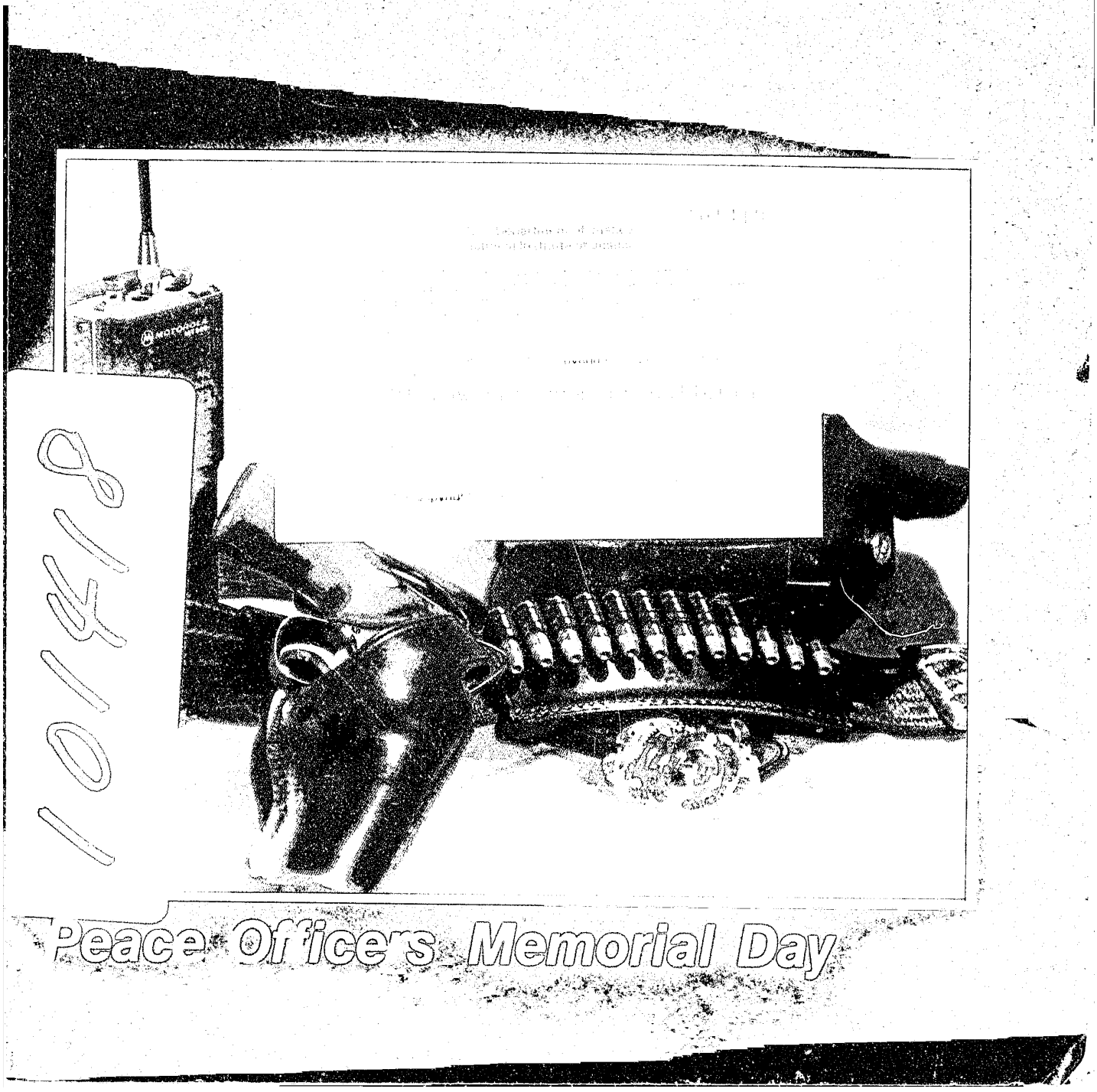

Peace Officers Memorial Day

Contents

May 1986, Volume 55, Number 5

101418

The Cover:
With the observance of Peace Officers Memorial Day on May 15th, tribute is paid to those law enforcement officers who made the ultimate sacrifice while keeping the peace and enforcing the law.

FBI
Law Enforcement Bulletin

United States Department of Justice
Federal Bureau of Investigation
Washington, DC 20535

William H. Webster, Director

The Attorney General has determined that the publication of this periodical is necessary in the transaction of the public business required by law of the Department of Justice. Use of funds for printing this periodical has been approved by the Director of the Office of Management and Budget through June 6, 1988.

Published by the Office of Congressional and Public Affairs, William M. Baker, *Assistant Director*

Editor—Thomas J. Deakin
Assistant Editor—Kathryn E. Sulewski
Art Director—Kevin J. Mulholland
Production Manager—Marlethia S. Black
Reprints—Robert D. Wible

ISSN 0014-5688 USPS 383-310

Raiding the Computer Room
Fourth Amendment Considerations (Part I)

"Computer-related crimes present new challenges in the establishment of probable cause...."

By
JOHN GALES SAULS
Special Agent
FBI Academy
Legal Counsel Division
Federal Bureau of Investigation
Quantico, VA

Law enforcement officers of other than Federal jurisdiction who are interested in any legal issue discussed in this article should consult their legal adviser. Some police procedures ruled permissible under Federal constitutional law are of questionable legality under State law or are not permitted at all.

For several decades, electronic computing machines have been changing the world. Businesses now record their activities by computer, law enforcement agencies maintain criminal records by computer, children are entertained by computer-driven electronic games, and authors process their words by computer. Even tasks such as medical diagnoses are being performed with the aid of computers.

In the last decade, the proliferation of low-cost "home computers" has facilitated the spread of computer power and knowledge to vast numbers of citizens. Thus, it should be no surprise that criminals have begun to use computers to commit crimes and to record the activities of their criminal enterprises. Consequently, law enforcement officers are finding it increasingly necessary to search for, examine, and seize computers and computerized records in successfully investigating and prosecuting many criminal acts.

While conducting investigations of computer-related crimes, officers must comply with an 18th century prohibition against "unreasonable searches and seizures"[1] and contend with 20th century electronic technology. For example, investigators may at times find themselves searching for intangibles rather than familiar physical evidence, such as guns or stolen stock certificates. As one court has noted, the target of a search may be "records [that] exist as electronic impulses in the storage banks of a computer."[2] This new technology creates the possibility of a criminal armed with a home computer in Wisconsin contacting a computer in New York by telephone and illegally causing funds to be transferred electronically to a bank account in France. Regardless of these technological advances, search and seizure by law enforcement officers continues to be governed by the fourth amendment to the U.S. Constitution.[3]

This two-part article will examine issues that arise when officers seek a warrant to search and seize a computer and the information it has processed. Part I will address the application of the fourth amendment warrant requirement to computer-related searches, focusing on special problems officers may encounter in establishing probable cause to search and particularly describing the computer equipment to be seized. Part II will address the description of computer-processed information to satisfy the particularity requirement and then consider issues that may arise in the execution of a warrant authorizing the seizure of a computer and computer-processed information.

Special Agent Sauls

WARRANT REQUIREMENT

The fourth amendment protects the right of the people to be "secure in their persons, houses, papers and effects" against unreasonable Government intrusion.[4] This protection extends to computers, which are effects, and to information processed by this electronic technology, which can be categorized as papers. The constitutional demand upon the officer seeking to seize a person's computer or computerized information is that the seizure be reasonable.[5] The U.S. Supreme Court, in establishing guidelines for reasonable searches and seizures, has stated a preference that they be made pursuant to a judicially issued search warrant. The "Constitution requires that the deliberate, impartial judgment of a judicial officer be interposed between the citizen and the police ... searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[6] This requirement that a warrant be obtained prior to a search or seizure is applied with special strictness where business or residential premises, the places computers are most likely to be located, must be entered to perform the search.[7]

The fourth amendment sets forth certain procedural requirements that must be met if a valid warrant is to be issued. There must be a showing of probable cause supported by oath or affirmation, and the warrant must particularly describe the place to be searched and the persons or things to be seized.[8] In addition, the Supreme Court has held that the probable cause determination must be made by a neutral, detached magistrate.[9] The requirements of oath or affirmation and of presentation to a neutral, detached magistrate raise no special problems where computer searches are concerned; however, the probable cause and particularity requirements pose unique problems where computers are the search target, and these issues merit discussion.

Probable Cause To Search

Central to the protections provided to citizens by the warrant requirement is the command that no warrants shall issue but upon probable cause.[10] This language has been interpreted to require that before a search warrant may be issued, the Government must set forth facts that would cause a reasonable person to conclude that it is probably true that (1) a crime has been committed, (2) that evidence of that crime is in existence, and (3) that the evidence presently exists at the place to be searched.[11] Obviously, satisfying this requirement necessitates the collection and presentation of information, and law enforcement officers perform this task daily in regard to numerous crimes. Computer-related crimes present new challenges in the establishment of probable cause though, because of the unfamiliar technology involved. Although a magistrate likely already understands how a murder may be committed with a gun, he may require considerable explanation before finding that an embezzlement was committed by means of a computer. The problem is largely an educational one.

Inasmuch as computers may be used in a wide variety of criminal endeavors, ranging from fraud to espio-

"... an officer seeking to convince a magistrate that a novel crime has been committed should use care to ensure that the explanation of the mechanics of the crime is clear and easily understood."

nage, it is difficult to state concisely what is required to satisfy the probable cause requirement in a computer-related crime. In general, probable cause will be established just as it would in a case where no computer was involved, except that additional facts will have to be presented regarding the role of the computer in the criminal activity.

That a Crime Has Been Committed

The first hurdle in establishing probable cause to search is articulating facts to indicate that a crime probably has been committed. In determining what additional facts a magistrate will need to make such a finding where a computer is involved in the crime, it is helpful to examine the role played by the computer in the criminal activity. For example, where a computer is stolen, the crime is the same as any other theft, and the required factual showing, describing the computer as the object of the crime, would likewise be the same. Where a computer is used as a tool to commit a crime, facts must be presented to show the crime was committed and to explain how the computer was used in the commission. Because computer systems are commonly installed so they may be used from distant locations by means of electronic communication over telephone lines, novel criminal opportunities have been created.[12] Valuable data may be transferred from one computer to another or modified to achieve advantage for the computer criminal.[13] Inasmuch as the means used to commit these crimes are unfamiliar, the officer must convince the magistrate that such a crime has been committed by detailing how it was committed.

An example of an officer successfully obtaining a search warrant in a case where new technology was being employed to commit the crime of fraud is found in the case of *Ottensmeyer* v. *Chesapeake & Potomac Telephone Co.*[14] Ottensmeyer, who ran a telephone answering service, decided to provide an alternative to his customers to normal, commercial long-distance telephone service. He found a strategically located town that enjoyed nontoll calling service to a larger city on either side, despite the fact that a call from one of the larger cities to the other was a toll call. Ottensmeyer installed an electronic device in the small town that allowed a customer in one of the large cities to "patch" a call to the other large city through the device, thereby avoiding a toll call and defrauding the phone company of revenues to which it was entitled.

The investigator, a police officer who had special training in electronic technology and telecommunications, sought a warrant to search the premises where the "patching" device was located. In his affidavit, the officer "informed the judge of his experience in the electronic field and of his independent investigation and conclusions."[15] The officer articulated facts that explained how the scheme to defraud functioned, and drawing on his expertise, cited inferences he had drawn from the facts he had observed. The warrant was issued and the search performed.[16]

Obviously, an officer seeking to convince a magistrate that a novel crime has been committed should use care to ensure that the explanation of the mechanics of the crime is clear and easily understood. If the officer wishes the magistrate to consider the officer's interpretations of the facts he has observed, he must inform the magistrate in his affidavit of the experience and training that accredit these interpretations. Consideration of such inferences by a magistrate determining probable cause has been approved so long as the officer sets forth the training and experience upon which they are based.[17]

An officer seeking to establish probable cause where the crime is unusual or unfamiliar may also elect to use the services of an expert. An example of using information provided by experts in affidavits for search warrants is found in *United States* v. *Steerwell Leisure Corp., Inc.*[18] Steerwell was charged with infringing upon the copyrights of a number of electronic video games, and the question of whether a crime had been committed turned on whether the games Steerwell was distributing were sufficiently similar to the copyrighted games to violate the copyright statute. The affidavits to support search warrants presented the magistrate with results of expert analysis in comparing the games distributed by the defendants with the copyright-protected games. In determining the validity of the warrants issued on those affidavits, the court concluded that the magistrate was entitled to accept the conclusions of the experts, but noted the "magistrate's determination of probable cause would be facilitated if the agents' affidavits contained more details concerning the comparisons between protected games and infringing games."[19]

"The primary rule of particularity should be to make the description of the items to be seized as precise as the facts will allow."

The court also made reference to the importance of explaining to the magistrate how the crime was committed, in this case by duplication of the circuit boards that control the action of electronic games.[20] Again, the task of the officer includes providing sufficient technical details in layman's terms to familiarize the magistrate with the mechanics of an unusual crime.

That Evidence of the Crime Exists

The second hurdle for an officer seeking to establish probable cause to search is setting forth facts to convince a magistrate of the probability that evidence of the crime exists. Where a computer is stolen, the stolen computer is evidence of the crime. If the theft is established factually, then the existence of the computer as evidence is likewise established. Similarly, where facts establish that a computer was used to commit a crime, the same facts establish that the computer used was an instrumentality of the crime. This was demonstrated in the *Steerwell Leisure Corp.* case where if the magistrate found that the circuit boards in question violated the copyright laws then the boards would also constitute evidence of that violation.[21]

Where an investigator seeks to establish that computerized records of criminal activity are in existence, his task is essentially the same as establishing the existence of noncomputerized records. He must factually establish that records of the criminal activity have probably been created and retained. There is authority for the position that it is unnecessary to establish factually in the affidavit the physical form in which the records sought are expected to be found.[22] If the officer can establish factually the creation and retention of the records, he need not specify (or know) whether they are being maintained in written, magnetic, or some other form. In *United States* v. *Truglio*, audio cassettes were seized during the execution of a search warrant authorizing the seizure of "... books, records, indices, movies regarding the interstate prostitution operation located at the King of the Road Health Club...."[23] In approving seizure of the audio cassettes, the court noted that "it would have been more precise for the warrant to have specified 'written or electronic records,' " but then stated that "[s]tandards of pragmatism and commonsense must necessarily be adaptable to changing times and technological advances."[24] The court concluded by saying that "[w]hile decades ago it might have been difficult reasonably to infer that records existed in some form other than written, in the mid-1980's commonsense demands that we refrain from remaining so inflexible."[25]

That Evidence of the Crime Presently Exists at the Place to be Searched

Finally, the investigator seeking to establish probable cause to search must factually establish the probability that the evidence sought is presently located at the place he is seeking authorization to search. Whether this requirement of recent information has been met is "... determined by the circumstances of each case."[26] As stated by the U.S. Supreme Court, "[t]he task of the issuing magistrate is simply to make a practical, commonsense decision whether, given all the circumstances set forth in the affidavit before him ... there is a fair probability that ... evidence of a crime will be found in a particular place."[27]

The requirement for recent information is easily satisfied where the investigator can set forth reliable information that the object sought has been recently observed at the proposed search site. Where such facts are not available, other facts must be used to infer that the items to be seized are presently at the place to be searched. At times, having a computer or its records as the target of the search may simplify meeting this requirement. If a computer has been used to commit a crime telephonically, it is possible that it has also been set up to "answer" incoming calls, to allow other computer operators to call it using their computer terminals and a telephone. If such an operation exists, an incoming call will be answered with a tone called a "carrier."[28] When a particular phone is answered with a "carrier," it seems reasonable for a magistrate who has been informed of the significance of the "carrier" to find that a computer and related equipment are probably present at the location of the telephone.

A somewhat analogous case involved a search warrant issued for the seizure of a "blue box," an electronic device used to create tones on the telephone system to facilitate the making of long-distance calls without being billed for the toll charges.[29] In this case, tones such as those produced by a "blue box" had been monitored by the telephone company on a particular telephone for a period of weeks, ending the day prior to the issuance of the warrant. This information was related to the magistrate in the affidavit. In

upholding the validity of the resulting search warrant, the court concluded that "[t]he affidavit set forth substantial information establishing clear probable cause to believe that a device emitting a 2600 cycle tone and Southwestern Bell multifrequency tones was being utilized ... at [the] residence."[30]

Where computerized records are sought, the magistrate should consider that records by their nature are created to be kept for at least a minimum period of time, along with the other facts presented, in determining whether the records are presently at the place to be searched.[31] Although each case must be evaluated on its own facts, the U.S. Supreme Court and lower courts have held that under certain circumstances, it is reasonable to expect that records seen 3 months previously will still be present at that same location.[32]

Particularity

The fourth amendment commands that "no warrants shall issue except [those] ... particularly describing the place to be searched and the persons or things to be seized."[33] This provision requires that a warrant authorize only a search of a specific place for specific named items. Coupled with the probable cause requirement, this provision prevents general searches by ensuring that the warrant describes a discrete, defined place to be searched, describes only items connected with criminal activity for which probable cause has been established, and describes the items so definitely that it removes from an officer executing the warrant the discretion of determining which items are covered by the warrant and which are not.[34] It also provides a signal of when a search is at an end, that is, when all items named in the warrant have been located and seized or when all possible hiding places for items not located have been explored.[35] Since the "place to be searched" portion of the particularity requirement has no special impact on computer searches, it will not be discussed. However, the "things to be seized" portion of the requirement has a marked impact in seeking a warrant to authorize the seizure of a computer or information processed by a computer. This portion will be examined in regard to both the computer and the processed information.

Describing the Computer

The primary rule of particularity should be to make the description of the items to be seized as precise as the facts will allow. A court measuring the particularity of a description in a search warrant may consider what facts could reasonably be known by the investigator at the time application for the warrant was made, so long as the investigator includes all the facts known to him in the affidavit.[36] Consequently, the circumstances of each case can help determine whether a description is sufficiently particular. The nature of the item sought also is considered in determining the degree of particularity required. A less precise description is required of items which are contraband, such as controlled substances.[37] Conversely, greater particularity is demanded when the item sought is of a type in lawful use in substantial quantities.[38] Generally, where computer equipment is sought for seizure pursuant to a search warrant, a quite particular description will be required.

Where a computer has been reported stolen, it is reasonable to expect that the owner will provide a detailed description of the stolen item. Therefore, if the object of the search is a stolen computer, a detailed description, including manufacturer, model number, and serial number if known, will probably be required. This is especially true if the computer sought is a type commonly in lawful use. Care should be taken to ensure all available descriptive information is included.

Where computer equipment is sought because it was used as an instrumentality to commit a crime, the most precise description the facts will allow may be a more general one.[39] Where a victim complains that his computer system has been accessed telephonically by an unknown person and a loss has resulted, it is likely that the investigator will only be able to determine generally what types of devices were used to accomplish the crime. He may, for example, learn that a computer terminal (a keyboard and display monitor) and a modem (a device that allows digitally encoded computer information to be transmitted over telephone lines) were necessary to perform the acts accomplished, but will have no information regarding the manufacturers of the equipment, model numbers, or serial numbers. If a telephone trace reveals the location from which the intruding call originated, the investigator may have probable cause to search. Under these circumstances, the general description of "a computer terminal and a modem of unknown make or model" may suffice.

An analogous case is *State* v. *Van Wert*,[40] where police had probable cause to believe Van Wert was using equipment to forge checks. A search warrant was issued authorizing the seizure of "check protectors and typewriters used in preparation of forged checks." The court approved use of this general language based upon the nature and information known con-

"Where a computer is used as a tool to commit a crime, facts must be presented to show the crime was committed and to explain how the computer was used in the commission."

cerning the crime, stating that greater particularity "... was not needed in this case, where defendant was under investigation for forgery rather than theft of a certain item."[41]

Similarly, the warrant in *United States* v. *Harvey* authorized the seizure of "a 'blue box,' an electronic device that allows a caller to make long distance calls without them being recorded for billing by the telephone company."[42] The Agents executing this warrant ultimately seized audio cassette tapes that had tones such as those produced by a "blue box" recorded on them. The court noted that the affidavit clearly established that a device emitting "blue box" type tones was being used at the place to be searched and then addressed the particularity question, observing that "[n]either the Southwestern Bell officials nor the FBI Agents knew the actual physical form which the device would take, and they assumed it would be in the form familiar to their research and experience...."[43] The court, in approving the seizure, said, "[t]he cassette tapes constituted 'an electronic device that allows a caller to make long distance phone calls without them being recorded for billing by the telephone company' and were thus properly seized as within the limitations of the warrant."[44]

Since computer systems are often comprised of a number of component parts,[45] an investigator applying for a warrant to seize a computer should ensure that the warrant describes all parts of the computer system that are probably present, as well as the various types of storage devices upon which the machine's operating instructions (computer programs) are maintained. It is prudent to consult an expert concerning the items to be listed. Equipment components will probably include a central processing unit, printers, terminals (keyboards and display screens), magnetic tape drives, and magnetic disc drives. Storage media will include magnetic tapes, magnetic discs, punched cards, and paper tapes. Computer printouts will also likely be present.[46] If information that has been processed is being sought, it is especially important to particularly describe the storage media. Consultation with an expert will increase the likelihood of a thorough listing of the items of evidence probably present, and provided the expert's education and experience are set forth in the affidavit, will give the magistrate a sound basis for concluding that the items sought are probably located at the place to be searched.

Part II of this article will conclude the particularity analysis and discuss problems with executing this type of search warrant.

FBI

Footnotes

[1]U.S. Const. amend. IV.
[2]*United States* v. *Hall*, 583 F.Supp. 717, 718 (E.D. Va. 1984).
[3]*See Katz* v. *United States*, 389 U.S. 347 (1967).
[4]U.S. Const. amend. IV.
[5]*See Katz* v. *United States*, 389 U.S. 347 (1967).
[6]*Id.* at 357.
[7]*See Michigan* v. *Tyler*, 436 U.S. 499 (1978).
[8]U.S. Const. amend. IV.
[9]*Coolidge* v. *New Hampshire*, 403 U.S. 443 (1971).
[10]U.S. Const. amend. IV.
[11]*Zurcher* v. *Stanford Daily*, 436 U.S. 547, 556–557 n. 6 (1978), quoting Comment, 28 U. Chi. L. Rev. 664, 687 (1961).
[12]For a discussion of computer telecommunication crime, see Marbach, "Beware: Hackers at Play," *Newsweek*, September 5, 1983, p. 42.
[13]For an interesting discussion of computer crimes, see T. Whiteside, *Computer Capers* (Thomas Y. Crowell Co., 1978).
[14]756 F.2d 986 (4th Cir. 1985).
[15]*Id.* at 990.
[16]*Id.* at 990, 991.
[17]*See, e.g., United States* v. *Ortiz*, 422 U.S. 891 (1975). *See also Johnson* v. *United States*, 333 U.S. 10 (1948).
[18]598 F.Supp. 171 (W.D.N.Y. 1984).
[19]*Id.* at 176.
[20]*Id.* at 177.
[21]*Id.*
[22]*United States* v. *Truglio*, 731 F.2d 1123 (4th Cir. 1984), *cert. denied*, 83 L. Ed.2d. 130 (1984).
[23]*Id.* at 1126.
[24]*Id.* at 1128.
[25]*Id.*
[26]*Sgro* v. *United States*, 287 U.S. 206 (1932).
[27]*Illinois* v. *Gates*, 462 U.S. 213, 238 (1983).
[28]See Fitzgerald and Eason, *Fundamentals of Data Communication*, pp. 42–43 (John Wiley & Sons, 1978).
[29]*United States* v. *Harvey*, 540 F.2d 1345 (8th Cir. 1976).
[30]*Id.* at 1354.
[31]*United States* v. *McManus*, 719 F.2d 1395 (6th Cir. 1983).
[32]*Andresen v. Maryland*, 427 U.S. 463, 478 n. 9 (1976).
[33]U.S. Const. amend. IV.
[34]*See Marron* v. *United States*, 275 U.S. 192 (1927). For a thorough discussion, *see* 2 W. LaFave, *Search and Seizure* 95–101 (1978).
[35]*See* 2 W. LaFave, *Search and Seizure* 162 (1978).
[36]*Cf. Andresen* v. *Maryland*, 427 U.S. 463 (1976).
[37]*See, e.g., Steele* v. *United States*, 267 U.S. 498 (1925).
[38]*Supra* note 35, at 99.
[39]*Id.* at 104. *See, e.g., Quigg* v. *Estelle*, 492 F.2d 343 (9th Cir. 1974).
[40]199 N.W.2d 514 (Minn. 1972).
[41]*Id.* at 515–516.
[42]*Supra* note 29, at 1353.
[43]*Id.* at 1354.
[44]*Id.*
[45]For a discussion of computer system components, see T. Schabeck, *Computer Crime Investigation Manual*, secs. 2.3–2.6 (Assets protection, 1980).
[46]An example of a detailed description of a computer system is: "One Alpha [Brand] Micro computer central processing unit, approximately four Alpha [Brand] Micro computer terminals, computer printers, and computer manuals, logs, printout files, operating instructions, including coded and handwritten notations, and computer storage materials, including magnetic tapes, magnetic discs, floppy discs, programs, and computer source documentation." Quoted from *Voss* v. *Bergsgaard*, 774 F.2d 402, 407 (1985) (warrant invalidated on other grounds).