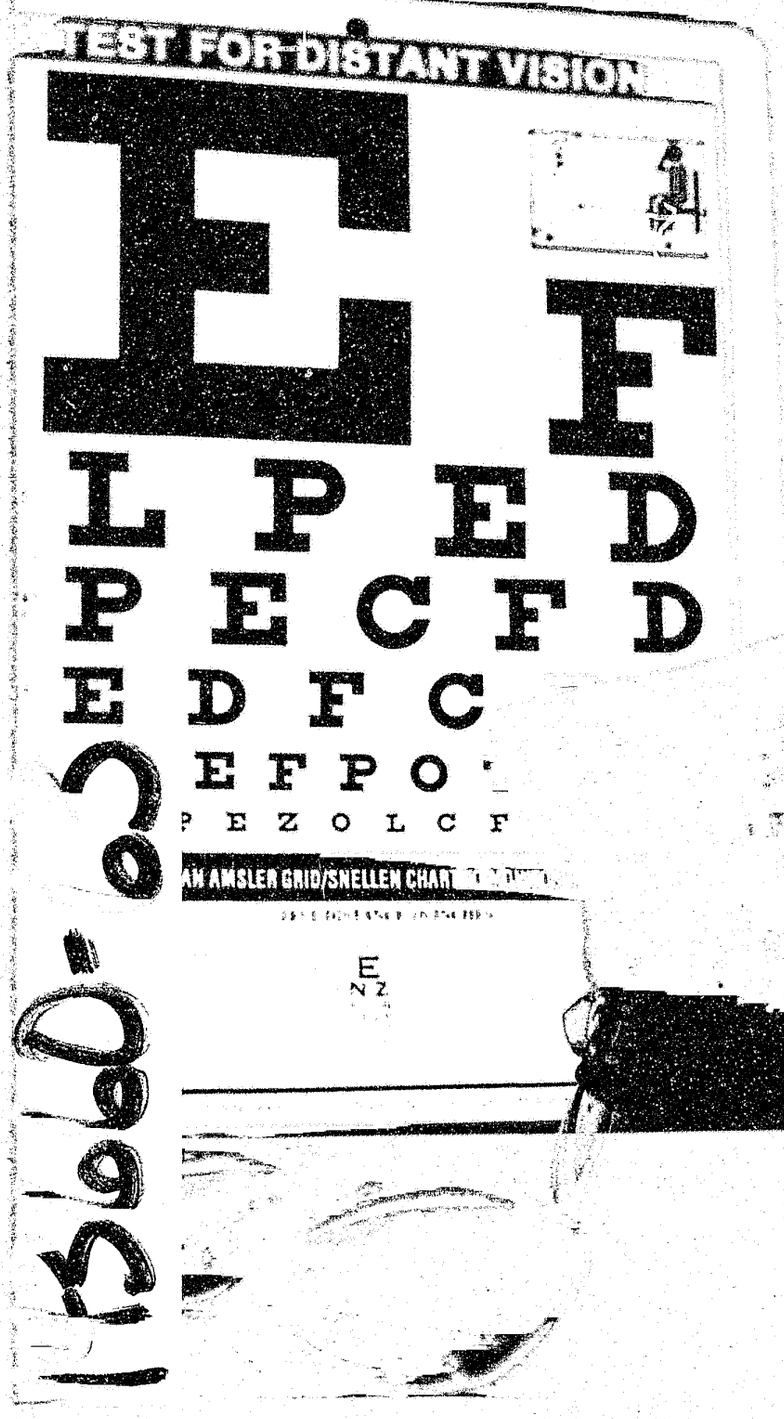


June 1993
Volume 62
Number 6

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

William S. Sessions,
Director

The *FBI Law Enforcement Bulletin* (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Avenue, N.W., Washington, D.C. 20535. Second-Class postage paid at Washington, D.C., and additional mailing offices. Postmaster: Send address changes to *FBI Law Enforcement Bulletin*, Federal Bureau of Investigation, Washington, D.C. 20535.

Cover photo by
K.L. Morrison

FBI Law Enforcement
B ◇ U ◇ L ◇ L ◇ E ◇ T ◇ I ◇ N

Features

Eyesight Standards: Correcting Myths
By Richard N. Holden
1 *Passage of the ADA, court rulings, and a recent survey of police officers call into question the use of uncorrected vision standards.*

The Computer: High-Tech Instrument of Crime
By Michael G. Noblett
7 *Law enforcement personnel should know how to examine computer evidence and records.*

Elevator Vandalism Squad
By Ronald Welsh and Peter Cestare
10 *Elevators create special problems for agencies that provide security to highrise buildings.*

Police Violence: Addressing the Issue
By Daniel B. Boyle
17 *The complexities of policing require a broad-based approach to reduce charges of police brutality.*

Computer Searches and Seizures: Challenges for Investigators
By John Gales Sauls
24 *Knowing the legal restraints on searches for computers and computerized information helps to ensure the admissibility of evidence.*

Departments

6 **Crime Data**
1992 Crime Trends

9 **Unusual Weapon**

14 **Police Practices**
Drug Education

16 **Book Review**
Police Administration

21 **Bulletin Reports**

22 **Focus on Training**
The Americans with Disabilities Act

ISSN 0014-5688 USPS 383-310

Computer Searches and Seizures

Challenges for Investigators

By
JOHN GALES SAULS

An informant tells a detective preparing an affidavit for a warrant to search a drug trafficker's home that the trafficker is a "computer wiz" who keeps all financial records on a "50 megahertz 486." To trace the drug trafficking proceeds for forfeiture purposes, the detective wishes to seize the financial records.

A second officer is investigating a crime in which a computer virus was introduced into a university's mainframe computer, shutting down the school's computer operations for 48 hours. As a result of the officer's investigation, a computer science student becomes a prime suspect. In order to search the student's computer "account" on the school's mainframe for the virus' computer code, the officer seeks a search warrant. He also suspects the "account" to contain an article that the student wrote on computer viruses.

These officers, in seeking to search for computerized information, must contend with both statutory and constitutional restraints that limit police authority. This article examines the effect of these legal restraints on searches for computers and computerized information and suggests strategies to ensure the admissibility of evidence detected.

THE PRIVACY PROTECTION ACT OF 1980

In 1980, Congress enacted a statute to give special protection to documentary materials prepared or gathered for dissemination to the public.[1] The statute requires the government to use a subpoena, rather than a search warrant, to acquire documentary materials, unless one of the statute's exceptions that permits the use of a search warrant applies.[2]

> ***"...officers, in seeking to search for computerized information, must contend with both statutory and constitutional restraints...."***

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

Although the statute specifically provides that its violation is not grounds to suppress evidence,[3] it does provide a civil remedy in Federal court against either the government entity or individual officers involved in the search where a search warrant is used contrary to its provisions.[4]

Because personal computers are used for word processing and desktop publishing with increasing frequency, officers contemplating use of a warrant to search for computerized information should consider the potential application of this statute.[5] When officers have reason to believe that the computer stores information created or gathered for public dissemination, they should make sure that one of the exceptions to the act's prohibitions applies before a search warrant is used.

The exception most likely applicable permits the use of a search warrant when there is probable cause to believe the person *possessing* the materials sought "has committed or is committing a criminal offense to which the materials relate...."[6] If none of the act's exceptions apply, a subpoena should be used to acquire the evidence.

DRAFTING THE APPLICATION AND SEARCH WARRANT

The fourth amendment protects the right of the people to be "secure in their persons, houses, papers, and effects" against unreasonable government intrusion.[7] This protection extends to computers, which are effects, and to information processed and stored by computers, which can be categorized as papers. The constitutional demand on the officer seeking to search for and seize a person's computer or computerized information is that the search and seizure be reasonable.[8]

"Reasonableness" is generally best achieved with a valid search warrant.[9] This is especially true when business or residential premises, the most likely locations for computers, must be entered to perform the search.[10]

The fourth amendment sets forth certain procedural requirements that must be met for a valid warrant 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.[11] The requirement of oath or affirmation raises no special problems where computer searches are concerned; however, the probable cause and particularity requirements pose unique problems where computers are the search target.

ESTABLISHING PROBABLE CAUSE

The fourth amendment probable cause requirement has been interpreted to command that before a search warrant is issued, the government must set forth facts that would cause a reasonable person to conclude that three factors are probably true. Specifically, it must be probably true that a crime has been committed, that evidence of the crime exists, and that the evidence presently exists at the place to be searched.[12]

Crime Committed

Magistrates are familiar with the mechanics of how a murder might be committed with a gun, but they may have difficulty understanding how an embezzlement might be accomplished by means of a computer. When computers are

used to commit a crime, officers need to detail how the suspect committed the crime, primarily because the process involves unfamiliar technology.[13] The problem becomes an educational one.[14]

Obviously, when seeking to convince a magistrate that a crime has been committed in a novel manner, an officer should explain the mechanics of the crime carefully and clearly. If the officer wishes the magistrate to consider the officer's interpretations of the facts, the officer must inform the magistrate in the affidavit of the experience and training that accredit these interpretations.[15]

An officer seeking to establish probable cause that an unusual crime has been committed may also elect to use the services of an expert.[16] The challenge for the officer is providing sufficient details in layman's terms to familiarize the magistrate with the mechanics of an unusual criminal technique.

Evidence of the Crime Exists

A computer may be used as a tool to commit a crime and to create and/or store records of crime. In order to acquire a search warrant to seize both the computer *and* records, officers need to establish factually the probability that each of these things exists and the link between them and the criminal activity. When facts establish the probability that a computer was used to commit a crime, those same facts establish the existence of the computer, as well as its link to the crime.[17]

When an officer seeks to establish that computerized records of criminal activity probably exist, the focus should be on establishing the creation and retention of records rather than the mechanism by which this was accomplished.[18] In the past decade, computer use to create and store records has become so pervasive that the concept of a document existing as binary code imprinted magnetically or optically on a computer disk is no longer novel. Consequently, when documents are the target of the search, the process by which the suspect created the documents need not be set forth for a magistrate in an affidavit. The critical facts are those that demonstrate the probability that records are being kept and that these records are evidence of the criminal activity.

> ***"Factually linking, in the affidavit, the relationship of the items to be seized to the alleged criminal activity is the key."***

United States v. *Falon*[19] is illustrative of this point. In *Falon*, investigators established probable cause that Falon was operating a fraudulent loan advance fee scheme out of two adjacent luxury apartments. They obtained a search warrant that authorized the seizure of "borrowers' files; lists of borrowers; banking and financial records; financial statements; advertising records; correspondence, memoranda and documents relating to loans, loan guarantees, potential loans and potential loan guarantees; and sales literature and brochures."[20] Also listed were "checkbooks; canceled checks; telephone records; address indexes; message slips; mail, telex, and facsimile records; calendars and diaries; memory typewriters; word processors; computer disks, both hard and floppy; and other electronic media devices, electronic storage media and related software."[21]

Items on the first list, because of the clear link to the fraudulent advance fee scheme set forth in the probable cause statement, were held to have been properly seized under the search warrant.[22] "Borrowers' files," for example, have a clear relationship to a loan advance fee scheme.

Items on the second list were held to be insufficiently linked to the alleged criminal activity, and their seizure was held improper, causing them to be inadmissible as evidence.[23] "Calendars and diaries" located in the search might as likely be innocent and personal as criminal.

Factually linking, in the affidavit, the relationship of the items to be seized to the alleged criminal activity is the key. Had the warrant specified, for example, "calendars listing events related to loan-making activity," the linking requirement would have been satisfied for such items. Likewise, listing "floppy disks containing documents related to making or guaranteeing loans" would make such items validly subject to seizure.

Evidence Present at the Search Site

An officer seeking to establish probable cause to search must also factually establish the probability that the evidence sought is *presently* located at the place to be searched.[24] At times, having a computer or its records as the target of the search may simplify meeting this requirement.

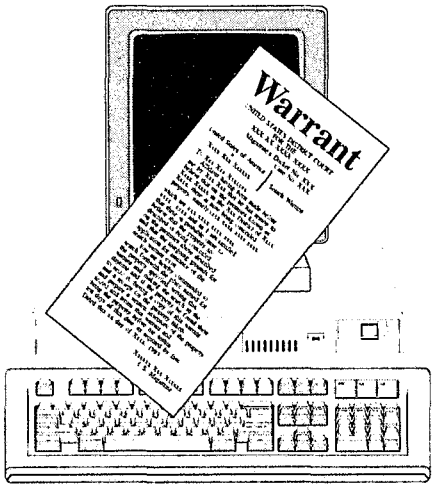
If a suspect used a computer to commit a crime telephonically, it is also possible that the suspect set up the computer to "answer" incoming calls. This allows other computer operators to call it using their computer terminals and a telephone.

When such an operation exists, an incoming call will be answered with a tone called a "carrier."[25] When a particular phone is answered with a "carrier," it seems reasonable for a magistrate, informed of the carrier's significance in the affidavit, to find that a computer and related equipment are probably present at the telephone's location.[26]

When computerized records are sought, the magistrate should consider that records, by their very nature, are created to be kept for at least a minimum period of time. This fact, along with the other facts presented, should be weighed in determining whether the records are presently at the place to be searched.[27] 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 the location where they were observed.[28]

SUFFICIENTLY PARTICULAR DESCRIPTIONS

The fourth amendment limits valid warrants to those "particularly describing the place to be searched and the persons or things to be seized."[29] This provision mandates that a warrant authorizes only a search of a specific place for specifically named items.



Coupled with the probable cause requirement, this provision prevents general searches by ensuring that warrants describe a discrete, defined place to be searched, describe only items connected with criminal activity for which probable cause has been established, and describe the items so definitely that it removes from an officer executing the warrant the unguided discretion of determining which items to seize.[30] It also provides a signal of when to end a search, 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.

The "place to be searched" portion of the particularity requirement has no special impact on computer searches. However, the "things to be seized" portion has a significant impact in seeking warrants to authorize the seizure of computers and information processed by computers.

Describe the Computer System

The primary rule of particularity is to describe the items to be seized as precisely as the facts allow. For example, when a computer has been reported stolen, it is reasonable to expect that the owner can provide a detailed description of the stolen item. Therefore, if the object of the search is a stolen computer, a detailed description, including make, model, and serial number, if known, will probably be required.

When computer equipment is sought because it was an instrumentality of crime, only a more general description may be possible. For example, when a victim complains that the computer system has been accessed telephonically by an unknown person, the investigating officer may only be able to determine what types of devices were used to accomplish the crime. The officer may determine that a computer terminal (a keyboard and display monitor) and a modem (a device that permits digitally encoded computer information to be transmitted over telephone lines) were necessary to perform the acts accomplished, but the officer may not have any information regarding the manufacturers of the equipment, model numbers, or serial numbers. If a telephone

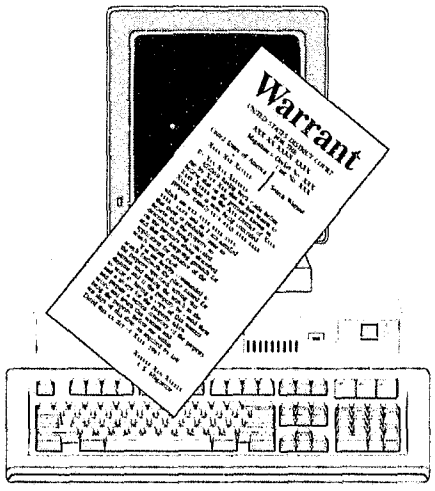
trace reveals the location from which the intruding call originated, the officer may have probable cause to search. Under such circumstances, a rather general description of "a computer terminal and modem of unknown make or model" would likely suffice.[31]

Because numerous component parts comprise computer systems, an investigator applying for a warrant to seize a computer should ensure that the warrant describes all computer system parts that are probably present, including mechanisms for data storage.[32] Consulting with an expert increases the likelihood of listing thoroughly the items of evidence probably present. The expert's education and experience should be set forth in the affidavit to give the magistrate a sound basis for concluding that the items sought are probably located at the place to be searched.

Information Processed By Computer

Because the fourth amendment particularity requirement is strictly applied where documents are concerned, the descriptive task where computerized information is the subject of a search warrant is often a demanding one.[33] Nonetheless, courts reviewing applications for search warrants evaluate the particularity of the document's description in light of the degree of precision that the facts of a case allow.

For example, in *United States* v. *Timpani*,[34] a search warrant authorizing the seizure of "any and all records relating to extortionate credit transactions (loansharking)"[35] was challenged as being insufficiently particular. In reviewing the warrant, the court noted that the warrant included a lengthy list of types of records (including "lists of loan customers, loan accounts, telephone numbers, address books"[36]) and that the warrant "provide[d] a standard for segregating the 'innocent' from the 'culpable' in the form of requiring a connection with [the] specific, indentifiable crime [of loansharking]."[37] The court upheld the particularity of the warrant, stating, "It is difficult to see how the search warrant could have been made more precise."[38]



When aware of specific documents sought, an officer should designate them by type (letter, memo, etc.), date, subject, author, and addressee, providing as much detail as possible. For example, when "a letter from John Jones to Bill Smith dated November 9, 1985, and concerning the ownership of 200 shares of IBM stock" is sought, officers should describe the letter in such specific terms.

When only the general nature of the information sought is known, a highly detailed description is impossible. In such cases, officers must use great care to give a description that includes the information sought but limits the search as narrowly as possible. This is accomplished by using a general description, qualified by some standard that will enable the executing officers to separate the information to be seized from innocent information that may also be present.

Such limiting phrases must be crafted based on the facts establishing probable cause to search. If the facts establish that the information sought comes from a particular time period, the phrase should limit the warrant to information of that time period. If the information sought is known to have been produced by a particular individual, the phrase should limit the description to material authored by that person. If the phrase combines several such factors, it is even more effective. As in *United States* v. *Timpani*, the phrase may restrict the description to particular criminal conduct. In that case, the limiting phrase was "records relating to extortionate credit transactions (loansharking)."[39]

It is most important that the limiting phrase restrict the scope of the search so that it remains within the bounds of the probable cause set out in the affidavit. A warrant may not validly authorize the seizure of items for which probable cause to search has not been established.

In upholding the description of items in the warrant in the *Timpani* case, the court noted that "[e]ach item is plausibly related to the crime—loansharking or gam-

bling—that is specifically set out [in the affidavit]."[40] The description, even though the items to be seized were described in generic terms, did not exceed the probable cause because of the use of an appropriately narrow limiting phrase.[41]

When information sought is described with sufficient particularity, the form in which the information may be found is not of great concern. Concluding the list of described items with the phrase "the documents listed above may be found in written or electronic form" should be sufficient to permit lawful seizures of the documents regardless of the form in which they are found.[42]

EXECUTING THE SEARCH WARRANT

The protection of the fourth amendment does not end when an officer obtains a valid search warrant. The right of citizens to be free of "unreasonable searches and seizures" extends to the manner in which officers execute a search warrant.

The "reasonableness" requirement demands that officers executing search warrants:

1) Give notice of their authority and purpose, under most circumstances, prior to forcibly entering premises to execute the warrant

2) Take only reasonable action, once inside, to control the premises and prevent the destruction of evidence

3) Conduct the search within the limits set forth in the warrant, and

4) Refrain from seizing items not listed in the warrant (unless there are independent, legal grounds for the seizure).

Each of these requirements has potential impact on computer searches.

The "Knock and Announce" Requirement

To protect safety, and because of a judicial preference for peacable entries based on submission to lawful authority, officers are generally required to knock and announce their identity and purpose before forcibly entering premises to perform a search.[43] This requirement is subject to certain exceptions that allow entry without notice under certain circumstances, including

> ***"Consulting with an expert increases the likelihood of listing thoroughly the items of evidence...."***

when officers have information that an announcement would likely result in the destruction of evidence.[44] The ease and rapidity of destruction of the evidence sought is a factor courts will consider in determining whether a "no-knock" entry was reasonable.[45]

Due to the manner in which it is processed and stored, computerized information is easily and quickly destroyed. Information in the computer's active memory can be instantly destroyed by switching off the machine's power. Information stored on magnetic media (with capacities of thousands of pages) can be quickly erased by exposing the storage device to a magnet. Consequently, when officers know prior to executing a warrant that information has been stored by computer and that persons with a motive to destroy the information are likely present at the place to be searched, an unannounced entry is likely reasonable.[46]

Controlling the Premises

The U.S. Supreme Court has noted that officers executing a search warrant exercise "unquestioned command of the situation."[47] Consequently, officers executing a search warrant have the power to control access to the premises being searched and to control the movement of persons present to facilitate the search and to prevent the removal or destruction of evidence. Because of the ease of destruction of computerized information and the size and complexity of some computer facilities, it will often be reasonable to take full control quickly of the facility to be searched.[48]

Searching Within the Scope of the Warrant

Requiring a particular description of the items to be seized limits the allowable scope of a search in two ways. First, it restricts where an officer may look to only those places where the items sought might reasonably be concealed.[49] Second, it restricts the duration of the search

to the point where either all listed items have been located and seized or until all possible places of concealment have been explored.[50] Failure to comply with either of these restrictions can result in a search that violates the fourth amendment.

A sensible first step is to ensure that all searching officers know the items listed on the warrant.[51] Once on the scene, the officers should carefully restrict the search to the items listed in the warrant.

A problem that frequently arises is that of sorting the items subject to seizure from those that are innocently possessed. This problem is especially common in cases where business records are the target of the search. In all cases, the officers must limit the examination of innocent items to that necessary to determine whether the items are among those listed in the warrant.[52]

A search for documents stored in electronic form by a computer will require use of the computer's display screen to view documents or the computer's printer to print them. A sorting process should be used where each document is briefly examined to determine if it is one of those to be seized, similar to that used to search through "ink on paper" documents.

Obviously, this type of search requires certain operational knowledge regarding computer equipment. For this reason, expert assistance during the search may be essential, especially where efforts have been made to encrypt or conceal the documents.[53]

In general, the sorting process should be performed at the scene of the search to prevent unnecessarily denying the owner access to and use of innocent records. The mere fact that the sorting process is time consuming does not justify a wholesale seizure of all records present.

Nonetheless, certain characteristics of computerized record-keeping support off-site sorting. First, the storage capacity of some computerized systems is so great that review of all documents stored in the system could take a very long time. Second, unlike with paper files, the number of investigators who may assist in the search is limited by the number of computer terminals available for document display. Finally, records stored by computer can usually be quickly duplicated in their computerized form, allowing copies to be left for the owner's use.

> ***"...it is sound practice to disconnect the computer from telephone lines at the outset of the search."***

Officers who anticipate the need to seize a large quantity of computerized documents for sorting at a later time should seek approval from the magistrate when applying for the search warrant. A likely legal concern in this situation is that the innocent documents included in the seized records will be available for unrestrained viewing by investigators, resulting in a postponed "general search." A potential control on such unrestricted viewing is continued judicial supervision of the sorting process.[54]

Disconnecting the Computer from Telephone Lines

The Electronic Communications Privacy Act of 1986 provides that in order to intercept an electronic communication (which includes transmission of words or characters from computer to computer) during its transmission, without the consent of one of the parties to that communication, an officer must obtain an extraordinary court order, similar to that required to lawfully wiretap.[55] Because the computer that is the subject of a search warrant may be connected electronically to others, forbidden interception of electronic communications might result during execution of the warrant. To avoid this, and to ensure that commands to destroy evidence are not transmitted to the computer from a remote location, it is sound practice to disconnect the computer from telephone lines at the outset of the search.

CONCLUSION

Addressing the situations faced by the two officers described at the beginning of this article, the first officer needs to establish factually in his affidavit the probable existence of financial records that are evidence of crime, and to describe particularly those records in the search warrant. The fact that the records may be computerized some-

what complicates the execution of the warrant, and the officer may need to seek expert guidance in order to locate and seize the records in question successfully.

The second officer needs to consider whether the Privacy Protection Act of 1980 permits the use of a search warrant in his case when he is seeking authority to search for items he reasonably believes are, in part, materials prepared for public dissemination that are in the possession of an innocent third party. If the officer determines that a search warrant is appropriate under the circumstances, the officer must then contend with the challenge of communicating to the magistrate how a novel criminal offense has been committed by means of a computer.

As officers approach such challenges, they should carefully adhere to established fourth amendment principles. These principles, coupled with the use of expert assistance where needed, enhance the likelihood of obtaining computerized evidence that is judicially admissible. ✦

Endnotes

[1] Privacy Protection Act of 1980, 42 U.S.C. 2000aa, *et seq.*

[2] 42 U.S.C. 2000aa.

[3] 42 U.S.C. 2000aa-6(e).

[4] 42 U.S.C. 2000aa-6. The statute also provides for award of costs and attorneys fees to a prevailing plaintiff. For a detailed discussion of the act, see Rissler, "The Privacy Protection Act of 1980," *FBI Law Enforcement Bulletin*, February 1981.

[5] Federal law enforcement officers should be aware that the Attorney General, as directed by 42 U.S.C. 2000aa-11, has issued guidelines to assure compliance with the Privacy Protection Act of 1980, which Federal officers must follow to avoid being the subject of disciplinary proceedings. These guidelines are found at 28 CFR Part 59.

[6] 42 U.S.C. 2000aa(a)(1), 2000aa(b)(1).

[7] U.S. Const. amend. IV.

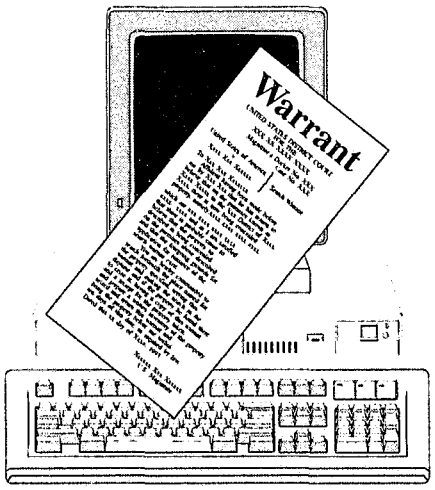
[8] *See Katz* v. *United States*, 389 U.S. 347 (1967).

[9] *Id.* at 357.

[10] *See Michigan* v. *Tyler*, 436 U.S. 499 (1978).

[11] U.S. Const. amend. IV.

[12] *Zurcher* v. *Stanford Daily*, 436 U.S. 547, 556-557 n. 6 (1978), quoting Comment, 28 U. Chi. L. Rev. 664, 687 (1961).



[13] *See, e.g., United States* v. *Morris*, 928 F.2d 504, (2d Cir. 1991), *cert. denied*, 112 S.Ct. 72 (1991) (defendant introduced computer "worm" into national research computer network, shutting down university and government computer systems across the country); *United States* v. *Taylor*, 945 F.2d 1050 (8th Cir. 1991) (defendant accessed American Express computer system by phone and acquired "working" but unissued credit card numbers, which he then used to purchase thousands of dollars worth of merchandise).

[14] An example of an officer successfully obtaining a search warrant in a case where novel technology was being employed to commit the crime of fraud is found in *Ottensmeyer* v. *Chesapeake & Potomac Telephone Co.*, 756 F.2d 986 (4th Cir. 1985).

[15] *See, e.g., United States* v. *Ortiz*, 422 U.S. 891 (1975).

[16] An example of using information provided by experts in affidavits for search warrants is found in *United States* v. *Steerwell Leisure Corp., Inc*, 598 F. Supp. 171 (W.D.N.Y. 1984).

[17] *See United States* v. *Steerwell Leisure Corp., Inc.*, 598 F. Supp. 171 (W.D.N.Y. 1984).

[18] *See, e.g., United States* v. *Truglio*, 731 F.2d 1123 (4th Cir. 1984), *cert. denied*, 469 U.S. 862 (1984).

[19] 959 F.2d 1143 (1st Cir. 1992).

[20] *Id.* at 1149.

[21] *Id.* at 1145.

[22] *Id.* at 1149.

[23] *Id.*

[24] *Illinois* v. *Gates*, 462 U.S. 213, 238 (1983).

[25] *See* Fitzgerald and Eason, *Fundamentals of Data Communication* (John Wiley & Sons, 1978), pp. 42-43.

[26] *Cf. United States* v. *Harvey*, 540 F.2d 1345 (8th Cir. 1976).

[27] *United States* v. *McManus*, 719 F.2d 1395 (6th Cir. 1983).

[28] *Andresen* v. *Maryland*, 427 U.S. 463, 478 n. 9 (1976).

[29] U.S. Const. amend. IV.

[30] *See Marron* v. *United States*, 275 U.S. 192 (1927). For a thorough discussion, *see* 2 W. LaFave, *Search and Seizure*, 95-101 (1978).

[31] An analogous case is *State* v. *Van Wert*, 199 N.W.2d 514 (Minn. 1972).

[32] Equipment components will probably include a central processing unit, printers, terminals (keyboards and display screens), magnetic disk drives, optical disk drives, and magnetic tape drives. Software and manuals are also critical components of an operating computer system and should be included as items to be seized, especially if the officer anticipates operating the system for investigative or evidentiary purposes. Common storage media include magnetic hard disks, floppy disks, and magnetic tapes, as well as optical disks.

[33] *See Andresen* v. *Maryland*, 427 U.S. 463 (1976).

[34] 665 F.2d 1 (1st Cir. 1981).

[35] *Id.* at 4.

[36] *Id.*

[37] *Id.* at 5.

[38] *Id.*

[39] *Id.* at 4.

[40] *Id.* at 5.

[41] An innovative means of limiting the items described to those for which probable cause to search has been established is found in the case *In Re Search Warrant Dated July 4, 1977, Etc.*, 667 F.2d 117 (D.C. Cir. 1981), *cert. denied*, 102 S.Ct. 1971 (1982). Here, the scope of the description of items to be seized was limited to documents related to "the crimes ... which facts recited in the accompanying affidavit make

out." The court, in upholding the warrant, noted with approval the limiting phrase. As was done in this case, it is often desirable to incorporate the affidavit into the warrant by appropriate language and to attach it to the warrant.

[42] *See United States* v. *Truglio*, 731 F.2d 1123 (4th Cir. 1984), *cert. denied*, 469 U.S. 862 (1984). *See also, United States* v. *Offices Known as 50 State Distrib.*, 708 F.2d 1371 (9th cir. 1983), *cert. denied*, 79 L.Ed.2d 677 (1984).

[43] For a thorough discussion, *see* 2 W. LaFave, *Search and Seizure*, 122-140 (1978).

[44] *Id.*

[45] *Id.*

[46] *Id.* The announcement requirement is also less stringently applied where warrants are executed against business premises. *See United States* v. *Francis*, 646 F.2d 251, 258 (6th Cir. 1981), *cert. denied*, 70 L.Ed.2d 616 (1981).

[47] *Michigan* v. *Summers*, 452 U.S. 692, 703 (1981).

[48] An example of such action is found in *United States* v. *Offices Known as 50 State Distrib.*, 708 F.2d 1371 (9th Cir. 1983), *cert denied*, 79 L.Ed.2d 677 (1984).

[49] *Harris* v. *United States*, 331 U.S. 145 (1947).

[50] *Id.* In addition to suppression of evidence, civil liabilityy may result when a search continues after all items named in the warrant have been seized. *See Creamer* v. *Porter*, 754 F.2d 1311 (5th Cir. 1985).

[51] *See In Re Search Warrant dated July 4, 1977, Etc.*, 667 F.2d 117, 123 (D.C.Cir. 1981), *cert. denied*, 102 S.Ct. 1971 (1982) (noting with approval that "[i]n preparation for the search the agents attended several meetings to discuss and familiarize themselves with the areas and documents described in the search warrant and accompanying affidavit. They were instructed to confine themselves to these areas and documents in their search. During the search each agent carried with him a copy of the search warrant and its 'Description of Property' and could contact one of three persons on the scene who carried the supporting affidavit.")

[52] An officer executing a search warrant will frequently need to sort through information to determine what portion of it may be seized pursuant to the warrant. If, during the course of the process, the allowed limited perusal of information is sufficient to cause the officer to conclude that the information is probable evidence of a crime, the officer may lawfully seize the document without obtaining a second warrant under the "plain view" exception provided he can later demonstrate that he was searching reasonably within the limits of the warrant he was executing when he encountered the evidence, and there was probable cause upon proper examination of the item that it was evidence of criminal activity. *Horton* v. *California*, 110 S.Ct. 2301 (1990).

[53] An expert accompanied officers executing the search warrant in *Ottensmeyer* v. *Chesapeake & Potomac Telephone Co.*, 756 F.2d 986 (4th Cir. 1985). Another case considering the role of an expert accompanying officers executing a search warrant is *Forro Precision, Inc.* v. *International Business Machines Corp.*, 673 F.2d 1045 (9th Cir. 1982).

[54] *See United States* v. *Tamura*, 694 F.2d 591 (9th Cir. 1982); *DeMassa* v. *Nunez*, 747 F.2d 1283 (9th Cir. 1984) (special master appointed to supervise sorting of documents during search of attorney's office).

[55] 18 U.S.C. 2511(1).

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

The Bulletin Notes

Law enforcement officers are challenged daily in the performance of their duties; they face each challenge freely and unselfishly while answering the call to duty. In certain instances, their actions warrant special attention from their respective departments. The *Bulletin* also wants to recognize their exemplary service to the law enforcement profession.

Officer Trimbur

Officer Walter Trimbur of the Lower Providence Township, Pennsylvania, Police Department responded to the report of a 17-year-old girl who had stopped breathing. As a relative carried the girl to an awaiting ambulance, Officer Trimbur observed that the victim showed no signs of life and immediately initiated CPR. Within minutes, the victim's pulse returned, and she began to take shallow breaths. The girl was later taken to a medical facility and treated for respiratory arrest resulting from a severe asthma attack.

Sergeant Courtney

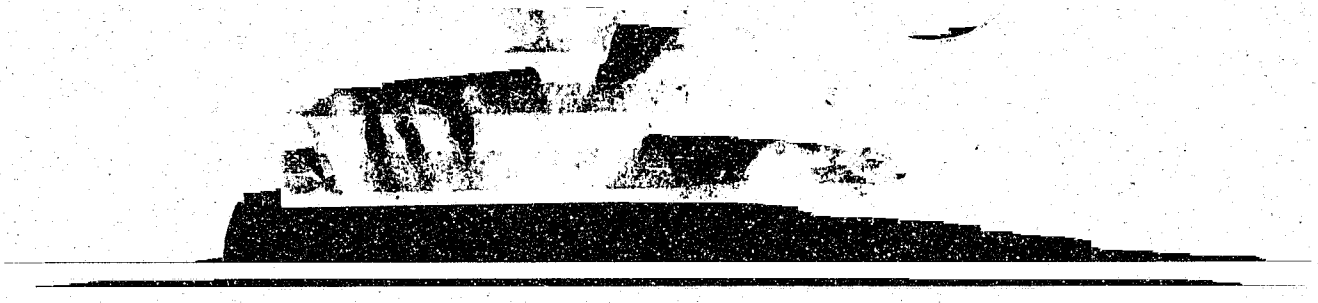
During an early morning traffic stop, a deputy with the San Diego County, California, Sheriff's Department sustained multiple gunshot wounds. After returning fire, the badly injured deputy broadcast descriptive information concerning the fleeing suspect's vehicle. Upon receiving the dispatch, Sergeant Al Courtney of the same department immediately responded to the scene. There, Sergeant Courtney quickly determined the nature of the deputy's injuries and took action to control the bleeding. The wounded deputy was eventually flown to an area medical center, where an attending physician stated that Sergeant Courtney's decisive actions greatly contributed to the survival of his fellow officer.

Detective Sergeant Bivona

Detective Evan

Det. Sgt. Sal Bivona and Det. Mark Evan of the Linden, New Jersey, Police Department joined the pursuit of several armed subjects who had just assaulted the staff of a jewelry store and shot a responding officer. After the subjects abandoned their vehicle following a car chase, Sergeant Bivona and Detective Evan located one of the assailants aiming a gun at a bystander in a residential area. To avoid placing the civilian in danger of being shot during a gun battle and to distract the offender's attention, both stepped out of cover and ordered the subject to drop his weapon. After a tense standoff, the assailant eventually surrendered.

Second Class Mail
Postage and Fees Paid
Federal Bureau of Investigation
ISSN 0014-5688



Patch Call