Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

OS REGISTRY
87-1366X

ROUTING AND RECORD SHEET

SUBJECT: (Optional)
Computer Crime

STAT
STAT
STAT

FROM:
C/ISG

EXTENSION | NO.

DATE
9/18/87

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
~~1. EO~~	~~22 SEP 1987~~	~~22 Sep~~	~~CB~~	
1. D/OS STAT	SEP 1987 22	24 SEP 1987	DL	FYI
2. Registry				file
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

FORM 610 USE PREVIOUS EDITIONS
1-79

☆ U.S. Government Printing Office: 1985—494-834/49156

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

EVIDENTIARY ASPECTS OF COMPUTER CRIME

BY

Stephen C. Gross

Crime in Commerce III: ~~Management~~ Information Systems
For 234
December 18, 1986

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

TABLE OF CONTENTS

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

I. INTRODUCTION

Computers and information systems have permeated today's society to such an extent that there is virtually no sector which does not rely heavily on their use. 1/ As might be expected, computer crime has also expanded, with resulting annual losses incurred, by any measure, enormous. In fact, respondents to an American Bar Association survey of private organizations and public agencies disclosed estimated total annual losses between $145 million and $730 million, highlighting the need for more and better computer crime investigative efforts. 2/ As is true in any investigation or preparation for court trial, the use of evidence is a significant element. In fact, the most likely of the principle defense strategies that will arise in a computer-related crime case will be an attack on the admissibility of computer generated physical evidence. This paper will discuss computer evidence issues based on general law principles and sound investigative procedures, including preventive measures to be considered during all investigative and prosecutive stages. 3/

Initially, the discussion will focus on computer evidence considerations from an investigative perspective. Search and seizure issues will be discussed, as well as procedures used in obtaining computer evidence, computer records and reports as evidence, proper handling and storage of computer evidence, and computer evidence privacy and secrecy considerations. Next, we will address foundational problems encountered in computer crime cases, problems associated with admitting computer records into evidence, and, finally, some practical recommendations for the successful prosecution of computer crime cases.

It is not surprising to see attention focusing on computer crime, considering the power and leverage of computers, the dependence upon them, and their increasing role in society. 4/ Suceeding in combatting the growing threat imposed by bomputer-related crime will depend upon the knowledge and

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

ingenuity of criminal investigators and prosecutors; a proper understanding of computer crime evidence will be crucial to this fight.

II. COMPUTER EVIDENCE CONSIDERATIONS

A. SEARCH AND SEIZURE

As computer technology becomes more accessable, so does the liklihood of computer crime; the computer is quickly becoming "abuser friendly". 5/ Investigators seeking and executing search warrants authorizing the seizure of computers and related computerized information are generally on untested ground since complete judicial guidance is still limited in this area. 6/ They must comply with an 18th century prohibition against "unreasonable searches and seizures" while contending with 20th century electronic technology; an often formidable task. They may sometimes find themselves searching for intangible rather than the ordinary and more familiar types of evidence, such as stolen guns and stock certificates. 7/ Very little has been done to overcome obvious problems in discovery, search warrants, and subpoenas. 8/ Thus, a pandora's box of legal issues becomes available to the defense regarding computer evidence, requiring alert prosecutors to be ever mindful of this potential. Fortunately, those routine issues concerning search and seizure, such as consent, informers, entry, and searches incident to arrest generally will arise and apply much as they would in noncomputer-related cases. 9/ But, what are the necessary steps to take in conducting a successful search and in gathering computer evidence in the non-routine situations?

In general, search warrants should be obtained and used in computer-related crime cases. 10/ Regardless of technological advances, search and seizure by law enforcement officers continues to be governed by the fourth amendment to the U.S. Constitution, protecting the right of the people to be secure against unreasonable Government intrusion. This protection extends to computers and to computer processed information and requires that proper search warrants be

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

obtained prior to legitimate searches. This requirement is applied with special strictness where businesses or residences, the places where computers are most likely to be located, must be entered to perform the search. There must be a showing of probable cause and the warrant must particularly describe the place to be searched and the persons or things to be seized. Unique problems can sometimes arise concerning probable cause and particularity where computers are the search target and will comprise the evidence to be seized. 11/

It is necessary to excercise great care in preparing a search warrant in a computer crime case, due in large part to this being a technical area often new and unfamilier to judges and magistrates. The investigator should have a detailed affidavit which covers all the technical bases, yet is understandable to someone who knows very little or nothing at all about computers. 12/ The difficulties involved in such a task become apparent when one considers the enormity and complexity of the "scene of the crime"in some of the larger business computer centers. For instance, in the litigation involving Equity Funding Corporation of America, thousands of fictitious insurance policies had been created and existed somewhere within a computer memory. At the same time, that particular computer was processing hundreds of thousands of valid insurance policies. 13/

It becomes apparent that one of the first obstacles to be overcome is explaining in an affidavit that certain records being sought may be contained in sophisticated technological equipment. Fortunately, this obstacle is normally easily overcome since the investigator seeking the search warrant can simply state that the information sought may be in electronic or written form, thereby circumventing a non-meaningful description of the computerized information in its encoded form. It is more critical that the information itself be described with particularity, rather than in the form in which it may be found. Also, the storage media which contains the information should be described as concisely as the facts known will allow. 14/

Another hurdle to overcome in establishing probable cause to search is to

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

articulate the necessary facts to show that a crime has actually been committed. In doing so, it is helpful to examine the role played by the computer in the criminal activity and then detailing to the magistrate that such a crime has been committed. The mechanics of the crime should be clear and easily understood. In instances where the crime is unusual or unfamiliar, the investigator should consider using the services of a computer expert.

At this point the investigator must set forth enough facts to convince a magistrate of the probability that evidence of the crime exists at the place to be searched. The legal requirement for recent information is satisfied where the investigator can set forth reliable information that the objects sought were recently observed at the proposed search site. 15/

Although search warrants are preferable in computer-related crime cases, special mention and consideration should also be given to situations providing application of exigent circumstance exceptions to preserve evidence because of the high degree of ease with which both the instruments and fruits of the crime can rapidly destroy or alter the computer evidence. 16/ Because any power interruption will result in the loss of information stored in the computer's internal memory, valuable evidentiary data can be destroyed in the instant it takes to flip a power interruption switch. Also, a magnetic device known as a degausser can instantly erase millions of data characters from a computer tape or disc. Therefore, a "no-knock" entry is reasonable where the investigator reasonably believes that making a pre-entry announcement will result in destruction of the evidence. 17/

The "plain view" doctrine is another possibility, however, this should be used cautiously since there is a strong liklihood that defense attornies will attempt to show the lack of sophistication of most investigators in computer technology. Also, avoid reliance on "expert" informants to point out at the scene what items should be seized. They will generally be insiders and will likely be legally

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

"untested" as an informant. 18/

Overall, investigators should be open to using imagination and ingenuity, as well as their training, to optimize their results in computer related search and seizure situations.

B. OBTAINING COMPUTER EVIDENCE

Evidence in a computer is much more "dense" than in any other information system, in that a single computer tape can contain as much information as a shelf full of books. As an example, in the Equity Funding case alone, approximately 3,000 reels of computer tapes were potential evidence ! 19/ Ensuring that the best evidence for prosecution available at the crime scene is obtained can be both challenging and rewarding for the careful investigator.

When a search is directed towards obtaining documents, they can normally be visually identified and expert knowledge of computer technology is unneccessary. 20/ Documentation practices vary from phenomenally obsessive and complete to non-existent. Ideally, they will thoroughly describe every aspect of the computer system and list each type of output that it produces. 21/ Documents such as systems manuals, computer run books, interpreted punch cards, program documentation logs, data and program input forms, and computer printed forms are usually labeled as to their contents and should be relatively easy to recognize. The completeness and originality of these documents can be determined by careful and complete questioning of those who are most familiar with them. 22/

Recognizing and requesting program documentation is somewhat more difficult and may require knowledge of computer program concepts to understand the types and extent of documentation required, such as source and object listings, flowcharts, test data, and storage dumps. It must also be realized that program documentation is frequently obsolete relative tocurrently used versions and,

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

thus, may necessitate new computer printouts. If the investigator is unsure about what may be obtained or identified, an expert should accompany him on the search. 23/

Taking possession of other computer media materials may be more technically complex. Magnetic tapes and disks will normally have external labels, however, logs and program documentation will normally be necessary to obtain full titles and descriptions of their contents. A trusted technologist may be necessary to check a tape or disk's contents by using a compatable computer and computer program. 24/

Also, where appropriate, consideration should be given to shutting down the operation of the business being searched for a reasonable time to protect the evidence covered by the warrant and to properly sort through the computer documentation. 25/ This sorting process, performed at the scene, can serve to prevent the seizure, and thus the denial of access and use by the owner, of innocent records. The mere fact that the sorting process is time consuming will not necessarily render a wholesale seizure of records reasonable. 26/

C. COMPUTER RECORDS AND REPORTS AS EVIDENCE

Computer records may be divided into two types: (1) computer-stored, where the printout produced from computer storage is a restatement of information or data previously supplied to the computer; and (2) computer-generated, where the computer makes a computation, performs a logical operation, or analyzes the input and other stored data. In judicial proceedings, a distinction appears to be drawn between the two types. It is more difficult to get computer reports containing computer-generated records into evidence. This is probably because computer-stored records are more easily equated with ordinary business records, while computer-generated data involves the complexity of examining the creation of the generated information and the deceptively neat package in which it is displayed. 27/

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

There is no clear-cut answer as to which kind of computer output can or cannot be admissable as evidence, whether from a printer, cathode ray tube, audio response, microfilm, or speech mail. In the case of "Cotton v. John W. Eshelman & Sons, Inc, the court held that computer generated output was admissable, since "our statute was intended to bring the realities of business and professional practice into the courtroom and should not be interpreted so as to destroy its obvious usefulness". Generally, the court will apply the following rules (Business Records Exception to the Hearsay Rule) to evaluate the admissibility of computer output as evidence: (1) that the records were made in the usual course of business, and not merely for the purpose of litigation; (2) it was normal business procedure for an employee with knowledge of the act to make the record; and (3) the record was made at or near the time of the act. 28/

Another possible basis for admission of computer digital-image printouts into evidence is the "Best Evidence Rule". This rule requires that original writing or recording is necessary to prove its own contents; however, if the original is unavailable, then other relevant evidence of its contents is admissable unless the original was lost or destroyed in bad faith. 29/

During the procedure of obtaining and using computer reports as evidence, errors and omissions or malicious intentional acts are possible at each stage of the report-producing process or through nonreal-time program or data modification. It is often not practical to detect or prevent these sufficiently sophisticated intentional acts to alter the reports. Thus, it becomes necessary to take varying degrees of precautions and to invoke the trust of the data processing personnel. Additional confidence in the integrity of the report can be gained by taking the storage medium (tape or disk) to a separate computer center to have its contents printed. Further "independence" can be ensured by verifying that personnel in the new center have no special interest in the work they would be required to do. Throughout the process, independant, trustworthy observers with the skills and knowledge to derermine correct op-

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

erations should observe and supervise all the production steps. 30/

D. STORING AND CARING FOR EVIDENCE

A basic requirement for the admission of evidence is proof that the physical condition of the object is substantially unchanged from its state at the time of seizure. 31/ On the surface, this would not appear to pose any additional problem for computer related evidence than would normally be expected in the handling and storage of regular investigative evidence. However, some types of computer evidence require special care and their storage environments must be controlled, with steps taken to minimize the chance of physical damage from manual handling. Even though most criminal justice agencies normally have acceptable storage facilities for regular types of evidence, these environments may not be suited to computer-related evidence, plus experience in correctly handling computer products may be lacking in their personnel. 32/

Separate types of computer evidence have special needs in their handling and storage. For instance, magnetic tapes and disks should be stored, handled, and transported in hard cover containers. Care should be taken to avoid dropping or squeezing, and no parts of the recording surfaces should be either touched, bent, or creased. The tape reels should be stored vertically in tape storage racks, where room temperatures are between 40 degrees and 90 degrees fahrenheit. Storage life for data retention and recovery is three years. Storage requirements for punch cards and paper tape is similar to that of magnetic tape, except the storage life is indefinite. Special care should be taken to avoid folding, spinning, or knicking edges and tape that might remove paper surfaces should not be used. Computer listings should be stored between binder covers and should not be subjected to strong light. They should

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

be broken into separate pages, unless having them in a continous sheet is important to the case. When storing electronic and mechanical components, it is always wise to consult the manufacturer or owner for special instructions. 33/

Some additional points on the proper handling of computer evidence are also worth mentioning. It is often crucial to a case to specifically identify the location where the physical evidence was acquired. Floor plans, line drawings of the system, and photographs may help in the preparation of the case for court. Lists of the computer evidence and what form it is in - tapes, printouts, cassettes, etc. - are good ideas. Also, the investigator should inscribe computer tapes, disk drives, and print-outs with his personal ID markings. It is appropriate to mark the tapes by writing on the dull side since the first fifteen to twenty feet of tape is "leader" tape and has nothing on it. Identification markings can also be etched on the bottom metal part of a disk pack. Care must be taken in handling these items due to their sensitivity to dust and physical damage. 34/

Finally, to establish that the evidence is substantially unchanged, a complete chain of custody must be readily available. From the initial stages of the search until its completion, careful indexing must be maintained of all the evidence that is seized. 35/

E. PRIVACY AND SECRECY OF EVIDENCE

Issues of personal privacy, trade secrets, or government secrets may sometimes arise since evidence seized in the form of computer media may have data stored that is immaterial to the investigation but that may be confidential to the rightful owner. An obvious consideration would be to ensure that all retrieving and copying on another computer medium contains only that data pertaining to the investigation. In those instances where this is not possible, the investigator should make assurances that any extraneous data will not

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

be revealed and will be stored in a secure manner.

In those situations where consent to release the information is denied by the owner, sufficient safeguards are available in most jurisdictions to minimize the problem. If necessary, a hearing can be held outside the presence of the jury or even " in camera", to allow the court to either overrule the objection or excise the specific objectionable portions. 36/

III. PROSECUTION AND COMPUTER EVIDENCE

As computer technologies and the means for abusing them have rapidly emerged, they have confronted a criminal justice system which is largely uninformed concerning the technical aspects of computerization. Additionally, this system is bound by traditional legal machinery that is often ineffective against unconventional criminal operations. Difficulties in coping with computer abuse arise because a great deal of the property involved does not neatly fit into the categories of property normally considered as subject to abuse or theft. 37/ It becomes obvious that prosecutors face new and demanding challenges in dealing with their fight against computer crime. Their use of computer evidence is clearly a significant element in the preparation of those difficult cases for prosecution and will be addressed as such in this section of the paper. Certain considerations have been mentioned previously, but merit reconsideration from the prosecutor's viewpoint.

A. FOUNDATIONAL PROBLEMS

Before proffered physical evidence can be admitted into trial evidence, certain foundational facts must be proved by the party seeking admission. When these facts are contrasted with the facts sought to be proved by the evidence, a principal defense avenue of attack is opened to which the prosecutor is particularly vulnerable.

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

One of the foundational problems encountered by the prosecutor is that of "authentication" which means, in general terms, being able to introduce evidence sufficient enough to sustain a finding that the written statement or document is, in fact, the writing the prosecutor claims it to be. Thus, it becomes necessary to have testimony from someone who can verify that the purported maker of the document (the computer system that generated the item) is the actual maker. Sufficient evidence should be introduced to convince the judge that the proffered item is authentic; however, it is critical at this stage to not claim more than simply the output process, for instance, that the item was generated by such-and-such computer at such-and-such place and time ....nothing more. The prosecutor significantly compounds the authentication problem if an attempt is made to claim that the item reflects a particular configuration or some internal process within the computer. To do so would allow defense to raise valid objections based on the authentication of the specific computer configurations and processes previously mentioned by prosecution. 38/

As stated earlier in the report, for computer media to be admitted as evidence, they must also qualify as business records which are excepted from the application of the Hearsay Rule. 39/ In a 1977 New Jersey case, Monarch Federal Savings and Loan Association v. Genser, the court delineated the requirements necessary in laying the foundation for business records. In Genser, the court held that personal knowledge testimony regarding the information received into the computer is not required, nor is the preparer required to testify. However, testimony is required of a qualified witness who can testify that the computer records were made in the ordinary course of business, were made contemporaneously, what the sources of the information were, and what was the method of preparation. 40/ Although the Genser decision represented a careful and extensive treatment of the problem of admission of

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

computerized documents into evidence, one should realize that this was only the decision of the court in one jurisdiction; foundational requirements will vary from state to state. 41/

B. EVIDENTIARY PROBLEMS WITH COMPUTER RECORDS

Computer-generated printed evidence produced to show proof in the courtroom must satisfy the Business Record Exception requirements before being admissable as a hearsay exception. Again, the prosecutor is faced with the burden of showing computer reliability, an area of complex technological issues. His best strategy will hinge upon leading a presumably non-technical court to focus upon the legal issues rather than getting lost in technical matterss. 42/ Although some look upon the computer as no more than a big adding machine, it is impossible to look at the phenomenom of computer crime without considering the varied effects of computers on our legal consciousness. 43/ It is important that the prosecutor be prepared to assist the court with prior and understandable case law dealing with the issue at hand. The best response to defense objections on Business Record Exception issues is to focus on the law, particularly the underlying purposes for the law. 44/

The majority of issues within the past few years regarding computer records and the law of evidence have fallen into three basic categories; (1) admissability of computer printouts; (2) computer printouts as the basis of expert testimony; and (3) discovery matters with regard to computer systems.

Of the above categories, admissibility receives the most attention from the courts. The admissability of computer printouts as evidence depends primarily on whether the data from which the report was generated were entered into the system during the normal course of business. If so, the data record and reports produced subsequently in the regular course of business, or even for trial purposes, may be admissable.

Many of the recent court decisions regarding admissibility of computer

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

printouts have addressed foundational requirements and most allowed the admission into evidence of a computer printout. Typically, in United States v. Farris, the the defendant, convicted of failure to file income tax returns, claimed the court had erred by admitting into evidence the output of a computerized data system. The 7th Circuit Court upheld the admission of the records under 28 U.S.C. #1733(b), which allows admission of authorized copies of documents of United States departments as if they were originals.

A 1976 decision bears on issues raised by computer records being used as the basis for expert testimony. In Perma Research and Development v. Singer Co, a breach of contracts civil suit, the defendant objected to the use of the results of computer simulations as a basis for the plaintiffs expert testimony. Although the court admitted that it would have been better for the plaintiff's counsel to have delivered to defense, prior to trial, the details of the underlying data and theorems so as to avoid discussion of their technical nature during trial, it did not charge the trial judge, however, with abuse of discretion for allowing the expert's testimony regarding the results of the computer simulation.

In United States v. Liebert, a discovery issue was raised as to whether pretrial discovery may be used by defense to secure extrinsic evidence to impeach the reliability of a computer printout. Again, the defendant in this case was charged for failure to file tax returns. The IRS computers had no record of the defendant's filing and the defendant requested that his computer expert have access to the IRS Service Center to test the reliability of the IRS data process system; the request was granted. The defendant then requested, for discovery purposes, records of any notices sent to persons stating that the IRS had failed to receive their returns. When the court granted the defendant's request as to a portion of the list of non-filers, the government refused to comply with the court order and the defendant's case was dismissed. On

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

appeal, the dismissal was reversed and theappellate court held that supplying the list requested by the defendant would be unreasonable because of the infringement of the right of privacy of those persons on the list. The IRS's willingness to make available all documents regarding their procedures, operations, and electronic data processing system to discover nonfilers, and their willingness to allow their expert witness to be deposed, was held sufficient to provide the defendant with an opportunity to question the accuracy of the system. 45/

C. PRACTICAL RECOMMENDATIONS

Computer crimes are difficult cases to develop and solve and sometimes require many more resources than most organizations have at their disposal. 46/ Often, legal problems are unavoidable. However, adherence to good investgative methodology, and thorough planning for trial will help the case work flow smoothly. 47/ The practical recommendations that follow, while certainly no panacea, are proven good advice and will enhance the prosecutor's chances of success.

Expert witnesses are often the keys to the admission of evidence in computer criminal trials. Since computer technologists have little or no experience as expert witnesses, they must be carefully "coached" prior to their testimony. It is crucial to keep the computer expert in control and force him to answer questions in court in as few words as possible. One means of achieving thisis to ensure the questions themselves are well formulated so as to elicit brief responses. Remember that good witnesses are those who know what they are talking about and can show that the method of generating the evidence is valid. 48/

Prosecutors should remember that the most likely image that the judge and jury have of computer technology is what they last read on the front page

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

of the newspaper, often a highly sensationalized and distorted recounting of events. It is therefore important to make the case as basic, simple,and free from computer technology and terminology as possible, explaining only those circumstances necessary to present the case. If possible, rely on paper records if they exist rather than introducing computer-generated records. Do not personify or anthromorphize computers in presentations; rather, treat them strictly as inanimate objects, machines, subject to use and manipulation by people. The bottom line, Keep It Simple! 49/

Prosecutors should also attempt to determine the trial judges degree of knowledge and attitude towards computer technology and gear their presentation accordingly. For example, Judge Van Graafeiland of the United States Second Circuit Court of Appeals has said, "As one of the many who have received computerized bills and dunning letters for accounts long since paid, I am not prepared to accept the product of a computer as the equivalent of Holy Writ." 50/ It is, therefore, important to present, and make common knowledge, a convincing argument depicting computerized record keeping as rapidly becoming a normal procedure in the business world.

IV. CONCLUSION

In this paper we have examined several different aspects of evidence in computer crime cases, and the criticality of evidentiary issues to the successful prosecution of computer criminals. Computer crime continues to grow by leaps and bounds, making it imperative that investigators and prosecutors become ever more reliant upon improving their training and skills in this area. In 1980, experts at the Federal Bureau of Investigation estimated that only one of 22,000 computer criminals goes to jail. Further, they estimated that only 1% of all computer crimes is detected, only 14% of that is reported, and only 3% of those cases ever result in jail sentences; clearly leaving

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

room for improvement by the separate law enforcement agencies. 51/

In addressing the different investigative evidentiary considerations, as well as the role of computer evidence in criminal prosecution, we have seen the value of being properly prepared for the investigation, from the initial search to the final court trial, and for careful adherence to established legal principles. We have also observed the apparent need for better training for both investigators and prosecutors in the area of computer crime evidence, as well as the need to better utilize the services and advice of those who are most knowledgeable of computer technology and operations.

In response to a survey by the American Bar Association Task Force on Computer Crime, an executive for a consumer reporting agency appropriately stated: " The most difficult task at present is to educate government so as to make them aware of the computer problem. Law enforcement agencies are not familiar enough with computers and the losses that can occur to properly conduct an investigation and prosecute the perpetrators." 52/ A step in the right direction is the FBI Academy's development of a computer crime course to assist investigators and prosecutors in gaining a better understanding of the technical and legal aspects of computer crime. 53/ Combining the expectation of hard work, friendly patience, access to the FBI computer, and a variety of motivational techniques, the Academy staff has proceeded with efficiency to create a core of law enforcement personnel with a expanded knowledge of computer crime. With this knowledge comes the ability to communicate more directly and meaningfully with the computer experts necessary at the various stages of the investigation and subsequent trial. 54/

Throughout the investigative process, the investigator should be willing to actively seek out the persons who are most knowledgeable of the particular computer regimen in question, to assist in identifying and explaining what

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

evidentiary items are present and how best to handle them. If the computer organization has a security specialist, he can be of great assistance in conducting the investigation. He will likely be very knowledgeable of the computer system and his records could provide significant amounts of evidence that might be used in criminal trial, particularly since they may be exceptions to hearsay evidence rules due to their being produced in the normal course of business. 55/

As Sen. Paul Tribile (R - Va), the leading sponsor of the Computer Fraud and Abuse Act, stated: "It is time to dispel the notion that computer crime is a game or a challenge to be overcome. The fact is, the computer criminal is a law breaker just like any other and deserves to be treated as such." 56/ Understanding and adhering to the proper evidentiary principles in computer crime investigations will undoubtedly assist in that effort.

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

FOOTNOTES

1/ House of Representatives Report 99-753, 99th Congress, 2d Session, Computer Security Act of 1986, August 6, 1986, p.1.

2/ House of Representatives Report 99-894, 98th Congress, 2d Session, Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, July 24, 1984,p.9.

3/ National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration, U.S. Department of Justice, Computer Crime-Criminal Justice Resource Manual, (Washington, D.C.: Government Offices, 1979), p.100.

4/ Donn Parker, Fighting Computer Crime, (New York: Charles Scribner's Sons, 1983), p.x .

5/ J.J. Bloombecker, "New Federal law Bolsters Computer Security Efforts", Computerworld, October 27, 1986,pp. 64-66.

6/ John Sauls, "Raiding the Computer Room, Fourth Amendment Considerations (Conclusion)," FBI Law Enforcement Bulletin, June 1986,pp. 24-30.

7/ John Sauls, "Raiding the Computer Room, Fourth Amendment Considerations (Part I)", FBI Law Enforcement Bulletin, May 1986, pp. 25-30.

8/ Task Force On Computer Crime, Section of Criminal Justice, American Bar Association, Report on Computer Crime, (Washington, D.C.: Government Printing Office, 1984), pp. II-8.

9/ National Criminal Justice Information and Statistics Service...., p.100.

10/ National Criminal Justice Information and Statistics Service...., p. 100.

11/ Sauls (Part I), p. 26.

12/ J.J.Becker, The Investigation of Computer Crime, An Operational Guide to White Collar Crime Enforcement, (Washington, D.C.: Government Printing Office, April 1980), p. 24.

13/ J.J. Becker, "Programmed For Crime", Los Angeles Lawyer, November 1979, pp. 16-31.

14/ Sauls (Conclusion), pp. 24-25.

15/ Sauls (Part I), pp. 26-29.

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

16/ National Criminal Justice Information and Statistics Service...., p. 27.

17/ Sauls (Conclusion), p. 27.

18/ National Criminal Justice Information and Statistics Service...., p. 100.

19/ Becker, The Investigation of Computer Crime...., p. 19.

20/ National Criminal Justice Information and Statistics Service....,p.101.

21/ Becker, The Investigation of Computer Crime...., p. 14.

22/ National Criminal Justice Information and Statistics Service...., p. 101.

23/ National Criminal Justice Information and Statistics Service...., p.10.

24/ National Criminal Justice Information and Statistics Service...., p.102.

25/ Becker, The Investigation of Computer Crime...., p. 25.

26/ Sauls (Conclusion), p. 29.

27/ James Vergari, "Evidential Value and Acceptability of Computer Digital - Image Printouts", Rutgers Computers and Technology Law Journal, Vol 9, (1984), p. 346.

28/ Chi K.L. Lam, "Can Computer Output Be Evidence?", The EDP Auditor, Journal of the Auditor's Foundation, Fall 1982, p.43.

29/ Vergari, p.347.

30/ National Criminal Justice Information andStatistics Servece...., p.110.

31/ Becker, The Investigation of Computer Crime...., p. 27.

32/ National Criminal Justice Information and Statistics Service...., p. 111.

33/ Bruce Goldstein, A Focket Guide to Computer Crime Investigation, (Madison, Wisconsin: Assets Protection, 1981), pp. 17-18.

34/ Goldstein, p. 15.

35/ Becker, The Investigation of Computer Crime...., p.112.

36/ National Criminal Justice Information and Statistics Service...., p. 112.

37/ House of Representatives Report 99-894...p. 9.

38/ NationalCriminal Justice Information and Statistics Service...., p. 113.

39/ Becker, The Investigation of Computer Crime...., p.30.

40/ National Criminal Justice Information and Statistics Service...., p.121.

41/ Becker, The Investigation of Computer Crime...., p. 30.

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

42/ National Criminal Justice Information and Statistics Service...,p.117.

43/ Becker, "Programmed For Crime"..., p.66.

44/ National Criminal Justice Information and Statistics Service..., p. 116.

45/ National Criminal Justice Information and Statistics Service...., p.124.

46/ Goldstein, p.5.

47/ Lam, p. 57.

48/ National Criminal Justice Information and Statistics Service...., p. 124.

49/ National Criminal Justice Information and Statistics Service...., p.125.

50/ Lam, p.52.

51/ Becker, The Investigation of Computer Crime...., p.6.

52/ Task Force on Computer Crime...., p.5.

53/ Glenn McLoughlin, "Computer Crime and Security Updated", Issue Brief, Congressional Research Service, Library of Congress, September 15, 1986, p. 9.

54/ J.J. Becker, "Computer Crime Fighters.... Go To Boot Camp At FBI Academy", Security World, September 1978, pp. 30-31.

55/ National Criminal Justice Service Information and Statistics Service..., p. 102.

56/ Kevin Power, "Congress Approves Law to Combat Computer Crime", GCN, October 24, 1986, p. 5.

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

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.

(Published by the Federal Bureau of Investigation, U.S. Department of Justice)
Reprinted from the FBI **Law Enforcement Bulletin**, May, and June 1986.

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

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-

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

"... 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]

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

"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

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

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-

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

"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.

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

"... the legal standard by which ... searches and seizures [of computers and computerized information] will be measured is the same as is applied to searches less concerned with modern technology."

Part I of this article examined the fourth amendment's requirements of establishing probable cause and particularly describing the items to be seized in affidavits which support warrants to search and seize computers and computer-processed information. Part I concluded with the particular description of computer equipment. Part II continues with a consideration of the particularity requirement as applied to computerized information and a discussion of fourth amendment standards regarding execution of search warrants on computer facilities.

Describing Computer-Processed Information

Officers seeking to describe particularly information that has been processed by a computer face two significant obstacles. The first obstacle is explaining in an affidavit for a search warrant that records being sought may be contained in sophisticated technological equipment. For example, digital computer systems store and process information in the form of electronic impulses.[47] For these purposes, this information is encoded into the binary number system, a "language" comprised only of the characters zero and one.[48] Since, for the officer seeking authority to search and seize and the court reviewing his application, "information (either numbers or text) in binary form is useless unless it can be decoded,"[49] describing computerized information in its encoded form is not meaningful. Fortunately, therefore, for officers drafting search warrant applications, this first obstacle is easily overcome, since officers are not required to confront the technological realities of what occurs when information is transformed into an electronic record. They can simply state that the information sought may be in electronic or written form.

It is the information itself that must be described with particularity, rather than the form in which the information may be found. Thus, if what is sought is "a letter from John Jones to Bill Smith dated November 9, 1985, and concerning the ownership of 200 shares of IBM stock," the letter should be described in those specific terms. The descriptive problem regarding whether the letter should be found in the form of paper with writing on it or magnetic tape electronically inscribed with binary code is solved by using more general terms. Concluding the description of the letter and similar items with the statement that "the records sought are 'written or electronic' " should be sufficient to permit lawful

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

seizures of the documents in either form, if the *information* sought is itself (as in the letter example) described with sufficient detail.[50] As previously noted, the storage media (magnetic discs, etc.) which could contain the information in electronic form should also be described as concisely as the facts known will allow.

The more-difficult obstacle then is particularly describing the information which is the object of the search. Information, whether recorded in written or electronic form, is generally collected into documents. Documents are what officers usually describe in warrants authorizing the seizure of information. Because the particularity requirement is strictly applied where documents are concerned,[51] the descriptive task is often a demanding one. Nonetheless, courts reviewing applications for search warrants evaluate the particularity of the description of a document in light of the degree of precision the facts of a case will allow.[52] The officer must be as precise as possible in describing a document, consistent with the facts that are available to him. The detailed description is required whether the information is computerized or not.

For example, in the *United States* v. *Timpani,*[53] a search warrant authorizing the seizure of "... any and all records relating to extortionate credit transactions (loansharking) ..."[54] 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 ..."[55]) 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, identifiable crime [of loansharking]."[56] Approving the particularity of the warrant, the court stated, "... most important, it is difficult to see how the search warrant could have been made more precise."[57]

The task of the officer is to describe the information sought with sufficient particularity to avoid a forbidden "general" warrant. If he is aware of specific documents sought, he should designate them by type (letter, memo, etc.), date, subject, author, addressee, providing as much detail as possible. The earlier description of the letter regarding ownership of IBM stock is an example of this technique.

Where 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 use of a general description that is 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. This qualifying standard is known as a limiting phrase.

The limiting phrase 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 ef-

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

"... it is often desirable to incorporate the affidavit into the warrant by appropriate language and to attach the affidavit to the warrant."

fective. 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)...."[58] 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. The warrant may not 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 gambling—that is specifically set out [in the affidavit]."[59] 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.

In *Application of Lafayette Academy, Inc.*,[60] a case involving a search for computerized information, the information sought was described in general terms with the inclusion of a limiting phrase, but the phrase was not made sufficiently narrow. Lafayette Academy, Inc., was being investigated for fraudulent activities in connection with their participation in the Federally Insured Student Loan Program (FISLP). The warrant authorized seizure of "books, papers, rosters of students, letters, correspondence, documents, memoranda, contracts, agreements, ledgers, worksheets, books of account, student files, file jackets and contents, computer tapes/discs, computer operation manuals, computer tape logs, computer tape layouts, computer tape printouts, Office of Education (HEW) documents and forms ... which constitute evidence of the commission of violations of the laws of the United States, that is violations of 18 U.S.C. Sections 286, 287, 371, 1001, and 1014...."[61] The probable cause in this case related to frauds pertaining to the FISLP. The court, in invalidating the search warrant, criticized the limiting phrase because it allowed seizure of items for crimes beyond the scope of the probable cause established. The court stated, "[t]he warrant is framed to allow seizure of most every sort of book or paper at the described premises, limited only by the qualification that the seized item by evidence of violations of 'the laws of the United States, that is violations of 18 U.S.C. Sections 286, 287, 371, 1001, and 1014.' The cited statutes, however, penalize a very wide range of frauds and conspiracies. They are not limited to frauds pertaining to FISLP, and there is no indication from the warrant that the violations of federal law as to which evidence is being sought stem only or indeed at all from Lafayette's participation in FISLP. Thus, the warrant purports to authorize not just a search and seizure of FISLP-related records as the government contends but a general rummaging for evidence of any type of federal conspiracy or fraud."[62] The court continued that "... the precise nature of the fraud and conspiracy offenses for evidence of which the search was authorized—fraud and conspiracy in the FISLP—needed to be stated in order to delimit the broad categories of documentary material and thus meet the particularity requirement...."[63]

Occasionally, the nature of the probable cause will allow a very broad description. In *United States* v. *Brien*,[64] a search warrant was issued for the premises of Lloyd, Carr & Company, a commodities brokerage firm. The warrant authorized the seizure of "Lloyd, Carr's bank statements, cash receipt books, option purchase records, sales material distributed to customers, employee compensation records, customer account records, sales training material and customer lists."[65] Noting that the described items constituted most of the business records of the company, the court nonetheless upheld the warrant's particularity, since the affidavit's facts "... warranted a strong belief that Lloyd, Carr's operation was, solely and entirely, a scheme to defraud...."[66] Since the facts in the affidavit established that *all* of the records of the business probably were evidence of the crime being investigated, the scope of the description was sufficiently particular. In upholding the validity of the warrant, the court stated, "... where there is probable cause to find that there exists a pervasive scheme to defraud, all the business records of an enterprise may be seized, if they are, as here, accurately described so that the executing officers have no need to exercise their own judgment as to what should be seized."[67]

The items to be seized should be described as precisely as the facts will allow, and items for which probable cause to search has not been established should not be included. 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.*[68] 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

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

make out...."[69] 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 the affidavit to the warrant. Officers preparing search warrants for computerized information should consider the use of this procedure.

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 a search warrant is executed.[70] For the search to be lawful, it must be done in a reasonable manner.[71] The U.S. Supreme Court has recognized the flexibility of this standard, stating "[t]here is no formula for the determination of reasonableness. Each case is to be decided on its own facts and circumstances."[72] Perhaps because of the vagueness of this standard, certain statutes also regulate the action of officers executing search warrants.[73]

Generally, officers must give notice of their authority and purpose prior to entering premises to execute a search warrant.[74] Once inside, the actions taken to secure control of the premises and prevent destruction of evidence must be reasonable under the circumstances.[75] The search itself must be performed within the scope of the warrant,[76] and care must be taken to cause no unnecessary damage during the search.[77] Finally, only items named in the search warrant may be seized, subject to a limited exception, the "plain view" doctrine.[78] These aspects of execution will be examined as they relate to computer searches.

The Announcement Requirement

To protect the privacy interests of citizens and the safety of both occupants of premises and the officers making entry to execute a warrant, officers are generally required to knock and announce their identity and purpose before forcibly entering premises to perform a search.[79] This requirement is subject to certain exceptions which allow entry without notice under some circumstances.[80] The exceptions include situations where the announcement would jeopardize the safety of the officers or others and where it would likely result in the destruction of evidence.[81] This latter exception, destruction of evidence, becomes relevant in searching for computer-processed information.

Due to the manner in which it is processed and stored, computerized information is easily and quickly destroyed. As previously discussed, information is encoded into the binary number system for processing purposes. This encoded information may then be stored in the computer's internal memory or on magnetic or other external storage media.[82] Generally, the internal memory is used to store data that must be immediately accessible to perform the tasks for which the computer is presently being used. Because any power interruption will result in the loss of information stored in the computer's internal memory, important information is usually duplicated and stored on an external storage device, such as a magnetic tape or disc. Information that is in the computer's internal memory that has not been "backed-up" by more permanent external storage may be destroyed in the instant it takes to flip a power interruption switch. Depending on the memory capacity of the computer, a considerable amount of information may be lost in this manner. Personal computers with internal storage capacities equal to 200 double-spaced typewritten pages are now common, and larger computers have much greater internal memory capacity. Information stored externally, especially if a magnetic storage medium is used, is likewise subject to rapid destruction. A device known as a degausser can instantly erase millions of data characters from a tape or disc.[83]

A pre-entry announcement is not required where officers know facts that cause them to reasonably believe that the making of an announcement will result in the destruction of evidence.[84] 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.[85] Consequently, where officers know prior to execution of a warrant that information sought 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.[86]

The announcement requirement is less stringently applied where warrants are executed against business premises.[87] Since computers are often located at businesses, this fact should also be considered in determining whether a pre-entry announcement is required.

Another alternative to the announced entry may exist when searching for processed data. Where computerized information is the target of the search, technology may allow the execution of the search without any physical entry. If the computer is one where access is available to persons with remote terminals via telephone lines, it is possible that the information sought

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

"Investigators executing a search warrant must use care to insure that the search is restricted to places where the items to be seized may be concealed."

may be obtained by an expert who "breaks in" the system remotely, using his own terminal and telephone.[88] Also, the electronic operations of some computer systems may be observed from as far away as one-half mile if the proper equipment is used.[89] Presumably, where no physical entry takes place, no announcement is required. Such searches do, however, fall within the application of the fourth amendment and its attendant requirements,[90] and in most cases, a search warrant will be required for performing such a search.[91] Additionally, some sort of notice to the operator of the computer that a search has been performed is likely required.[92]

Controlling The Premises

The U.S. Supreme Court has noted the utility of officers who are executing a search warrant exercising "unquestioned command of the situation."[93] Consequently, officers executing a search warrant have the power to control access to the premises being searched and to control the movements of persons present to facilitate the search and to prevent the removal or destruction of evidence. Due to the previously noted ease of destruction of computerized information and the size and complexity of some computer facilities, the need likely will exist to quickly take control of a computer facility being searched. Actions taken to control the premises and prevent the destruction of evidence will be evaluated based upon the reasonableness of the actions under the circumstances.

An example of this analysis is found in *United States* v. *Offices Known as 50 State Distrib.*,[94] where a search warrant was executed on a building housing a large "boiler room" sales operation that was engaged in fraud and misrepresentation in selling its promotional merchandise. About 50 local and Federal officers entered the premises to perform the search. At least 300 employees were present. The warrant authorized the seizure of almost all business records present. Upon entry, the officers required all persons present to remain at desks or in their assigned work areas. No one was permitted to go to the restroom without an escort. The court, in upholding the validity of the execution of the warrant, noted, "[t]he breadth of the warrant ... rendered the execution of the warrant a most difficult task at best. Some control over the 300 ... employees was necessary for an orderly search."[95]

Searching Within The Scope Of The Warrant

The requirement of a particular description of the items to be seized limits the allowable scope of a search in two ways. First, it restricts the places where an officer may look. An officer may look only in places where the item sought might reasonably be concealed.[96] Second, it restricts the time of execution. An officer may only search under the authority of the warrant until all named items have been located or seized or until all possible places of concealment have been explored.[97] Failure to comply with either of these restrictions can result in an illegal, general search that violates the fourth amendment.

Investigators executing a search warrant must use care to insure that the search is restricted to places where the items to be seized may be concealed. This can be quite difficult where records are sought and a great number of files are present. Regardless of the difficulty, reasonable steps must be taken to ensure that the search is no broader than authorized by the warrant.

A sensible first step is to make sure that all searching officers are aware of what items are listed in the warrant. In upholding the execution of the warrant in *In Re Search Warrant dated July 4, 1977 Etc.*, the court noted the procedure followed in that case, saying, "[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."[98] In upholding a warrant execution in *United States* v. *Slocum*,[99] the court also noted a pre-execution meeting.[100] Familiarizing the search team with the language of the warrant will increase the likelihood that a search will be performed in a manner a court will deem reasonable.

Once on the scene, the officers should continue to use care to 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, officers must restrict their search to places where the items named in the warrant are likely to be found and to limit the examination of innocent items to an extent no greater than that necessary to deter-

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

mine whether the item being examined is one of the items named in the warrant.[101] Again, the yardstick is reasonableness.

In many cases, a simple sorting process will be upheld as reasonable.[102] In *United States* v. *Slocum*, a warrant authorizing the seizure of business records related to illegal importation of tropical birds was executed. The U.S. Court of Appeals for the 11th Circuit described the execution process as follows: "... [T]he offices were a shambles and ... there was no apparent filing system; it was therefore concluded that it would be necessary to view each document to determine if it fell within the warrant. When an agent discovered a document that he or she believed covered by the warrant, the document was taken to one of four supervising agents who made the ultimate decision whether to seize the document."[103] The court approved use of "a common sense standard"[104] in evaluating the reasonableness of the search method and noted that where a warrant authorizes the seizure of documents, "some perusal, generally fairly brief, was necessary in order for police to perceive the relevance of the documents to the crime."[105] The court cautioned, however, that "the perusal must cease at the point of which the warrant's inapplicability to each document is clear."[106]

In Re Search Warrant Dated July 4, 1977, Etc. also concerned the execution of a search warrant requiring the examination of a multitude of documents. Fifteen agents conducted a search which lasted 9½ hours, during which they examined the contents of 93 file drawers, 14 desks, 3 bookshelves, and numerous boxes and piles of loose documents. The court described a systematic search where each document encountered was evaluated by search personnel to determine whether it fell within the description of items to be seized contained in the warrant. The U.S. Circuit Court of Appeals for the District of Columbia Circuit, in upholding the reasonableness of the search, noted that nothing in the record indicated a "general rummaging operation"[107] had taken place and that the agents involved in the search had been "... extensively briefed, instructed and supervised."[108]

Search for documents stored in electronic form by a computer will require use of the computer to view documents on a display screen or to print them by means of a printer. A sorting process similar to that employed in a search for "ink on paper" documents would seem reasonable under the circumstances. Such a sorting process was employed in *United States* v. *Harvey*.[109] There, an agent seeking, pursuant to a search warrant, an electronic device that produced telephone switching tones discovered some cassette audio tapes. He played about 12 of the tapes on a cassette player on the scene and determined that 2 contained recorded telephone switching tones. These tapes were seized. The U.S. Court of Appeals for the Eighth Circuit held these tapes were "properly seized as within the limitations of the warrant."[110] Use of computer equipment to examine computerized records should likewise be reasonable, since the records are otherwise incomprehensible to the searchers. Obviously, certain operational knowledge regarding the computer equipment will be required to perform this type of search. Under these circumstances, expert assistance during the search may be essential.[111]

The sorting process, performed at the scene of the search, serves to prevent the seizure, and thus the denial of access and use by the owner, of innocent records. The mere fact that the sorting process is time consuming will not make a wholesale seizure of records reasonable. Obviously, where a valid warrant authorizes the seizure of all business records, no sorting is required other than the elimination of nonbusiness records.[112] Otherwise, the reasonableness standard may require an arduous sorting process. Thus, where agents seized 11 cardboard boxes of computer printouts which were bound in 2000-page volumes, 34 file drawers of vouchers bound in 2000-page volumes, and 17 drawers of cancelled checks and hauled these records to another location where they sifted through them to extract the relevant documents (that were described in the search warrant) as a consequence of their determination that sorting at the site of the search would take a very long time, the seizure was held to be an unreasonable one.[113] Sorting at the scene of the search is generally required.

Certain characteristics of computerized recordkeeping may result in different treatment for computerized records.[114] First, the storage capacity of some computerized systems is such 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, where the records are stored magnetically, they may be quickly duplicated in their computerized form. Based on these considerations, it may be reasonable in some cases to duplicate the records quickly, leave copies for the use of the owner of the records, and seize the original records for later examination.

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

The likely legal concern in this situation is that the innocent documents included in the records would be available for unrestrained viewing by investigators resulting in a postponed "general search." A potential control for this problem would be continuing judicial supervision of the sorting process.[115]

Finally, when all items named in a warrant have been located and seized, the warrant provides no authority to continue the search.[116] Absent other legal justification, the search must terminate.

Avoiding Damage During a Search

A further requirement for the reasonable execution of a warrant is that the officers take care to avoid unnecessary damage to the property being searched and seized. Since computers are complex and fragile,[117] considerable care must be exercised where one is seized. Expert assistance may be necessary to ensure a damage-free seizure.

The "Plain View" Doctrine

As previously noted, 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, he is not required to leave the document behind, even through it is not described in the warrant. He may seize it under the "plain view" exception to the warrant requirement provided that he is lawfully present (searching reasonably within the scope of the warrant), it is readily apparent that the document is evidence, and the discovery of the document is "inadvertent" (that is, the officer did not possess probable cause to search for the document prior to beginning the search he is presently engaged in).[118]

CONCLUSION

Since judicial guidance is still limited in the area, investigators seeking and executing search warrants authorizing the seizure of computers and computerized information are on untested ground. However, the legal standard by which such searches and seizures will be measured is the same as is applied to searches less concerned with modern technology. Careful adherence to established fourth amendment principles, coupled with the use of expert assistance where needed, will enhance the likelihood of obtaining computerized evidence that is judicially admissible.

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).
[47]14 *Am. Jur. Proof of Facts 2d* 183 (1977).
[48]*Id. See also King* v. *State ex rel Murdock Acceptance Corporation*, 222 So.2d 393, 398 (1969).
[49]*Id.* at 184.
[50]*See United States* v. *Truglio*, 731 F.2d 1123 (4th Cir. 1984), *cert. denied*, 83 L.Ed.2d 130 (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).
[51]*See Andresen* v. *Maryland*, 427 U.S. 463 (1976).
[52]For a thorough discussion, see Rissler, "Documentary Search Warrants," *FBI Law Enforcement Bulletin*, vol. 49, No. 7, July 1980, pp. 27–31.
[53]665 F.2d 1 (1st Cir. 1981).
[54]*Id.* at 4.
[55]*Id.*
[56]*Id.* at 5.
[57]*Id.*
[58]*Id.* at 4.
[59]*Id.* at 5.
[60]610 F.2d 1 (1st Cir. 1979).
[61]*Id.* at 3.
[62]*Id.*
[63]*Id.* at 3, 4.
[64]617 F.2d 299 (1st Cir. 1980), *cert. denied* 446 U.S. 919 (1980).
[65]*Id.* at 306.
[66]*Id.* at 308.
[67]*Id.* at 309, *contra Voss* v. *Bergsgaard*, 774 F.2d 402 (10th Cir. 1985).
[68]667 F.2d 117 (D.C. Cir. 1981), *cert. denied*, 102 S.Ct. 1971 (1982).
[69]*Id.* at 141.
[70]*Go-Bart Importing Company* v. *United States*, 75 L.Ed. 374 (1931).
[71]*Id.*
[58]*Id.* at 382.

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7

[73]An example is 18 U.S.C. §3109.

[74]*Cf. Ker v. California*, 374 U.S. 23 (1963) (concerning an entry to arrest). For a thorough discussion, see 2 W. LaFave, *Search and Seizure*, 122–140 (1978).

[75]*See United States v. Offices Known as 50 State Distrib.*, *supra* note 50.

[76]*Cf. Harris v. United States*, 331 U.S. 145 (1947). For a thorough discussion, see 2 W. LaFave, *Search and Seizure* 160–163 (1978).

[77]See 2 W. LaFave, *Search and Seizure* 161 (1978).

[78]*See Coolidge v. New Hampshire*, 403 U.S. 443 (1971). For a thorough discussion, see 2 W. LaFave, *Search and Seizure* 163–184 (1978).

[79]*Supra* note 74.

[80]*Id.*

[81]*Id.*

[82]See generally 16 *Am Jur. Proof of Facts* 285–291 (1965).

[83]D. Parker, *Fighting Computer Crime*, page 42 (Charles Scribner's Sons, 1983).

[84]*Supra* note 74.

[85]*Id.*

[86]*Id.*

[87]*See United States v. Francis*, 646 F.2d 251, 258 (6th Cir. 1981), *cert. denied*, 70 L.Ed.2d 616 (1981).

[88]For a discussion of the ease with which an expert can gain access to a supposedly secure system, see T. Whiteside, *Computer Capers*, pp. 117–121 (1978).

[89]T. Schabeck, *Computer Crime Investigation Manual*, section 9.2.9 (Assets Protection, 1980).

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

[91]*Id.*,

[92]*See Berger v. New York*, 388 U.S. 41 (1967).

[93]*Michigan v. Summers*, 452 U.S. 692, 703 (1981), citing 2 W. LaFave, *Search and Seizure* 150–151 (1978).

[94]*See United States v. Offices Known as 50 State Distrib.*, *supra* note 50.

[95]*Id.* at 1376.

[96]*Supra* note 76.

[97]*Id.*

[98]*Supra* note 68, at 123.

[99]708 F.2d 587 (11th Cir. 1983).

[100]*Id.* at 601.

[101]See generally 2 W. LaFave, *Search and Seizure* 173–178 (1978).

[102]*See, e.g., In Re Search Warrant Dated July 4, 1977. Etc.*, *supra* note 68. *See also United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982).

[103]708 F.2d 587, 602 (11th Cir. 1983).

[104]*Id.* at 604.

[105]*Id.*

[106]*Id.*

[107]*Supra* note 68, at 124.

[108]*Id.*

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

[110]*Id.* at 1354.

[111]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).

[112]*See United States v. Brien*, *supra* note 64.

[113]*United States v. Tamura*, *supra* note 102.

[114]*See e.g., United States v. Tamura*, *supra* note 102.

[115]*Id. See also DeMassa v. Nunez*, 747 F.2d 1283 (9th Cir. 1984) (special master appointed to supervise sorting of documents during search of attorney's office).

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

[117]For a discussion of the ways a computer may be physically damaged, see *Fighting Computer Crime*, *supra* note 82, pages 41–42.

[118]*Supra* note 78.

Declassified in Part - Sanitized Copy Approved for Release 2011/12/02 : CIA-RDP89B01356R000100140025-7