purpose of “committing any criminal or tortious act in violation of” constitutional, federal or state law. While the Maryland act does authorize a law-enforcement officer to intercept oral or wire communication on the strength of the “prior consent” of one of the parties to the communication, it limits its use to the crimes of “murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in controlled dangerous substances.” Of singular importance, oral or wire communications concerning crimes other than those specified may not be intercepted unless all the parties to the communication have given their prior consent, and only then if the interception is not to be used for the purpose of committing a violation of the Constitution or laws of the United States or Maryland or for any other injurious act. Of course, if the interceptor is armed with a judicially issued interception order, made in accordance with the provisions of the state act, a subject discussed in greater detail below, the prohibition established by subsection (c)(2) does not apply.

53. Id.
54. Md. Cts. & Jud. Proc. Code Ann. § 10–402(c)(2) (Supp. 1977). The General Assembly, by enacting House Bill 475 as Law of May 2, 1978, ch. 339, 1978 Md. Laws 1424, effective July 1, 1978, added “any felony punishable under the ‘Arson and Burning’ subheading of Article 27” to the offenses for which the interception of wire or oral communication is permissible under section 10-402(c)(2). By failing to enact House Bill 701, the 1978 legislature refused also to permit the interception of wire or oral communication evidence of “receiving stolen goods” and “larceny.” The Court of Special Appeals, in Reed v. State, 35 Md. App. 472, 372 A.2d 243 (1977), upheld the recordation of tapes of telephone conversations made by Reed to his rape victim. The offense in that case occurred prior to the effective date of the current Maryland statute so that the federal act was applicable thereto. The court noted that while Md. Ann. Code art. 27, § 125A proscribed the ex parte recording of communications the statute did not prohibit the admission of such recording into evidence, but merely imposed a criminal sanction therefor if the state’s attorney for Montgomery County elected to pursue that avenue, a highly dubious possibility.
Section 10-403: Manufacture, Possession or Sale of Intercepting Device

This section makes unlawful the manufacturing, assembling, possessing, or selling of "any electronic, mechanical, or other device" if the manufacturer, assembler, possessor, or seller knows or should know that the device is primarily useful in the surreptitious interception of either wire or oral communications. Anyone convicted of violating this provision of the statute is subject to the same penalty as that prescribed for illegal eavesdropping or wiretapping of oral or mechanical communication.57

The application of section 10-403 is markedly different in many respects from that of 18 United States Code, section 2512. Expressly deleted from the state statute are law-enforcement officers of the federal government,58 and state law-enforcement officers who manufacture, assemble, possess, or sell such a device under the specific authorization of the chief administrator of that particular law-enforcement agency of which the assembler or manufacturer or possessor is an employee.59 Any sale of the device by a federal agent or a state employee "may only be for the purpose of disposing of obsolete or surplus devices."60 A similar restriction on the sale of the interception device by law-enforcement officers is not contained in the federal act. It should be noted that the state wiretapping and electronic surveillance law makes no attempt to establish a procedure for the determining of obsolescence or surplusage, nor does it designate the person or persons who are required to make that vital decision. It can be inferred from the general tenor of section 10-403 that the "sale," when made on the grounds of obsolescence or surplusage will find a very limited market in light of the prohibition against possession of interception devices enumerated in section 10-403(a). Furthermore, expressly exempted from the breadth of the state act are those persons61 who are under contract with the federal government, or the government of any state or political subdivision thereof, or the District of Columbia to manufacture, assemble, possess, or sell electronic or other interception devices for the use and benefit of the government so

59. Id. § 10-403(b)(4).
60. Id. § 10-403(b)(3)(4).
61. Id. § 10-401(5) defines "Person" as "any employee or agent of this State or a political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation. . . ."
contracting with them. Both the federal act, 18 United States Code, section 2512(2)(a) and the state statute, Maryland Courts and Judicial Proceedings Code Annotated, section 10-403(b)(1) exclude a communications common carrier, and a person under a contract with a carrier, from the interdiction of the respective statutes.

Section 10-404: Forfeiture of Device

The state law commands that any electronic or other device used, possessed, assembled, manufactured, or sold in violation of section 10-402 or section 10-403 be seized and forfeited to the Department of Public Safety and Correctional Services of Maryland. Section 2513 of the federal statute authorizes forfeiture of the device to the United States, but directs that the forfeiture shall be governed by "the customs laws contained in title 19 of the United States Code."63

Section 10-405: Admissibility of Evidence

This section forbids the receipt into evidence of any information before "any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of this State, or a political subdivision [of Maryland] if the disclosure of that information would be in violation" of the act.64

The Court of Appeals, in Carter v. State,65 said that evidence obtained as the result of an illegal search or seizure of property must not only be excluded at trial, but also "cannot be used, because of its taint, as a valid basis to justify the existence of probable cause in a subsequent search and seizure warrant."66 Judge O'Donnell, writing for a unanimous court, then said,

Thus, if any conversation of Carter or any conversation overheard upon his premises — whether he was present and participating in it or not — was subjected to a "search and seizure" by the use of any wire tap or eavesdropping device, in violation of his rights under the Fourth Amendment . . . any information garnered as "fruits" of such primary

62. Id. § 10-403(b)(2). Apparently it is unlawful for any manufacturer, assembler, possessor or seller of electronic or other types of interception devices to contract with the local governments of United States possessions such as Puerto Rico, Guam, and the Virgin Islands, et alia. Seemingly, if one of those governments wanted to contract with a Maryland manufacturer, assembler, possessor or seller of interception devices, it would have to do so through the federal government.
66. Id. at 438, 337 A.2d at 431.
illegality and "come upon" by the "exploitation" of that illegality cannot, . . . be used as derivative evidence for an application for a search and seizure warrant; to hold otherwise would permit the prosecution to use knowledge acquired in violation of the Fourth Amendment and "gained by its own wrong." 67

Prior to the Carter case, the Court of Special Appeals reached a similar conclusion in Washburn v. State. 68 Washburn contended in the appellate court that he should have been afforded a hearing before trial at which time he might have been able to produce evidence demonstrating that the police ascertained the identity of an informant as the direct result of an illegal wiretap. Washburn asserted that if the wiretap was illegal, then the knowledge the police obtained as to the informant's identity was "the product of illegally intercepted evidence." 69

Although the Court of Special Appeals found that the "original taint" was "so diluted" by attenuation "as to make it virtually non-existent,"70 the court discussed the prosecution's burden in overcoming the taint of illegally seized evidence:

Once it is shown that the identity of a State witness was discovered through an illegal wiretap, that witness's information — whether by way of testimony at trial or as support for a finding of probable cause — must be excluded unless the State can establish: (1) that the identity of the witness originated from an independent source, or (2) that the taint, resulting from the witness's identity being discovered as a result of an originally unlawful wiretap, has become so attenuated that there is no rational basis to exclude the evidence obtained from the witness. . . . We decline to adopt a rule which would, ipso facto, exclude all testimony of a witness identified as a consequence of an illegal search. 71

Carter and Washburn were decided under section 2515 of the federal statute, but they would clearly be applicable to section 10-405 of the Maryland act because the wording of the two statutory sections upon which the cases are grounded is identical except for minor stylistic differences.

67. Id. at 438-39, 337 A.2d at 431 (citations omitted).
69. Id. at 201, 310 A.2d at 184.
70. Id. at 202, 310 A.2d at 185.
71. Id. at 201-02, 310 A.2d at 184-85. See also Carter v. State, 274 Md. 411, 437-38, 337 A.2d 415, 430-31. (citations and footnote omitted).
Section 10-406: Attorney General or State's Attorney May Apply for Order Authorizing Interceptions

This section provides that,

the Attorney General or any State's attorney may apply to a judge of competent jurisdiction, and the judge, in accordance with the provisions of . . . this article, may grant an order authorizing the interception of wire or oral communications by investigative or law enforcement officers when the interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or dealing in controlled dangerous substances, or any conspiracy to commit any of the foregoing offenses. No application or order shall be required if the interception is lawful under the provisions of §10-402(c) of this subtitle.72

The state act substantially modifies 18 U.S.C. section 2516. The Maryland law not only prohibits the delegation of authority to apply for wiretap authorizations by the Attorney General to "any Assistant Attorney General specifically designated by the Attorney General," as permitted under the federal act,73 but also the offenses in which the interception may be used are severely curtailed in number to fourteen, counting conspiracy to commit any of the specified seven offenses set out in section 10-406, above, as compared with the plethora of crimes in which interception has been authorized by the Congress.74

74. The Attorney General or his specifically designated Assistant Attorney General may authorize an application to a federal judge of a court of competent jurisdiction for an order authorizing or approving the interception of wire or oral communications in the following instances, "when such interception may provide or has provided evidence of:

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), or chapter 102 (relating to riots);
(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;
(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1084 (transmission of wagering information), section 1503 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law
The Supreme Court, in *United States v. Giordano*,\(^75\) interpreted the phrase in section 2516(1), "The Attorney General, or any Assistant Attorney General specifically designated by the Attorney General, may authorize an application to a Federal judge . . ." to mean precisely what the words state. Consequently, the approval of an application for an interception order by the "Executive Assistant to the Attorney General" did not satisfy the statutory requirement irrespective of the Executive Assistant's "knowledge of the Attorney General's actions on previous cases."\(^76\) The result of the Court's holding in *Giordano* was that a wiretap order of the United States District Court for the District of Maryland was invalidated and the evidence derived therefrom was suppressed.

The Court of Special Appeals, in *Poore v. State*,\(^77\) interpreted section 2516(2)\(^78\) as follows:

Section 2516(2) speaks of "[t]he principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision. . . ." The language of that section does not confer upon the principal prosecuting attorney any power to delegate to an assistant the authority to apply for an electronic interception. The Congress would

---

enforcement), section 1751 (Presidential assassinations, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), sections 2314 and 2315 (interstate transportation of stolen property), section 1963 (violations with respect to racketeer influenced and corrupt organizations) or section 351 (violations with respect to congressional assassination, kidnapping, and assault);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving bankruptcy fraud or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title; or

(g) any conspiracy to commit any of the foregoing offenses.


76. Id. at 510.


78. 18 U.S.C. § 2516(2) (1976) provides in pertinent part:

The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire or oral communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute. . . .
not have so carefully limited the power of the Attorney General of the United States to delegate to a specifically designated assistant the authority to seek orders to intercept oral or telephonic communications and at the same time bestowed upon the principal prosecutor of any State, city or county in the nation an unbridled license to clothe any or all of his or her assistants with permission to seek such orders. It is inconceivable that the country's highest legal officer would be so shackled while the principal prosecutor of the least populated county in the United States was free to permit any designee to apply for an interception order. We think the intent of the Congress to be that the authority devolved upon the principal prosecutor of the State or of the political subdivision, is personal to him, and may not be delegated. "[T]he authority to apply for court orders is to be narrowly confined . . . to those responsive to the political process, a category to which the . . . [Assistant State's Attorney] obviously does not belong. . . ."

We are supported in our holding by an examination of former Md. Cts. & Jud. Proc. Code Ann. § 10-403 (1974) and former Md. Ann. Code art. 27, § 125A-D, which were in effect at all times during the surveillance, indictment, and trial of this case, as well as the current Md. Cts. & Jud. Code Ann. § 10-406 (Supp. 1977). All speak of "The Attorney General or a state's attorney" as being the person to apply for "an order authorizing the interception of wire or oral communications. . . ." Id. Nowhere in any of the former statutes or the present statute is there so much as a hint that the Attorney General or the State's Attorney may delegate the authority to apply for interception orders. The statutes, both past and present, empower only the Attorney General or the State's Attorney to seek such orders. It is a power entrusted solely to them as they are the ones answerable through the political process to the electorate.79

The court has thus passed upon section 10-406 of the current state electronic surveillance and wiretap law, and the message is crystal clear: the authority to apply for an order to intercept by electronic device or otherwise is personal, by virtue of the office he or she holds, to the Attorney General of the state and to the State's Attorney of the City of Baltimore or one of the twenty-three counties. It may not be delegated by the Attorney General or by any State's Attorney to another person irrespective of any specific designation.80

80. "The Attorney General of Maryland, the City of Baltimore State's Attorney, and all county State's Attorneys are answerable directly to the electorate. An assistant to any of them is not so answerable." Id. at 57 n.10, 384 A.2d at 112 n.10.
Section 10-407: Lawful Disclosure or Use of Contents of Communication

This section of the Maryland act is almost identical to 18 United States Code, section 2517. Both statutes permit a police officer to relay information to another law-enforcement officer "to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure."81 Any law-enforcement officer who has obtained knowledge of the contents of a wire or oral communication or evidence derived therefrom, may use it to the extent it is appropriate to the proper performance of his duty, but only if the knowledge has been acquired "by any means authorized" by statute.82 Hence, if officer "A" has illegally intercepted an oral or wire communication, he may not pass it on to officer "B," for "B's" use in further investigation, apprehension or prosecution. The taint attached to officer "A's" acquisition of the content of the communication is not eradicated by being once, or twice removed from the source of that taint. Nevertheless, if either officer "A" or "B" were able to demonstrate that he, separate and apart from the primary taint, had discovered evidence from an independent source or that the original taint "has become so attenuated that there is no rational basis to exclude the evidence,"83 then the evidence would be admissible. In this connection it is well to consider the advice of one legal scholar:

The critical question when dealing with attenuation should be whether the admissibility of the challenged evidence will create an incentive for illicit police activity in the future. The attenuation doctrine can play an important role in the application of a derivative evidence rule. Experienced trial judges must carefully scrutinize sophisticated arguments which attempt to make the illegal link in the chain appear weak when, in fact, the entire chain depends on and encourages illicit police activity.84

A law-enforcement officer may disclose the information he has lawfully obtained as a result of an authorized interception in "any

---

84. R. Pitler, "The Fruit of the Poisonous Tree" Revisited and Shepardized, 56 Calif. L. Rev. 579, 646 (1968); See also Comment, Fruit of the Poisonous Tree — A Plea for Relevant Criteria, 115 U. Pa. L. Rev. 1136 (1967).
proceeding held under the authority of the United States or of [Maryland] or any political subdivision thereof.”

The original federal act allowed the disclosure in “any criminal proceeding” only, but the act was amended so as to delete the requirement that the testimony or evidence be given only in “criminal” proceedings.

If the Maryland and federal statutes mean what they seem to say, there appears to be no barrier to the disclosure. The intercepting officer apparently may testify as to the content of a wire or oral communication at any civil proceeding authorized by state or federal law.

Interesting hypothetical situations that cast some doubt upon the wisdom of the use of the term “any proceeding,” vis a vis, “any criminal proceeding,” provide food for thought. Maryland Courts and Judicial Proceedings Code Annotated section 10-408(g) mandates that “[i]mmediately upon the expiration of the period of the order,” the tapes of the contents of wire or oral communications that have been intercepted shall be “made available” to the issuing judge and “sealed under his directions.” Custody of the tapes “shall be wherever the judge orders” provided that the terms of the order have been fully met and that there is no defect in the application, including probable cause. Assume, for example, that the State’s Attorney finds no basis to prosecute, but that the tapes reveal that the suspect’s wife is engaged in an affair with a lover. The suspect-husband independently discovers his wife’s infidelity and sues for a divorce. While the tapes of the communications were sealed and not usable in the divorce case, the officer’s lips are not so sealed. The plaintiff learns of the interception as a result of the notice requirement of section 10-408(g)(4). The divorce case is unquestionably a “proceeding held under the authority of . . . this State . . . .”

May the officer who has conducted the interception testify in the divorce case that he heard, during his electronic surveillance, the plaintiff’s wife acknowledge her prior adultery with her paramour, and agree to further assignations with him?

Suppose that on proper application an order was issued permitting, within the ambit of the statute, a wiretap on the telephone at “The Bucket of Blood,” a bar and grill with a propensity for trouble, and a reputation as the “front” for a gambling ring. The

88. It is to be observed that the legislative history to 18 U.S.C. § 2517(3) (1976) reveals that the amendment was designed “to permit evidence obtained through the interception of wire or oral communications under court order to be employed in civil actions.” 1970 U.S. Code Cong. & Ad. News 4007, 4036.
wiretap conducted for thirty days discloses no violations of the
criminal laws of this state, but does indicate that the licensees of the
bar are violating one or more rules of the Board of Liquor License
Commissioners. The tapes of the intercepted communications are
sealed by order of the issuing judge and placed, pursuant to the same
order, in proper custody. The state's attorney, after reviewing a
transcript of the tapes, decides that there is simply nothing to
prosecute, and that he has been on a wild goose chase. After the
licensees, the targets of the interception order, are notified of the
interception pursuant to section 10-408(g)(4), they complain vigour­
ously, but ignorantly, to the liquor board. Sensing it has found a way
to rid itself of a troublesome licensee, the board ascertains the name
of the officer who conducted the physical interception. The officer is
summoned to appear and testify before the board and answer any
questions put to him, not concerning crimes, but about liquor board
rule violations. The proceeding before the board is civil in nature.
May the officer testify?

It is possible that if either of these two or other similar situations
reach the appellate courts they may decide that inasmuch as the
entire act is directed toward the detection, apprehension, and
conviction of violators of certain criminal laws, that implicit in the
term "any proceeding" as employed in section 10-407(c) is the word
"criminal." Such a ruling would narrow the existing broad language
of the section. Of course, the legislature has within its power the
authority to amend section 10-407(c) and thus possibly thwart
judicial interpretation.

Section 10-407(d) tracks the federal act, section 2517(4), with
respect to assuring that an otherwise privileged communication does
not "lose its privileged character" because it is intercepted in
accordance with or in violation of the act. Stripped of legalese, the
sections provide that simply because a privileged conversation is
overheard, legally or illegally, the conversation does not lose its
privileged status and permit the party to whom the communication
was addressed to treat it as published and thus no longer privileged.
By way of illustration, if "C," client, telephones "A," his attorney,
and communicates to his attorney privileged matters, the fact that
"A" later ascertains that the conversation was intercepted by the
police who had lawfully or unlawfully tapped "C's" telephone does
not remove the privileged character of "C's" conversation with "A."
"A" must still treat the communication as privileged.

Section 10-408: Ex Parte Order Authorizing Interception

Unquestionably, section 10-408 and its federal cousin, section
2518, by virtue of their nature as "the meat" of the acts, have
received the greatest amount of judicial attention.
The legislature has carefully set out a procedure that must be followed by the attorney general or the state's attorney of the City of Baltimore or of one of the twenty-three counties [91] in order to obtain a valid order allowing interception of an oral or wire communication. The application for an electronic or other device to intercept an oral or wire communication must be in writing [92] and be made on oath or affirmation to a judge of the Supreme Bench of Baltimore City or of the circuit court of the county wherein the order is to be executed. The application must inform the issuing judge of the identity of the law-enforcement officer who is making the application as well as that of the officer who has authorized the application. It must set forth a "full and complete statement of the facts and circumstances" [93] upon which the applicant justifies his belief that an order should be issued by the judge. The statement must be more than a mere conclusory summary by the applicant. The statute necessitates that it contain details of the offense that "has been, is being, or is about to be committed," [94] a description of the type and location from which the interception will be made or the place where the communication will be intercepted, [95] "particular description of the type of communications sought to be intercepted," [96] and the identity, if known, of the person "committing the offense and whose communications are to be intercepted." [97]

Although the Maryland appellate courts have not yet passed upon the question of whether, under Maryland law, the person who is identified in the application must play a central role in the crime or suspected crime leading to the application, the Supreme Court has said that there is no such requirement in the federal act. Identification does not impose a limitation on the use of intercept procedures. [98]

---

91. See text accompanying notes 72–80 supra.
92. 18 U.S.C. § 2518(1) (1976); Md. CTS. & JUD. PROC. CODE ANN. § 10-408(a) (Supp. 1977). The Court of Special Appeals, in Shingleton v. State, 39 Md. App. 527, 387 A.2d 1134 (1978), chided an issuing judge who orally authorized an interception to be made on a public pay telephone, based on an oral application from a state police officer. The Court took the occasion to exclaim:

"We look with much disfavor upon the procedure used in the instant case, both as to the application for the order and the authorization of the interception. We note that had the application and order been made subsequent to July 1, 1977, there would not be the slightest argumental justification for the issuance of such an order because the Maryland law [section 10–408] does not recognize the "emergency situation" exception specified in 18 U.S.C. § 2518(7)."

39 Md. App. 527, 537, 387 A.2d 1134, 1140 (1978). Section 2518(7) permits oral application under certain conditions and subject to strict post-order compliance in cases of the national security and organized crime. No provision, for obvious reasons, similar to section 2518(7) is incorporated in the Maryland statute.

93. Id. § 10–408(a)(2)(i).
94. Id. § 10–408(a)(2)(ii).
95. Id. § 10–408(a)(2)(iii).
96. Id. § 10–408(a)(2)(iv).
Because the Maryland act follows so closely the federal statute, the possibility is strong that if the courts of Maryland are confronted with the issue, the result will be the same as that reached by the Supreme Court.

Of critical importance in Maryland, but not regarded as stringently by some of the United States Courts of Appeal is the adherence to the statutory mandate that the application for the order demonstrate:

1) whether other investigative procedures have been tried and failed; or
2) why they appear to the applicant to be not likely to succeed if tried; or
3) why it is too dangerous to undertake them.

The Fifth Circuit in *United States v. Cacae*, the Second Circuit in *United States v. Steinberg*, the Third Circuit in *United States v. Armocida*, and the First Circuit in *In re Dunn* have all adopted what is styled as a practical and common sense approach in evaluating affidavits in support of applications for interception orders. The seeds of that approach were planted in the legislative history of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which states:

Subparagraph (c) requires a full and complete statement as to whether or not normal investigative procedures have been tried and failed or why these are unlikely to succeed if tried, or to be too dangerous. . . . 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. Merely because a normal investigative

---


102. 525 F.2d 1126 (2d Cir. 1975), cert. denied, 425 U.S. 971 (1976).
104. 507 F.2d 195 (1st Cir. 1974).
The factual situation in Dunn is wanting in clarity. One may glean from it, however, that the contents of the affidavit indicated that the "target" of the investigation was suspicious of strangers. Physical surveillance would be difficult at best because of its possible detection and was, therefore, potentially dangerous to the undercover agent. The nature of loan sharking deterred normal investigative methods. The court held that there was sufficient compliance with section 2518(1)(c), the federal relative of section 10-408(a)(3), when the section was read in a "practical and commonsense fashion."  

The Steinberg affidavit contained the following: "I allege the facts contained in the numbered paragraphs to show that: . . . (c) Normal investigative procedures reasonably appear unlikely to succeed, or are too dangerous to be used . . . ." The application described the progress made in the agent's investigation, deliveries of drugs, representations of the suspect, the lack of undercover access to the suspect, as well as the unlikelihood of gaining access to the suspect, and the affiant's experience and knowledge. The Steinberg court held that the affidavit substantially complied with section 2518(1)(c) and (3)(c).

In Armocida the court found substantial compliance based on a factual predicate within the confines of the affidavit which the court noted included: (1) a history of a physical surveillance; (2) use of informants; and (3) undercover agents, as well as (4) other wiretap interceptions. None of those techniques was successful. The affidavit also indicated that (1) the informant would not testify; (2) physical surveillance was too easily detected and could jeopardize further investigation; and (3) a search warrant would, in all probability, not reveal the identities of those involved in the conspiracy or of the source of heroin.

The Supreme Court, in United States v. Giordano, said:

106. 507 F.2d at 197.
107. 525 F.2d at 1130 n.3.
108. Id. at 1130.
Congress legislated in considerable detail in providing for applications and orders authorizing wiretapping and evinced the clear intent to make doubly sure that the statutory authority be used with restraint and only where the circumstances warrant the surreptitious interception of wire and oral communications. These procedures were not to be routinely employed as the initial step in criminal investigation. Rather, the applicant must state and the court must find that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.\textsuperscript{111}

The Court of Special Appeals, in \textit{Calhoun v. State}, stated that,

\begin{quote}
[c]ourts are not free to infer from the mere presentation of an application or petition, supported by an affidavit, that normal investigative procedure will not work. There must be specific compliance with 18 U.S.C. § 2518. The affidavit must demonstrate to the issuing judge that normal investigative measures have been tried and failed, or they are unlikely to be successful under the circumstances, or that their use is too perilous to the investigators. That a prior affidavit for another time and another place so demonstrates, even when incorporated by reference, is not compliance with the strict requirements of the Act.\textsuperscript{112}
\end{quote}

The conclusion is easily reached that irrespective of the "substantial compliance" view held by some courts, Maryland insists upon strict compliance, and will, in the words of Judge Digges in \textit{Siegel}, "not abide any deviation, no matter how slight, from the prescribed path,"\textsuperscript{113} for pre-intercept application requirements.

Section 10-408(a)(4) directs that the application contain a "statement of the period of time for which the interception is required to be maintained." If the investigation is of such a nature that it "should not automatically terminate" when the type of communication sought is first obtained, a particular description of "facts establishing probable cause to believe that additional communications of the same type will occur thereafter"\textsuperscript{114} is also required.

Section 10-408(a)(5) commands the revelation to the issuing judge of any and all previous applications for interceptions known to the applicant that concern the person or persons whose

\begin{footnotes}
\textsuperscript{111} \textit{Id.} at 515 (citations omitted) (emphasis added).
\textsuperscript{112} 34 Md. App. at 376-77, 367 A.2d at 46 (emphasis in original).
\textsuperscript{113} 266 Md. at 274, 292 A.2d at 95.
\textsuperscript{114} MD. CTS. & JUD. PROC. CODE ANN. § 10-408(a)(4) (Supp. 1977).
\end{footnotes}
communications are proposed to be intercepted, the place or places where those interceptions occurred or are proposed to occur, and "the action taken by the judge on each application." The latter requirement appears to be surplusage unless it refers to the sealing of tapes and the placing of them in custody under the direction of the judge. Otherwise the interception clearly demonstrates what action the judge took. On the other hand, disclosure of a denied request indicates the judge refused to grant an order.

Section 10-408(a)(6) provides for an extension of the interception order initially granted. The application for the extension must include the results obtained as of that time and why the intercept has failed.

Sections 10-408(a)(4),(5) and (6) must be read together with section 10-408(e). The latter section prescribes the time limits in which the order or any extension of it has vitality. It contains language strikingly similar to that of 18 United States Code section 2518(5) from which it has been cloned and limits interception orders to the minimum necessary to obtain the objective. The order's duration may not exceed thirty days. It may be extended, however, for an additional period of "no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than 30 days." These statutorily sanctioned "extensions" make it crystalline that neither the Attorney General nor the "principal attorney" of a political subdivision is restricted as to the number of extensions that may be authorized.115

One of the weaknesses of the state's case in Siegel was its utter failure to comply with section 2518(5) of the Omnibus Crime Control and Safe Streets Act of 1968. By that section the Congress mandated that any intercept order be for no "longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days." The first Siegel order was for five days, a period well within the statutory time, except that it made no effort to limit the interception to a shorter period, if the objective was achieved in less time. The Court of Appeals held that the failure to require termination of the interception upon attaining the objective within five days "left too much discretion in the hands of the state police."116 Furthermore, Siegel noted that the two renewal orders, permitted by section 2518(5) were void because the original order upon which the latter two were grounded lacked the statement of limitation to the attainment of the objective if it was achieved prior to the outer time limit specified in the order.117 Section 10-408(e) provides, in effect, the same limitations imposed by the Congress in

115. Id. § 10-408(e) (Supp. 1977).
116. 266 Md. at 273, 292 A.2d at 95.
117. Id.
section 2518(5), and the construction placed upon section 2518(5) by Siegel will undoubtedly be transferred to any issue arising in the appellate courts of Maryland out of section 10–408(e).

Before a judge may issue an order authorizing electronic or other type of interception of oral or wire communications, he or she must be satisfied that the facts submitted by the applicant establish probable cause for the belief that the person or persons whose communications are sought to be intercepted have committed or are about to commit one of the offenses enumerated in section 10–406. The facts must indicate to the judge that there is probable cause to believe that "particular communications" relative to the offense will be obtained through interception. Additionally, the application must demonstrate that there is probable cause to believe that "the facilities from which, or the place where" the interception is to be made are leased to, listed in the name or names of, or commonly used by the person whose communication is to be intercepted.

The application, as has been previously noted, must also contain the statement relative to why normal investigative procedures will not work or have not worked, or are too dangerous. An application for an extension of an order was held to be defective in Calhoun because the application for the extension did not allege that normal investigative methods had been tried or would not succeed if tried, nor that they were too dangerous to the police. The investigating officers in Calhoun endeavored to "piggy-back" the defective affidavit onto the prior valid affidavit under an incorporation by reference theory. The tap uncovered an illegal gambling operation taking place in a residential neighborhood. Based on this information a search and seizure warrant was executed and gambling paraphernalia was impounded. The court struck down the intercept order for the private phone and directed suppression of the evidence derived from the illegal tap.

The Maryland statute also requires that each order allowing interception of an oral or wire communication shall specify the name of the person, if known to the applicant, whose communications are to be intercepted; the nature and place of the interception; the type of communication to be intercepted and the offense to which it relates; the agency that will conduct the interception and the name of the person authorizing the application.

Subsection (d)(1)(v) of section 10–408 provides that the order shall also contain "[t]he period of time during which the interception

119. Id. § 10–408(c)(2). The law does not sanction mere "fishing expeditions" or intrusion into private communications on bare "hunches."
120. Id. § 10–408(c)(4).
121. Id. § 10–408(c)(3).
is authorized, including a statement as to whether the interception shall automatically terminate when the described communication has been first obtained.” At a first reading, this subsection appears to conflict with the federal statute, section 2518(5), which, as we have seen, requires an interception to cease when it has achieved its objective, but actually there is no clash between the two. The fact is that subsection (d)(1)(v) is lifted from section 2518(4)(e) verbatim. Subsection (d)(1)(v) of section 10-408 must be read together with subsection (e). When that is done, it becomes clear that what is meant is that orders for interception shall contain a provision that when the objective is obtained, the interception shall cease, but there are exceptions to that rule. If the police can satisfy the issuing judge, and ultimately an appellate court, if it is called upon to review the order, that the nature of the investigation necessitates that the “interception should not automatically terminate” when the police first obtain the particular information sought, because there is probable cause to believe that “additional communications of the same type will occur thereafter,”124 the issuing judge may permit the interception to continue past the first achievement of the objective. This order is not operative for more than thirty days in any event.125

Upon request of the applicant, the issuing judge “shall direct that a communications common carrier, landlord, custodian or other person furnish” such facilities and technical assistance as may be required in order to carry out the interception with a minimum of interference and the maximum confidentiality as circumstances allow.126 Landlords, custodians, and communication common carriers or other persons rendering assistance are to be compensated for the use of their facilities or aid to the state “at the prevailing rates.”127

The statute mandates that progress reports be submitted to the issuing judge while the interception order is in effect. In fact, the order authorizing the interception shall contain a provision requiring reports to be made to the judge with such frequency as he or she directs.128

Last, but by no means least, is the state and federal requirement that interceptions are to minimize eavesdropping of communications “not otherwise subject to interception.”129 This restriction is designed to protect the privacy of non-relevant communications as

127. Id. By whom and how the “prevailing rates” are to be determined is not disclosed by the act.
128. Id. § 10–408(f).
well as those privileged under law. The Poore court pointed out the practical difficulty with minimization orders. The court, in response to an attack on the overhearing and recording of a conversation between one of the targets of the interception and her attorney, said:

If the police were required to cease all listening, recording, and spot-checking because the conversation appeared superficially to be a privileged communication, it would not be long before those involved in unlawful activity would circumvent the wiretap by creating the impression to the monitor that the conversation was a privileged communication irrespective of its content. The titles of "attorney," "doctor," "reverend," "priest," or "father" might well become underworld code words in order to defeat electronic interception.\(^\text{130}\)

Shortly after Poore was decided, the Supreme Court, in Scott v. United States,\(^\text{131}\), a seven-to-two decision,\(^\text{132}\) stated that:

> [b]ecause of the necessarily ad hoc nature of any determination of reasonableness, there can be no inflexible rule of law

\(^\text{130}\) 39 Md. App. at 71, 384 A.2d at 119.
\(^\text{132}\) The author of the opinion, Mr. Justice Rehnquist, was joined by the Chief Justice and Mr. Justices Stewart, White, Blackmun, Powell, and Stevens. Mr. Justice Brennan dissented and Mr. Justice Marshall joined therein. In his critical dissent of the majority decision, Mr. Justice Brennan wrote as follows:

In a linguistic tour de force the Court converts the mandatory language that the interception "shall be conducted" to a precatory suggestion. Nor can the Court justify its disregard of the statute's language by any demonstration that it is necessary to do so to effectuate Congress' purpose as expressed in the legislative history. On the contrary, had the Court been faithful to the congressional purpose, it would have discovered in § 2518(10)(a) and its legislative history the unambiguous congressional purpose to have enforced the several limitations on interception imposed by the statute. Section 2518(10)(a) requires suppression of evidence intercepted in violation of the statute's limitations on interception and the legislative history emphasizes Congress' intent that the exclusionary remedy serve as a deterrent against the violation of those limitations by law enforcement personnel. See S. Rep. No. 1097, 90th Cong., 2d Sess., 96 (1968).

The Court's attempted obfuscation in Part II, ante, 6-10, of its total disregard of the statutory mandate is a transparent failure. None of the cases discussed there deciding the reasonableness under the Fourth Amendment of searches and seizures deals with the discrete problems of wire interceptions or addresses the construction of the minimization requirement of § 2518(5). Congress provided the answer to that problem and the wording of its command and not general Fourth Amendment principles must be the guide to our decision. The Court offers no explanation for its failure to heed the aphorism: "Though we may not end with the words in construing a disputed statute, one certainly begins there." Frankfurter, Some Reflections on the Reading of Statutes, 47 Colum. L. Rev. 527, 636 (1947).

\(^\text{Id.}\) at 145-47 (footnotes omitted).
which will decide every case. The statute does not forbid the interception of all nonrelevant conversations, but rather instructs the agents to conduct the surveillance in such a manner as to "minimize" the interception of such conversations. Whether the agents have in fact conducted the wiretap in such a manner will depend on the facts and circumstances of each case.

We agree with the Court of Appeals that blind reliance on the percentage of nonpertinent calls intercepted is not a sure guide to the correct answer. Such percentages may provide assistance, but there are surely cases, such as the one at bar, where the percentage of nonpertinent calls is relatively high and yet their interception was still reasonable. The reasons for this may be many. Many of the nonpertinent calls may have been very short. Others may have been one-time only calls. Still other calls may have been ambiguous in nature or involve guarded or coded language. In all these circumstances agents can hardly be expected to know that the calls are not pertinent prior to their termination.

In determining whether the agents properly minimized it is also important to consider the circumstances of the wiretap. For example, when the investigation is focusing on what is thought to be a widespread conspiracy more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise. And it is possible that many more of the conversations will be permissibly interceptable because they will involve one or more of the co-conspirators. The type of use to which the telephone is normally put may also have some bearing on the extent of minimization required. For example, if the agents are permitted to tap a public telephone because one individual is thought to be placing bets over the phone, substantial doubts as to minimization may arise if the agents listen to every call which goes out over the phone regardless of who places the call. On the other hand, 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.

. . . In a case . . . involving a wide-ranging conspiracy with a large number of participants even a seasoned listener would have been hard pressed to determine with any precision the relevancy of many of the calls before they were completed. A large number were ambiguous in nature, making characterization virtually impossible until the completion of these calls. And some of the nonpertinent conversations were one-time conversations. Since these calls did not give the agents an opportunity to develop a category of innocent calls which should not have been intercepted,
their interception cannot be viewed as a violation of the minimization requirement.\textsuperscript{133}

Minimization, it would appear, is not the bogeyman police and prosecutors portray it to be, nor is it a panacea for defense counsel claiming every intercept to be an abuse of legislative intent. To quote Mr. Justice Rehnquist in \textit{Scott}, each case must be determined "on the facts and circumstances" peculiar to it.\textsuperscript{134}

After the interception has occurred and the communication, when possible, recorded "on tape or wire," custody of the tape or wire is in such place as the issuing judge shall order. The recordings may not be destroyed for at least ten years. Although the code provides for duplicates of recordings for use during investigations, the presence of the judge's seal on the originals, or its absence satisfactorily explained, is a prerequisite to admission of the recordings' contents into evidence. The same requirement applies to physical evidence or testimony derived from the intercepted communication attempted to be placed into evidence.\textsuperscript{135}

Of singular importance in both the federal and state statutes is the inventory notice. This requirement commands the issuing judge to serve an inventory notice on the person or persons whose communications have been intercepted. Such notice must disclose to that person, or persons, that an order authorizing the interception was in fact granted, the date of the order, and the period of time during which the interception was authorized, along with a statement as to whether wire or oral communications were actually intercepted. In addition to the person or persons whose communications were sought to be intercepted, the issuing judge may notify any other party whose oral or wire communications were intercepted as a result of the order, if the judge deems that notification is in the interest of justice.\textsuperscript{136}

Unlike the federal act, the state statute makes no provision for notification to a person whose interception of oral or wire communications was sought but denied. Title 18 United States Code, section 2518(8)(d) provides in pertinent part that,

\[\text{within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of an order or extensions ... the issuing or denying judge shall cause [notice] to be served.}\textsuperscript{137}

\begin{itemize}
\item \textsuperscript{133} \textit{Id.} at 139-40, 142 (citation omitted).
\item \textsuperscript{134} \textit{Id.} at 140.
\item \textsuperscript{137} (Emphasis added). The federal act was utilized in \textit{Poore} where the order postponing the service of an inventory was lost by the assistant state's attorney.
\end{itemize}
Congress's purpose in requiring service of an inventory including notice of the order's denial was to prevent the government from establishing or attempting to establish electronic surveillance on a person without that person ever learning about it.\textsuperscript{138} Whether the Maryland statute, with respect to notification, will be construed as less restrictive than the federal law remains to be seen. The safer course is for the legislature to conform section 10-408(g)(4) to section 2518(8)(d), thereby eliminating all doubt. Pending action by the General Assembly or an appellate decision upholding the state's version of non-notification, the better practice is for the judge to whom the application is made and by whom it is denied to follow the strictures of 18 United States Code, section 2518(8)(d).

Extensions of time for service of the inventory required by section 2518(8)(d) is not provided for in the Maryland law. Therefore, the issuing judge must order service of inventory on the individual whose communications were intercepted, such service to be made within ninety days of the termination of the original intercept order or its extension. Counsel for the "target" of the interception or other persons who receive an inventory may file a motion to inspect portions of the intercepted communications.\textsuperscript{139}

The Maryland Code makes unmistakable that neither the contents of an intercepted communication nor the evidence derived therefrom is admissible in any proceeding in Maryland, unless each party has been furnished with a copy of the order and the application for the order, within not less than ten days before the proceeding.\textsuperscript{140} In those cases where interception has been made without an order,\textsuperscript{141} the parties shall be notified, not less than ten days before trial, hearing or other proceeding, of the interception and the reason why an order was not required.\textsuperscript{142}

Notwithstanding the unambiguous language of \textit{Siegel} that the court will not abide the slightest deviation from strict compliance with the federal wiretap code, the court, in \textit{Spease}, held that a notification of inventory, while not precisely following the act, did provide "actual notice of the wiretap . . . almost six months prior to trial, [and thus] Spease . . . [and Ross, Spease's codefendant] did not suffer any prejudice."\textsuperscript{143} Patently, \textit{Spease} announced a "substantial

\begin{itemize}
\item \textsuperscript{138} \textit{In re United States Authorizing Interception of Wire Communications}, 413 F. Supp. 1321 (E.D. Pa. 1976).
\item \textsuperscript{140} \textit{MD. CTS. & JUD. PROC. CODE ANN.} § 10-408(h) (Supp. 1977).
\item \textsuperscript{141} \textit{Id.} § 10-402(c).
\item \textsuperscript{142} \textit{Id.} § 10-408(h).
\item \textsuperscript{143} 275 Md. at 109, 338 A.2d at 296.
\end{itemize}
compliance” standard while simultaneously declaring in a footnote, “[n]othing in our opinion in this case is intended to depart in any way from our holding in Siegel.” 144 It was left to the Court of Special Appeals in Poore to explain what appeared to be a conflict between Spease and Siegel. That court observed that,

[a] careful reading of both cases makes it transpicuous that Siegel is directed to pre-intercept and intercept conditions. As to those two (2) happenings, not the slightest deviation from the statute will be sanctioned. On the other hand, Spease indicates that when post-intercept events are brought into question, the Court looks to the facts so as to ascertain whether there has been substantial compliance with the post-intercept provisions of the act and whether there has been actual prejudice to the defendant. Thus, it is obvious that there is a distinction between pre-order and post-order compliance. In the former, a defect will void the order and cause suppression of the evidence, 145 but in the latter, a defect will not vitiate the order if there has been substantial compliance and no prejudice to the defendant is shown. 146

The contents of a communication will be suppressed as will any evidence derived therefrom on application from an aggrieved party if the communication was unlawfully intercepted, the order permitting interception is invalid, or the interception was not made in accordance with the order. 147

The state possesses the right of appeal from the denial of an application for an order. 148 It appears that such an appeal will take the nature of an ex parte proceeding because the party whose communications are to be intercepted, under Maryland State law, is not notified if the application is denied, 149 and if the federal act applies, notification need not be made for ninety days following the denial. 150 Theoretically, the appeal can be prosecuted and determined before the expiration of the ninety days. But what if it is not, and the fact that the interception order was denied is served upon the

144. Id. at 108 n.3, 338 A.2d at 295 n.3.
145. In Shingleton v. State, 39 Md. App. 527, 387 A.2d 1134 (1978), an oral order, an absolute nullity, to intercept a wire communication was authorized. Not only was the order invalid but the “application” was made by a state police officer over a telephone. The state police officer was not, of course, the principal prosecuting attorney for the state or of any political subdivision thereof, and completely lacked authority to apply for the order. While the order was held to be void, there was, it developed, nothing to suppress because there was not a recording of any communication that may have been intercepted, if any.
146. 39 Md. App. at 53–54, 384 A.2d at 110 (emphasis in original).
148. Id. § 10–408(i)(3).
149. Id. § 10–408(g).
individual whose oral or wire communications are sought to be intercepted? May he or she intervene in the appeal so as to oppose the state's action? Would the notification of the application for an order render the issue moot for practical purposes because the surreptitious nature of the interception is irretrievably lost?

Section 10-408(i)(1) provides that an "aggrieved person" may "in any trial, hearing, or proceeding in or before any court . . . of this State . . . move to suppress the contents of any intercepted wire or oral communication . . . ." That language is not sufficient to embrace the case of an individual endeavoring to uphold a court's refusal to issue an intercept order because the section is confined to an "aggrieved person" whose communication has been intercepted. The expectation of an interception is not the equivalent of an actual interception.

Section 10-409: Reports to Administrative Office of the Courts and to the General Assembly

To assure that intercept orders are not arbitrarily issued or denied, the judge must file a detailed report with the administrative office of the courts within thirty days of the decision. The report should incorporate all pertinent information except the identity of the person whose oral or wire communication was ordered to be intercepted or whose interception was denied.\textsuperscript{151} The attorney general and state's attorneys are directed to file annual detailed reports relative to interception orders to the administrative office of the courts.\textsuperscript{152} The state court administrator, in turn, must advise the General Assembly by "a full and complete report" as to the number of applications "granted or denied," and he is authorized to issue "binding regulations" dealing with the content and form of the reports required to be filed by the issuing judge, attorney general and state's attorneys.\textsuperscript{153} By requiring the annual report, the legislature may keep check on the wiretap eavesdrop law to assure that it is not being abused.

Section 10-410: Civil Liability, Defense to Civil or Criminal Action

Any interception or disclosure in violation of the State electronic surveillance and eavesdrop law entitles the person whose privacy has been violated to maintain a civil action for "[a]ctual damages but not less than liquidated damages . . . of $100 a day for each day" or a total of "$1,000, whichever is higher," plus punitive damages where actual damages are found, reasonable attorney's

\textsuperscript{151} Md. CTS. \& JUD. PROC. ANN. § 10-409(a) (Supp. 1977).
\textsuperscript{152} Id. § 10-409(b).
\textsuperscript{153} Id. § 10-409(c).
fees, and costs. A good faith reliance on an order of court or legislative authorization is a complete defense to any civil or criminal action brought under section 10-410 "or under any other law."

Section 10-411: Registration of Intercepting Devices; Serial Number

Penultimately, the act necessitates a registration with the Department of Public Safety and Correctional Services of "all electronic, mechanical or other devices" which are designed to be used primarily for the "surreptitious interception of wire and oral communications . . . ." Each device so registered shall be issued a serial number which is affixed to the device.

Section 10-412: Breaking and Entering, etc., to Place or Remove Equipment

Ultimately, the General Assembly has condemned and made a felony punishable by imprisonment "for not more than ten years" any breaking or entering, or entering under false pretenses, or trespass without a court order upon any premises with the intent to place, adjust, or remove wiretapping or electronic surveillance equipment. This section does not seem to have exempted police officers from its scope nor to have permitted judges to issue an order contrary thereto. Additionally, Maryland has no statute conferring upon the Attorney General or State's Attorneys the blanket authority to grant immunity to one person in exchange for his testimony against another, although there are limited statutory provisions allowing the grant of immunity of certain specific offenses.

Title 18 United States Code sections 6002 and 6003 confer the authority to grant immunity from prosecution on a United States Attorney when in his judgment, with the approval of the Attorney General, he deems it advisable to so do to protect the public interest or to induce testimony or other information when the witness is likely to invoke the fifth amendment "privilege against self-

154. Id. § 10-410(a). There is no monetary limitation upon the recovery of punitive or exemplary damages other than that such an award be warranted under the circumstances of the case. See D. C. Transit System, Inc. v. Brooks, 264 Md. 578, 287 A.2d 251 (1972); Vancherie v. Siperly, 243 Md. 366, 221 A.2d 356 (1966); Galusca v. Dodd, 189 Md. 666, 57 A.2d 313 (1948); Dennis v. Baltimore Transit Co., 189 Md. 610, 56 A.2d 813 (1948).

155. MD. CTs. & JUD. PROC. CODE ANN. § 10-410(b) (Supp. 1977).

156. Id. § 10-411(a).

157. Id. § 10-411(c).

158. Id. § 10-412.

incrimination.” As with most immunity statutes, the witness is not exempt under section 6002 from prosecution for perjury or contempt.

It is to be observed that if, upon application to the court, the witness is ordered to testify or produce evidence which may incriminate him, and he does so after refusing “on the basis of his privilege against self-incrimination,” the compelled testimony or evidence shall not be used against him in a criminal case. Inferentially, the triggering mechanism that brings about immunity must be pulled by the witness’s claiming his fifth amendment right not to incriminate himself. It would appear that if he refuses to testify without invoking the fifth amendment but is ordered by a court to so do under penalty of contempt, he might be successfully prosecuted in the same or another proceeding. As a practical matter, the problem may never arise because of the necessity to insure the witness’s cooperation, his willingness to avoid prosecution, and the knowledge by the judge and United States Attorney that such testimony under threat of punishment for contempt would, in and of itself, be a violation of the witness’s constitutional protections.

IV. PEN REGISTERS

The Supreme Court, in United States v. New York Telephone Company, held in a plurality opinion that “pen registers” do not fall within the definition of “intercept” as that word is employed in 18 United States Code sections 2510–2520. Mr. Justice White, in New York Telephone, wrote that “Congress defined ‘intercept’ to mean ‘the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device.’ 18 United States Code section 2510(4).” The rationale of the decision is that pen registers do not overhear nor disclose the content of a wire or oral communication but merely reveal that one telephone was used to dial the number of another. In short, the pen register records only that a communication was made or attempted.

Of material aid to Justice White was the legislative history of section 2510(4) wherein it is stated that,

161. Id. § 6002 (emphasis added).
163. Mr. Justice Powell, in United States v. Giordano, 416 U.S. 505, 549 n.1 (1974), said:

[a] pen register is a mechanical device attached to a given telephone line and usually installed at a central telephone facility. It records on a paper tape all numbers dialed from that line. It does not identify the telephone numbers from which incoming calls originated, nor does it reveal whether any call, either incoming or outgoing, was completed. Its use does not involve any monitoring of telephone conversations.
164. 434 U.S. at 166 (emphasis in original).
The proposed legislation is not designed to prevent the tracing of phone calls. The use of a "pen register," for example, would be permissible. . . . The proposed legislation is intended to protect the privacy of the communication itself and not the means of communication.\textsuperscript{165}

The Court did not reach the question of whether the use of a "pen register" was a "search and seizure" within the meaning of the fourth amendment. Instead it confined its discussion to the sphere of the Omnibus Crime Control and Safe Streets Act of 1968.\textsuperscript{166}

At the time \textit{New York Telephone} was decided, there was pending before the Court of Appeals of Maryland \textit{Smith v. State},\textsuperscript{167} a "pen register" case in which the use of the register was challenged not only as violative of Maryland statutory provisions, but also of the fourth amendment because of the failure of the police to obtain a search and seizure warrant permitting the utilization of the register. In an opinion authored by Chief Judge Murphy for a sharply divided court,\textsuperscript{168} the majority, paralleling the \textit{New York Telephone} decision, held that the use of the pen register did not violate the then Maryland Courts and Judicial Proceedings Code Annotated section 10-402 because it was not an interception of a communication.

Unlike the Supreme Court, the Court of Appeals did consider and rule upon whether, under the fourth amendment, a court order was needed in order to attach the pen register. Chief Judge Murphy observed that "the expectation of privacy protected by the fourth amendment attaches to the content of a telephone conversation and not to the fact that a conversation took place."\textsuperscript{169} The majority of the court declared:

\begin{quote}
We hold that there is no constitutionally protected reasonable expectation of privacy in the numbers dialed in a telephone system and hence no search within the fourth amendment is implicated by the use of a pen register installed at the central offices of the telephone company. While the guarantees of the fourth amendment are broad, they are not boundless, \textit{State v. Siegel}, 266 Md. 256, 292 A.2d 86 (1972); not everything a person may want to be private is protected by the fourth amendment. . . . The intrusion
\end{quote}

\begin{footnotes}
\item[166.] That the Supreme Court did not reach the search and seizure issue is explained by Mr. Justice White: "The [United States] Court of Appeals held that pen register surveillance was subject to the requirements of the Fourth Amendment. This conclusion is not challenged by either party, and we find it unnecessary to consider the matter." 434 U.S. at 165 n.7.
\item[168.] The Court split four to three. Judge Eldridge wrote a dissent in which Judge Diggles joined. Judge Cole penned a separate dissent.
\item[169.] ___ Md. at ___, 389 A.2d at 864.
\end{footnotes}
involved in pen register surveillance is minimal; no violation of the integrity of the communication system itself is entailed; and no conversation is overheard.\textsuperscript{170}

Judge Eldridge, writing for himself and Judge Digges, saw no distinction between the pen register’s recording of numbers dialed and the action of police in conducting a warrantless search. He pointed out that except for a relatively minor number of long distance calls, the telephone company keeps no record of numbers dialed from a particular phone. He asked how the majority could conclude that because of the recordation by the telephone company of long distance calls, a telephone user did not expect privacy in the dialing of local calls.\textsuperscript{171} Furthermore, the dissenters expressed their dismay that the majority would distinguish between verbal and digital transmission. Communication is protected under \textit{Katz v. United States},\textsuperscript{172} they concluded, whatever its form. He and Judge Digges, as well as Judge Cole, believed that the use of the pen register requires the obtaining of a judicially passed order based on probable cause, before the police may install a pen register.

The obtention \textit{vel non} of a search warrant before the installation of a pen register is allowed is largely contingent upon the viewer’s philosophical outlook on the fourth amendment. Those who believe that the dialer of a telephone has no reasonable expectation of privacy in the number called because of its going through the telephone company’s intricate communications system will rally to the side of the majority. On the other hand, those who think that the dialer of a telephone call is entitled to the protection of the fourth amendment in using the telephone argue that under \textit{Smith}, the police are now licensed to install pen registers at will on any one’s phone for whatever purpose, without any cause, much less “probable cause” being first demonstrated to a judicial officer.

The final outcome will have to await a definitive decision of the Supreme Court. Until then, however, it is clear that in Maryland the police no longer need judicial authorization for the installation of a pen register on any telephone, private or public.

\textbf{V. CONCLUSION}

The General Assembly of Maryland, demonstrating its displeasure generally with eavesdropping and wiretaps, has tracked the Omnibus Crime Control and Safe Streets Act of 1968, 18 United States Code sections 2510–2520, in enacting sections 10–401 through 10–412. In so doing, the legislature has narrowed the ambit of the

\textsuperscript{170} Id. at ___, 389 A.2d at 867–68.
\textsuperscript{171} Id. at ___, 389 A.2d at 868–69 (Eldridge, J., dissenting).
\textsuperscript{172} 389 U.S. 347 (1967) (communication deserving of fourth amendment protection, provided reasonable expectation of privacy exists).
act, with the addition of arson, by Act of May 2, 1978, chapter 339, 1978 Maryland Laws 1424, to eight specific crimes and conspiracy to commit any of those eight. Observing the signal flag flown in Siegel that the state may adopt a more restrictive act than that of the federal government, the General Assembly has circumscribed the Maryland wire and oral communications interception law well within the confines of that passed by Congress.

The state statute, however, may not mean what it seems to say relative to testimony and evidence derived from wiretaps or other interceptions of oral or wire communications being admissible in any proceeding.

Prior decisions of the Court of Appeals and of the Court of Special Appeals, interpreting sections of the federal law that appear in the new state act in verbatim form or in a form substantially like that adopted by the Congress, make indubitable that most of the state law will certainly withstand constitutional attack. The failure of the state law to require the service of notice on an individual whose oral and wire communications are sought to be intercepted by the state, but denied by the judge, casts doubt upon that particular section in light of the federal act's more restrictive provisions, but the legislature may remove any doubt by way of amendment. The act as written guarantees to the people of Maryland, insofar as the state, itself, is concerned, greater protection from surreptitious eavesdropping and wiretapping than that afforded the people by the Congress.

How often we do complain,
That our spoken words go unheard,
That no one really cares what we maintain,
Our utterances are thought absurd.
Cheer up! There is one to hear,
An electronic recorder is in gear,
And now we live in fear,
For what we earlier did state
May be recorded on government tape.