US Department of Justice
Criminal Division
Office of Professional Development and Training

FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS

JULY 1994

PREFACE

These Guidelines are the product of an interagency group, informally called the Computer Search and Seizure Working Group. Its members were lawyers, agents, and technical experts from the Federal Bureau of Investigation; the United States Secret Service; the Internal Revenue Service; the Drug Enforcement Administration; the United States Customs Service; the Bureau of Alcohol, Tobacco, and Firearms; the United States Air Force; the Department of Justice; and United States Attorneys' offices. Most of us have consulted widely within our own agencies to find the diversity of opinion on these topics. Our object was to offer some systematic guidance to all federal agents and attorneys as they wrestle with cases in this emerging area of the law. These Guidelines have not been officially adopted by any of the agencies, and are intended only as assistance, not as authority. They have no regulatory effect, and confer no right or remedy on anyone. Moreover, the facts of any particular case may require you to deviate from the methods we generally recommend, or may even demand that you try a completely new approach.

Many of our recommendations must be tentative, because there is often so little law directly on point. As the law develops and as technology changes (thereby altering or even transforming our assumptions), the Working Group may well find itself a Standing Committee with open membership.

If you have any comments, corrections, or contributions, please contact Marty Stansell-Gamm at the Computer Crime Unit, General Litigation Section, Department of Justice (202-514-1026). As you confront these issues in your practice, we will be eager to hear about your experience and to assist in any way we can.

Scott C. Charney, Chief, Computer Crime Unit

Martha J. Stansell-Gamm
Computer Crime Unit
Chair, Computer Search and Seizure Working Group

General Litigation and Legal Advice Section Criminal Division Department of Justice

TABLE OF CONTENTS

INTRODUCTION 1

I. KEY TERMS AND CONCEPTS

A. DEFINITIONS 3
B. LIST OF COMPUTER SYSTEM COMPONENTS 5
C. DETERMINING THE COMPUTER'S ROLE IN THE OFFENSE 7

II. GENERAL PRINCIPLES

A. SEARCH WARRANTS 9
B. PLAIN VIEW 9
C. EXIGENT CIRCUMSTANCES 9
D. BORDER SEARCHES 12
E. CONSENT SEARCHES 13
1. Scope of the Consent 13
2. Third-Party Consent 14
a. General Rules 14
b. Spouses 17
c. Parents 17
d. Employers 18
e. Networks: System Administrators 22

F. INFORMANTS AND UNDERCOVER AGENTS 24

[page ii]

III. SEIZING HARDWARE
A. THE INDEPENDENT COMPONENT DOCTRINE 25
B. HARDWARE AS CONTRABAND OR FRUITS OF CRIME 26

1. Authority for Seizing Contraband or Fruits of Crime 26
2. Contraband and Fruits of Crime Defined 27

C. HARDWARE AS AN INSTRUMENTALITY OF THE OFFENSE 28

1. Authority for Seizing Instrumentalities 28
2. Instrumentalities Defined 28

D. HARDWARE AS EVIDENCE OF AN OFFENSE 30

1. Authority for Seizing Evidence 30
2. Evidence Defined 30

E. TRANSPORTING HARDWARE FROM THE SCENE 31

IV. SEARCHING FOR AND SEIZING INFORMATION

A. INTRODUCTION 35
B. INFORMATION AS CONTRABAND 36
C. INFORMATION AS AN INSTRUMENTALITY 36
D. INFORMATION AS EVIDENCE 37
1. Evidence of Identity 38
2. Specific Types of Evidence 39
a. Hard Copy Printouts 39
b. Handwritten Notes 40

E. PRIVILEGED AND CONFIDENTIAL INFORMATION 40

1. In General 40
a. Doctors, Lawyers, and Clergy 41
b. Publishers and Authors 41
2. Targets 42
3. Using Special Masters 43

[page iii]

F. UNDERSTANDING WHERE THE EVIDENCE MIGHT BE: STAND-ALONE PCs, NETWORKS AND FILE-SERVERS, BACKUPS, ELECTRONIC BULLETIN BOARDS, AND ELECTRONIC MAIL..... 43

1. Stand-Alone PCs..... 43

a. Input/Output Devices: Do Monitors, Modems, Printers, and Keyboards Ever Need to be Searched? 44
b. Routine Data Backups..... 46
2. Networked PCs..... 46
a. Routine Backups 48
b. Disaster Backups..... 49

G. SEARCHING FOR INFORMATION 49
1. Business Records and Other Documents 49
2. Data Created or Maintained by Targets 50
3. Limited Data Searches 51
4. Discovering the Unexpected 53
a. Items Different from the Description in the Warrant .. 53
b. Encryption 54

H. DECIDING WHETHER TO CONDUCT THE SEARCH ON-SITE OR TO

REMOVE HARDWARE TO ANOTHER LOCATION 55
1. Seizing Computers because of the Volume of Evidence 56
a. Broad Warrant Authorizes Voluminous Seizure of Document. 56
b. Warrant is Narrowly Drawn but Number of Documents to be Sifted through is Enormous 58
c. Warrant Executed in the Home 59
d. Applying Existing Rules to Computers 60

2. Seizing Computers because of Technical Concerns 61

a. Conducting a Controlled Search to Avoid Destroying Data 61
b. Seizing Hardware and Documentation so the System Will Operate at the Lab 62

I. EXPERT ASSISTANCE 63
1. Introduction 63
2. Finding Experts 64
a. Federal Sources..... 65
b. Private Experts..... 66
(1) Professional Computer Organizations..... 66
(2) Universities..... 67
(3) Computer and Telecommunications Industry Personnel 67
(4) The Victim 67
3. What the Experts Can Do 68
a. Search Planning and Execution 68
b. Electronic Analysis 68

[page iv]

c. Trial Preparation 69
d. Training for Field Agents 70

V. NETWORKS AND BULLETIN BOARDS

A. INTRODUCTION 71

B. THE PRIVACY PROTECTION ACT, 42 U.S.C. 2000aa 72
1. A Brief History of the Privacy Protection Act 72
2. Work Product Materials 73
3. Documentary Materials 77
4. Computer Searches and the Privacy Protection Act 78
a. The Reasonable Belief Standard 79
b. Similar Form of Public Communication 82
c. Unique Problems: Unknown Targets and Commingled Materials ...83
5. Approval of Deputy Assistant Attorney General Required 84

C. STORED ELECTRONIC COMMUNICATIONS 85

Vl. DRAFTING THE WARRANT

A. DRAFTING A WARRANT TO SEIZE HARDWARE 91

B. DRAFTING A WARRANT TO SEIZE INFORMATION 92
1. Describing the Place to be Searched 92
a. General Rule: Obtain a Second Warrant 93
b. Handling Multiple Sites within the Same District 93
c. Handling Multiple Sites in Different Districts 94
d. Information at an Unknown Site 95
e. Information/Devices Which Have Been Moved 96
2. Describing the Items to be Seized 97
3. Removing Hardware to Search Off-Site: Ask the Magistrate for Explicit
Permission..... 99
4. Seeking Authority for a No-Knock Warrant 100
a. In General 100
b. In Computer-Related Cases 101
[page v]

VII. POST-SEARCH PROCEDURES

A. INTRODUCTION 103

B. PROCEDURES FOR PRESERVING EVIDENCE 104
1. Chain of Custody 104
2. Organization 104
3. Keeping Records 105
4. Returning Seized Computers and Materials 105
a. Federal Rules of Criminal Procedure: Rule 41(e) 106
b. Hardware 109
c. Documentation 110
d. Notes and Papers 110
e. Third-Party Owners 111

VIII. EVIDENCE

A. INTRODUCTION 113

B. THE BEST EVIDENCE RULE 114

C. AUTHENTICATING ELECTRONIC DOCUMENTS 115
1. "Distinctive" Evidence 116
2. Chain of Custody 119

3. Electronic Processing of Evidence 120

D. THE HEARSAY RULE 122

IX APPENDICES

APPENDIX A: SAMPLE COMPUTER LANGUAGE FOR SEARCH WARRANTS 125
1. Tangible Objects 125
a. Justify Seizing the Objects 125
b. List and Describe the Objects 126
(1) Hardware 127
(2) Software 127
(3) Documentation 128
(4) Passwords and Data Security Devices 128

[page vi]

2. Information: Records, Documents, Data 128
a. Describe the Content of Records, Documents, or other Information ... 129
b. Describe the Form which the Relevant Information May Take 130
c. Electronic Mail: Searching and Seizing Data from a BBS Server under 18 U.S.C. 131
(1) If All the E-Mail is Evidence of Crime 131
(2) If Some of the E-Mail is Evidence of Crime 132
(3) If None of the E-Mail is Evidence of Crime 132
d. Ask Permission to Seize Storage Devices when an Off-Site Search is Necessary 133
e. Ask Permission to Seize, Use, and Return Auxiliary Items, as Necessary 134
f. Data Analysis Techniques 135
3. Stipulation for Returning Original Electronic Data 135

APPENDIX B: GLOSSARY 139

APPENDIX C: FEDERAL EXPERTS FOR COMPUTER CRIME INVESTIGATIONS..... 143

APPENDIX D: COMPUTER SEARCH AND SEIZURE WORKING GROUP 145

APPENDIX E: STATUTORY POPULAR NAME TABLE.....153

APPENDIX F: TABLE OF AUTHORITIES 155
Cases 155
Statutes 162
Federal Rules 162
Federal Regulations 163

Legislative History 163
Reference Materials 164
[page a]

INTRODUCTION

As computers and telecommunications explode into the next century, prosecutors and agents have begun to confront new kinds of problems. These Guidelines illustrate some of the ways in which searching a computer is different from searching a desk, a file cabinet, or an automobile. For example, when prosecutors must interpret Rule 41 (which requires that the government obtain a search warrant in the district where the property to be searched is "located"), applying it to searches of physical items is usually uncomplicated. But when they must try to "locate" electronic data, the discussion can quickly become more metaphysical than physical.

Even so, it is important to remember throughout the process that as dazzling and confounding as these new-age searches and seizures may be, they are in many essential ways just like all other searches. The cause must be just as probable; the description of items, just as particular. The standard investigative techniques that work in other cases (like finding witnesses and informants) are just as valuable in computer cases. The evidence that seals a case may not be on the hardware or software, but in an old-fashioned form: phone bills, notes in the margins of manuals, or letters in a drawer.

The sections that follow are an integration of many legal sources, practical experiences, and philosophical points of view. We have often had to extrapolate from existing law or policies to try to strike old balances in new areas. We have done our best to anticipate the questions ahead from the data available today. Even so, we recognize that rapid advances in computer and telecommunications technologies may require that we revisit these Guidelines,~perhaps in the near future. In the meantime, as law struggles to catch up to technology, it is important to remember that computer cases are just like all others in one respect at least: under all the "facts and circumstances," there is no substitute for reasonable judgment.

[no page 2] [page 3]

I. KEY TERMS AND CONCEPTS

Searching and seizing computers raises unique issues for law enforcement personnel. Before addressing these issues, however, it is important to have a basic understanding of key terms and fundamental concepts that will influence the government's search and seizure decisions. This section describes these central terms and concepts. A more complete

glossary can be found at APPENDIX B, p. 139.

A. DEFINITIONS

When people speak of searching or seizing computers, they usually are not referring only to the CPU (Central Processing Unit). After all, a computer is useless without the devices that allow for input (e.g., a keyboard or mouse) and output (e.g., a monitor or printer) of information. These devices, known as "peripherals,"[1] are an integral part of any "computer system."

Failure to more specifically define the term "computer" may cause misunderstandings. Having probable cause to seize a "computer" does not necessarily mean there is probable cause to seize the attached printer. Therefore, we need to be clear about our terms.

1. Hardware -- "The physical components or equipment that make up a computer system...." Webster's Dictionary of Computer Terms 170 (3d ed. 1988). Examples include keyboards, monitors, and printers.

2. Software -- "The programs or instructions that tell a computer what to do." Id. at 350. This includes system programs which control the internal operation of the computer system (such as Microsoft's Disk Operating System, "MS-DOS," that controls

---

1 Peripheral equipment means "[t]he input/output units and auxiliary storage units of a computer system, attached by cables to the central processing unit." Webster's Dictionary of Computer Terms 279 (3d ed. 1988).

IBM-compatible PCs) and applications programs which enable the computer to produce useful work (e.g., a word processing program such as WordPerfect).

3. Data -- "A formalized representation of facts or concepts suitable for communication, interpretation, or processing by people or by automatic means." Id. at 84. Data is often used to refer to the information stored in the computer.

4. Documentation -- Documents that describe technical specifications of hardware components and/or software applications and how to use them.

5. Input/Output (I/O) Device -- A piece of equipment which sends data to, or receives data from, a computer. Keyboards, monitors, and printers are all common I/O devices.

6. Network -- "A system of interconnected computer systems and terminals." Id. at 253.

7. System Administrator (or System Operator, "sysop") -- The individual responsible for assuring that the computer system is functioning properly. He is often responsible for computer security as well.

For search and seizure purposes, unless the text specifically indicates otherwise, the term "computer" refers to the box that houses the CPU, along with any internal storage devices (such as internal hard drives) and internal communications devices (such as an internal modem or fax card). Thus, "computer" refers to the hardware, software, and data contained in the main unit. Printers, external modems (attached by cable to the main unit), monitors, and other external attachments will be referred to collectively as "peripherals" and discussed individually where appropriate. When we are referring to both the computer and all attached peripherals as one huge package, we will use the term "computer system." "Information" refers to all the information on a computer system, including both software applications and data.

It is important to remember that computer systems can be configured in an unlimited number of ways with assorted input and output devices. In some cases, a specific device may have particular evidentiary value (e.g., if the case involves

[page 5] a bookie who prints betting slips, the printer may constitute valuable evidence); in others, it may be the information stored in the computer that may be important. In either event, the warrant must describe, with particularity, what agents should search for and seize.

B. LIST OF COMPUTER SYSTEM COMPONENTS

The following is an abridged list of hardware components which may play a role in a criminal offense and, therefore, be subject to search and seizure under warrant. For a more extensive list, see the "GLOSSARY" at APPENDIX B, p. 139. It is important to remember that electronic components are constantly changing, both in nature and in number, and no list can be comprehensive.

Device Name Description

CPU: The central processing unit.

Hard Disk Drive: A storage device based on a fixed, permanently mounted disk drive. It may be either internal or external. Both applications and data may be stored on the disk.

Floppy Disk Drive: A drive that reads from or writes to floppy diskettes. Information is stored on the diskettes themselves, not on the drive.

Mouse: A pointing device that controls input. Normally, the user points to an object on the screen and then presses a button on the mouse to indicate her selection.

Modem: A device allowing the computer to communicate with another computer, normally over standard telephone lines. Modems may be either external or internal.

[page 6] Fax Peripheral: A device, normally inserted as an internal card, that allows the computer to function as a fax machine.

CD ROM: CD ROM stands for Compact Disk Read-Only Memory. CD ROMs store and read massive amounts of information on a removable disk platter. Unlike hard drives and diskettes, CD ROMs are read-only and data cannot be written to the platter.

Laser Disk: Similar to a CD ROM drive but uses lasers to read and write information.

Scanner: Any optical device which can recognize characters on paper and, using specialized software, convert them into digital form.

Printer: A number of technologies exist, using various techniques. The most common printers are:

1. Dot matrix - characters and graphics are created by pins hitting the ribbon and paper;

2. Laser - electrostatically charges the printed page and applies toner;

3. Ink jet - injects (sprays) ink onto the paper;

4. Thermal - a hot printer head contacts special paper that reacts to heat;

5. Band - a rotating metal band is impacted as it spins;

6. Daisy wheel - a small print wheel containing the form of each character rotates and hits the paper, character by character; [page 7]

7. Plotter - moves ink pens over the paper surface, typically used for large engineering and architectural drawings.

C. DETERMINING THE COMPUTER'S ROLE IN THE OFFENSE

Before preparing a warrant to seize all or part of a computer system and the information it contains, it is critical to determine the computer's role in the offense. First, the computer system may be a tool of the offense. This occurs when the computer system is actively used by a defendant to commit the offense. For example, a counterfeiter might use his computer, scanner, and color printer to scan U.S. currency and then print money. Second, the computer system may be incidental to the offense, but a repository of evidence. For example, a drug dealer may store records pertaining to customers, prices, and quantities delivered on a personal computer, or a blackmailer may type and store threatening letters in his computer.

In each case, the role of the computer differs. It may constitute "the smoking gun" (i.e., be an instrumentality of the offense), or it may be nothing more than an electronic filing cabinet (i.e., a storage device). In some cases, the computer may serve both functions at once. Hackers, for example, often use their computers both to attack other computer systems and to store stolen files. In this case, the hacker's computer is both a tool and storage device. Whatever the computer's role in each case, prosecutors must consider this and tailor warrants accordingly.

By understanding the role that the computer has played in the offense, it is possible to focus on certain key questions:

Is there probable cause to seize hardware?

Is there probable cause to seize software?

Is there probable cause to seize data?

[page 8]

Where will this search be conducted? Is it practical to search the computer system on site, or must the examination be conducted at a field office or laboratory?

If agents remove the system from the premises to conduct the search, must

they return the computer system, or copies of the seized data, to its owner/user before trial?

Considering the incredible storage capacities of computers, how will agents search this data in an efficient, timely manner?

Before addressing these questions, it is important to recognize that general Fourth Amendment principles apply to computer searches, and traditional law enforcement techniques may provide significant evidence of criminal activity, even in computer crime cases. Therefore, we begin with a brief overview of the Fourth Amendment.

[page 9]

II. GENERAL PRINCIPLES

A. SEARCH WARRANTS

There is, of course, "a strong preference for warrants," and courts will scrutinize a warrantless search. Indeed, as the Supreme Court indicated in United States v. Leon, 468 U.S. 897, 914 (1984), a warrant can save a search where probable cause is doubtful or marginal. Most searches of computer systems will be pursuant to warrant, but the recognized exceptions to the warrant requirement apply equally to the search and seizure of computers.

B. PLAIN VIEW

Evidence of a crime may be seized without a warrant under the plain view exception to the warrant requirement. To rely on this exception, the officer must be in a lawful position to observe the evidence, and its incriminating character must be immediately apparent. See Horton v. California, 496 U.S. 128 (1990). For example, if agents with a warrant to search a computer for evidence of narcotics trafficking find a long list of access codes taped to the computer monitor, the list should also be seized.

C. EXIGENT CIRCUMSTANCES

"When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if there is probable cause to believe that the item seized constitutes evidence of criminal activity." United States v. David. 756 F. Supp. 1385, 1392 (D. Nev. l991).2 If a target's screen is displaying evidence

---------- 2 See also United States v. Talkington, 875

F.2d 591 (7th Cir. 1989) (warrantless entry to residence and seizure of counterfeit money was justified since agents knew that (1) the suspects had previously discussed burning money; (2) there was a fire in the backyard: and (3) the agents were confident that residents were not having a cookout.

[page 10]

which agents reasonably believe to be in danger, the "exigent circumstances" doctrine would justify downloading the information before obtaining a warrant. For example, agents may know that the incriminating data is not actually stored on the suspect's machine, but is only temporarily on line from a second network storage site in another building, city, or district. Thus, even if the agents could secure the target's computer in front of them, someone could still electronically damage or destroy the data -- either from the second computer where it is stored or from a third, unknown site. Of course, when agents know they must search and seize data from two or more computers on a wide-area network, they should, if possible, simultaneously execute separate search warrants. (See "Describing the Place to be Searched," infra p. 92.) But sometimes that is not possible, and agents must then analyze the particular situation to decide whether the "exigent circumstances" exception applies. In computer network cases, as in all others, the answer is absolutely tied to the facts.

In determining whether exigent circumstances exist, agents should consider: (1) the degree of urgency involved, (2) the amount of time necessary to obtain a warrant, (3) whether the evidence is about to be removed or destroyed, (4) the possibility of danger at the site, (5) information indicating the possessors of the contraband know the police are on their trail, and (6) the ready destructibility of the contraband. United States v. Reed, 935 F.2d 641, 642 (4th Cir.), cert. denied, 112 S. Ct. 423 (1991).

Under the "exigent circumstances" exception to the warrant requirement, agents can search without a warrant if the circumstances would cause a reasonable person to believe it to be necessary. The Supreme Court has upheld warrantless entries and searches when police officers reasonably believe that someone inside needs "immediate aid," Mincey v. Arizona, 437 U.S. 385, 392~-93 (1978), or to prevent the destruction of relevant evidence, the escape of a suspect, or the frustration of some other legitimate law enforcement objective. United States v. Arias, 923 F.2d 1387 (9th Cir.), cert. denied, 112 S. Ct. 130 (1991). The officer's fears need not be correct so long as they are reasonable. See United States v.

Reed, supra (proper inquiry is what objective officer could reasonably believe).

[page 11]

Recognizing the strong preference for warrants, courts have suppressed evidence where the officers had time to get a warrant but failed to do so. United States v. Houle, 603 F.2d 1297 (8th Cir. 1979). Some courts have even ruled that exigent circumstances did not exist if the law enforcement officers had time to obtain a warrant by telephone. United States v. Patino, 830 F.2d 1413, 1416 (7th Cir. 1987)(warrantless search not justified when officer had adequate opportunity to obtain telephone warrant during 30-minute wait for backup assistance; not permissible for agents to wait for exigency and then exploit it), cert. denied, 490 U.S. 1069 (1989).

Additionally, while exigencies may justify the seizure of hardware (i.e., the storage device), this does not necessarily mean that they support a warrantless search. In United States v. David, 756 F. Supp. 1385 (D. Nev. 1991), the court held that although the agent was correct to seize the defendant's computer memo book without a warrant (because the agent saw him deleting files), the agent should have gotten a search warrant before re~accessing and searching the book. The court held the exigencies allowed the agent to take the computer memo book but, once taken, there was time to get a warrant to look inside. Therefore, the seized evidence had to be suppressed. Id. at 1392.

This holding is, of course, analogous to cases which address other kinds of containers. In the David case, the computer book itself was not contraband, instrumentality, fruit, or evidence of crime. It was, instead, a small file cabinet, a locked box, a container of data. The agent was not interested in the hardware but in the information inside. As the cases make clear, authority to seize a container does not necessarily authorize a warrantless search of the container's contents. See Texas v. Brown, 460 U.S. 730, 750 (1983)(Stevens, J., concurring)(plain view justified seizure of party balloon but additional justification was required to open balloon without warrant). Courts have suppressed warrantless searches when the defendant still had a reasonable expectation of privacy in the contents of the container. See United States v. Turk, 526 F.2d 654 (5th Cir.)(although seizure of tape was proper, playing taped conversation of private telephone communication was not), cert. denied, 429 U.S. 823 (1976); Blair v. United States, 665 F.2d 500 (4th Cir. 1981).

Agents must always remember, however, that electronic data is perishable. Humidity, temperature, vibrations, physical mutilation, magnetic fields

created by passing a strong magnet over a disk, or computer commands (such as "erase *.*" or "format") can destroy data in a matter of seconds. [page 12]

Thus, the exigent circumstances doctrine may justify a warrantless seizure in appropriate cases.

D. BORDER SEARCHES

The law recognizes a limited exception to the Fourth Amendment's probable cause requirement at the nation's borders. Officials may search people and property without a warrant and without probable cause as a condition of crossing the border or its "functional equivalent." United States v. Ramsey, 431 U.S. 606 (1977), cert. denied, 434 U.S. 1062 (1978). Both incoming international baggage (United States v. Scheer, 600 F.2d 5 (3d Cir. 1979) and incoming international mail at the border are subject to search without a warrant to determine whether they contain items which may not lawfully be brought into the country. Border searches or international mail searches of diskettes, tapes, computer hard drives (such as laptops carried by international travelers), or other media should fall under the same rules which apply to incoming persons, documents, and international mail.

On the other hand, the border search exception to the warrant requirement probably will not apply to data transmitted electronically (or by other non-physical methods) into the United States from other countries. For example, if an individual in the United States downloads child pornography from a foreign BBS, a warrantless search of his home computer could not be supported by the border search exception. In such cases, it is difficult to find a "border" or its functional equivalent as data travels over international telephone lines or satellite links. What seems clear, however, is that once data has been received by a computer within the United States, that data resides in the country and has passed beyond the border or its functional equivalent. Because the justification for the border search exception is grounded on the sovereign's power to exclude illegal articles from the country, that exception no longer applies once such articles (in this case electronic data) have come into the country undetected.

[page 13] E. CONSENT SEARCHES

Agents may search a place or object without a warrant or, for that matter, without probable cause, if a person with authority has consented. Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973). This consent may be explicit or implicit. United States v. Milan-Rodriguez, 759 F.2d 1558, 1563-64 (11th Cir.)(telling police where to find a key constitutes

implicit consent to a search of the locked area), cert. denied, 474 U.S. 845 (1985), and cert. denied, 486 U.S. 1054 (1988).

Whether consent was voluntarily given is a question of fact which the court will decide. United States v. Scott, 578 F.2d 1186, 1189 (6th Cir.), cert. denied, 439 U.S. 870 (1978). The burden is on the government to prove that the consent was voluntary, United States v. Price, 599 F.2d 494, 503 (2nd Cir. 1979), and, in making its decision, the court will consider all the facts surrounding the consent. Schneckloth, supra, at 226-7; United States v. Mendenhall, 446 U.S. 544, 557-8 (1980). See generally United States v. Caballos, 812 F.2d 42 (2d Cir. 1987). While no single aspect controls the result, the Supreme Court has identified the following important factors: the age of the person giving consent; the person's education, intelligence, mental and physical condition; whether the person was under arrest; and whether he had been advised of his right to refuse consent. Schneckloth, supra, at 226.

In computer crime cases, several consent issues are likely to arise. First, did the scope of the search exceed the consent given? For example, what if a target consents to a search of his machine, but the data is encrypted? Does his consent authorize breaking the encryption scheme? Second, who is the proper party to consent to a search? Does a system administrator have the authority to consent to a search of a file server containing the files of all the system users?

1. Scope of the Consent

A person who consents to a search may explicitly limit this consent to a certain area. United States v. Griffin, 530 F.2d 739, 744 (7th Cir. 1976). When the limits of the consent are clearly given, either at the time of the search or even afterwards, agents must respect their bounds. In Vaughn v. Baldwin,

[page 14]

950 F.2d 331 (6th Cir. 1991), the plaintiff dentist had voluntarily turned over records to the IRS. The IRS agent kept the records for months and refused several informal requests for their return. Plaintiff then formally, in writing, revoked his consent to the IRS, which still kept the records to make copies. Finally, plaintiff sued and the IRS returned the originals but kept the copies. The court found that the IRS had violated the Fourth Amendment. Although the IRS was entitled to copy the records while they lawfully had them, they could not keep the records once plaintiff revoked his consent. Moreover, considering the long period of time that the IRS held the documents, the court rejected the argument that once the plaintiff demanded return of his documents the government

should be entitled to retain them for a reasonable period for copying.

Consent may also be limited implicitly. In United States v. David, 756 F. Supp. 1385 (D. Nev. 1991), the court held that while the defendant had consented, pursuant to a cooperation agreement, to share some of the information contained in his hand-held computer memo book, his attempt to prevent agents from seeing the file password constituted a limit on his consent. Although the agent did nothing wrong by leaning over defendant's shoulder to watch him enter the password, the government clearly exceeded the implicit limits of David's consent when agents used the password to read the whole computer book without David's permission. For a more extensive discussion of encryption issues, see, infra p. 54.

2. Third-Party Consent

a. General Rules

It is not uncommon for several people to use or own the target computer equipment. If any one of those people gives permission to search for data, agents may generally rely on that consent, so long as that person has authority over the computer. In these cases, all users have assumed the risk that a co~-user might not just discover everything in the computer but might also permit law enforcement to discover the "common area" as well.

[page 15]

In United States v. Matlock, 415 U.S. 164 (1974), the Supreme Court stated that one who has common authority over premises or effects may consent to a search even if the absent co-user objects. In an important footnote, the Court said that "common authority" is not a property law concept but

rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.

Id. at 171 n.7.

Extending this analysis, a third party with common authority may consent even if he is antagonistic toward the defendant. One could even argue that sharing access to a common premises with an unsympathetic person would objectively increase the risk of disclosure, and thus reasonable expectations of privacy actually diminish. This is especially true where

the consenting individual agrees to a search of common premises to exculpate himself from the defendant's criminal activity. See 3 W. LaFave, Search and Seizure: A Treatise on the Fourth Amendment 8.3(b) at 244-45 (2d ed. 1987). See also United States v. Long, 524 F.2d 660 (9th Cir. 1975) (wife in fear of her husband could still consent to a search of the jointly owned house even though she had moved out and he had changed the locks).

Where two or more people enjoy equal property rights over a place, they may still have exclusive, private zones within the shared premises. Housemates with separate bedrooms, spouses with private areas or containers, and housemates with separate directories on a shared computer may reasonably expect to own that space alone. But when do these individual expectations overcome another's common authority over premises or property? Although there is no bright line test, courts will generally regard a defendant's claims of exclusive control in this situation with some skepticism. See Frazier v. Cupp, 394 U.S. 731, 740 (1969).

Even so, courts may honor claims to privacy where the defendant has taken some special steps to protect his personal effects from the scrutiny of others, and others lack ready access. 3 W. LaFave, supra 8.3(f), at 259-60. In United States v. Block, 590 F.2d 535 (4th Cir. 1978), the Fourth Circuit

[page 16]

held that a mother's authority to permit police officers to inspect her 23-year-old son's room did not include his locked footlocker in the room. The court stated that the authority to consent to search

cannot be thought automatically to extend to the interiors of every discrete enclosed space capable of search within the area.... Common experience .... teaches all of us that the law's "enclosed spaces"--mankind's valises, suitcases, footlockers, strong boxes, etc. -- are frequently the objects of his highest privacy expectations, and that the expectations may well be at their most intense when such effects are deposited temporarily or kept semi-permanently in public places or in places under the general control of another.

Id. at 541.

In a footnote, however, the Block court noted that not every "enclosed space" within a room is exempt from the reach of the authorized search area. A rule of reason applies, one that considers the circumstances "indicating the presence or absence of a discrete expectation of privacy with respect to a particular object: whether it is secured, whether it is

commonly used for preserving privacy, etc." Id. at n.8. Cf. United States v. Sealey, 830 F.2d 1028, 1031 (9th Cir. 1987) (spousal consent valid because sealed containers were not marked in any way that would indicate defendant's sole ownership). Thus, creating a separate personal directory on a computer may not sufficiently mark it as exclusive, but protecting that separate directory with a secret password may "lock the container." In that event, if law enforcement analysts search the directory by breaking the password (because the co-user who consented to the search did not know that password), a court would probably suppress the result.

Matlock did not address whether a consent search is valid when police have reasonably, but mistakenly, relied upon the consent of someone who appeared to have common authority over the premises, but in fact did not. In Illinois v. Rodriguez, 497 U.S. 177 (1990), however, the Supreme Court held that a consent search is valid when police are reasonable in thinking they have been given authorized consent. The Court cautioned, however, that police cannot simply rely upon someone at the scene who claims to have authority if the surrounding circumstances indicate otherwise. If such authority is unclear, the police are obligated to ask more questions. Determining who has power to consent is an objective exercise, the Court stated, and the test is whether the

facts available to the police officer at the moment would warrant a person of reasonable caution to believe that the consenting party had authority over the premises. Id. at 2801.

b. Spouses

Under the Matlock "common authority" approach, most spousal consent searches are valid. Although spouses who create exclusive areas may preclude their partners from consenting to a search, that circumstance will be unusual. Indeed* spouses do not establish "exclusive use" just by being the only one who uses the area; there must be a showing that the consenting spouse was denied access. 3 W. LaFave, supra p. 11, 8.4(a), at 278. In United States v. Duran, 957 F.2d 499, 504-5 (7th Cir. 1992), for example, the defendant and his wife lived on a farm with several outbuildings. The wife consented to the search of a building which she believed defendant used as a private gym, but the police found marijuana plants inside. The court emphasized the presumption that the entire marital premises are jointly held and controlled by the partners, and said this presumption can be overcome only by showing that the consenting spouse was actually denied access to the area in question.

With spouses, as with roommates, the Rodriguez "reasonable belief" rule

(supra p. 16) allows investigating agents to draw reasonable conclusions, based upon the situation they encounter, about who has authority to consent. In the absence of objective evidence to the contrary, agents will be reasonable in presuming that spouses have authority to consent to a search of anything on the marital property. Illinois v. Rodriguez, supra.

c. Parents

In some recent computer crime cases the perpetrators have been relatively young and, even if no longer legally minors, have resided with their parents. Under the Matlock rationale, it is clear that parents may consent to a search of common areas in the family home. Additionally, with regard to minor children, the courts have found parents to hold superior rights in the

[page 18]

home and "even rather extraordinary efforts by the child to establish exclusive use may not be effective to undermine the parents' authority over their home, including rooms occupied by the child." 3 W. LaFave, supra p. 15, 8.4(b), at 283. Therefore, if parents consent to a search and seizure of floppy disks or passwords locked in the minor child's room, that consent should be upheld.

The issue becomes more complicated, however, when the sons and daughters who reside with their parents are adults. In these situations, courts may reach the opposite result when, as a practical matter, the adult child has established an exclusive area in the home that the parents have respected. Id. at 285. See discussion of United States v. Block, supra p. 15.

d. Employers

Employers may be either public (i.e., government) or private. The distinction is important because government employers, unlike private employers, are bound by the Fourth Amendment. In construing the reach of the Fourth Amendment into the workplace, the Supreme Court has held that government employers may search employee offices, without either a warrant or the consent of the employee, when the search is administrative in nature; that is, it is work-related (e.g., the supervisor needs to find a case file) or involves work-related misconduct. O'Connor v. Ortega, 480 U.S. 709 (1987).

The Court found that government employees can have a reasonable expectation of privacy even though the physical area is owned by the

government. Id. at 717 (specifically rejecting a contention made by the Solicitor General that public employees can never have a reasonable expectation of privacy in their place of work). The realities of the workplace, however, suggest that an employee's expectation of privacy must be reduced to the degree that fellow employees, supervisors, subordinates, guests, and even the general public may have access to that individual's work space. Recognizing that government agencies could not function properly if supervisors had to establish probable cause and obtain a warrant whenever they needed to look for a file in an employee's office, the Supreme Court held that two kinds of searches are exempt. Specifically, both (1) a non-investigatory, work-related intrusion and (2) an investigatory search for evidence of suspected work-related employee misfeasance are permissible without a warrant and should be judged by the standard of reasonableness. Id. at 725-6.

[page 19]

Even so, the court made clear that "[n]ot everything that passes through the confines of the business address can be considered part of the workplace context...." Id. at 717. For example, the contents of an employee's purse, briefcase, or closed luggage do not lose their private character just because the employee has brought them to work. Thus, while the circumstances may permit a supervisor to search in an employee's desk for a work-related file, the supervisor usually will have to stop at the employee's gym bag or briefcase. This analysis may have interesting implications for "containers" like floppy disks, which certainly may be either work-related or private, depending on the circumstances. It will probably be reasonable for employers to assume that floppy disks found at an office are part of the workplace, but there may be cases where a court will treat a floppy disk as if it were a personal container of private items.

Of course, there may be some government agencies where employees do consent (either expressly or tacitly) to searches of even private parcels because of the nature of the job. For example, employees with security clearances who work with classified material may expect that their purses, briefcases, and other bags may be inspected under certain circumstances. The factual variations on this "reasonable expectation" theme are endless, and are tied absolutely to the details of each case.

The O'Connor Court did not address the appropriate standard to be applied when a government employee is being investigated for criminal misconduct or breaches of other non-work-related statutory or regulatory standards. Id. at 729. In a case involving employee drug testing, at least one court has noted, in dicta, that "[t]he government may not take advantage of any arguably relaxed `employer' standard for warrantless searches....when its

true purpose is to obtain evidence of criminal activity without complying with the more stringent standards that normally protect citizens against unreasonably intrusive evidence-gathering." National Federation of Federal Employees v. Weinberger, 818 F.2d 935, 943 n.12 (D.C. Cir. 1987). Therefore, it would appear that whenever law enforcement is conducting an evidence-gathering search, even if the search is to take place at a government office, agents must either obtain a warrant or fall within some generally recognized exception to the warrant requirement. Appropriate consent from a third party is, of course, one of those exceptions.

Generally speaking, an employer (government or private) may consent to a search of an employee's computer and peripherals if the employer has

common authority over them. Agents and prosecutors must consider whether, under the facts, the employee would expect privacy in those items and whether that expectation would be objectively reasonable. Relevant factors include whether (1) the area/item to be searched has been set aside for the employee's exclusive or personal use (e.g., does the employee have the only key to the computer or do others have access to the data); (2) the employee has been given permission to store personal information on the system or in the area to be searched; (3) the employee has been advised that the system may be accessed or looked at by others; (4) there have been past inspections of the area/item and this fact is known to the employee; and (5) there is an employment policy that searches of the work area may be conducted at any time for any reason. And when the employer is the federal government, another factor is (6) whether the purpose of the search was work-related, rather than primarily for law enforcement objectives. See generally O'Connor, 480 U.S. at 717 (employee's expectation of privacy must be assessed in the context of the employment relationship).

There are currently no cases specifically addressing an employer's consent to search and seize an employee's computer (and related items). But there are cases that discuss searches of an employee's designated work area or desk. For example, the Seventh Circuit has upheld the search of a hotel room that served as a welfare hotel's business office after the hotel owner consented. United States v. Bilanzich, 771 F.2d 292 (7th Cir. 1985). The room searched was used by the defendant/manager of the hotel for hotel business, the hotel's books were stored there, and the room was also used by doctors and welfare officials when they visited residents. The manager kept the key to the room. In affirming the manager's theft and forgery convictions (based in large part on documents seized from the business office/hotel room), the Seventh Circuit found

that the hotel owner had the requisite control over and relationship to the business office to consent to its search. The court rejected the manager's argument that she had sole control over the business office because she generally had the key, finding that the owner could request access to the room at any time, that the room was shared with others (visiting physicians and welfare officials), and that the items sought were business records (e.g., welfare checks that the manager had forged). Thus, the manager did not have exclusive control over the area nor was it for her personal use. In addition, the purpose of the search was "employment related," since the manager was defrauding the employer and the customers.

[page 21]

In United States v. Gargiso, 456 F.2d 584, 587 (2d Cir. 1972), the Second Circuit upheld the search of a locked, wired-off area in the basement of a book company -- a search to which the highest official of the book company then on the scene (the company's vice president) had consented. The defendant, an employee of the book company, objected to the search. Both the defendant and the vice president had supervisory authority over the area searched, and both also had keys to the area, as did other company personnel. The court found that the vice president's control over the area was equal to that of the employee's, making the consent effective. The vice president had sufficient control over the area to permit inspection in his own right and the employee had assumed the risk that the vice president would do so.

In Donovan v. A.A. Beiro Construction Co.. Inc., 746 F.2d 894, 900 (D.C. Cir. 1984), the D.C. Circuit found the D.C. Government's consent to a search conducted by OSHA inspectors of a D.C. construction site effective against one of the contractors. The site was a large, multi-employer area surrounded by a chain link fence with no interior fences separating the various contractors' work areas. There was considerable overlap and interaction among the various contractors and their employees. The Court found that the defendant/contractor had no reasonable expectation of privacy in the area searched, because it was a common construction site shared by many. Thus, the defendant/contractor had assumed the risk that anyone with authority at the site would permit inspection of the common construction area.

In an earlier case, United States v. Blok, 188 F.2d 1019 (D.C. Cir. 1951), the D.C. Circuit affirmed the reversal of a petty larceny conviction of a government employee, finding that the search of the employee's desk violated the employee's right of privacy. The court found that the employee had exclusive use of the desk and a reasonable expectation of privacy in it. Her employer's consent to a police search

of the desk did not make the search reasonable. There was no policy putting employees on notice that they should not expect privacy in their desks. Nor was the search conducted by the employer for employment purposes (e.g., searching for a file). "It was precisely the kind of search by policemen for evidence of a crime against which the constitutional prohibition was directed." Id. at 1021 (quoting the district court). Thus, the employer's consent was ineffective because the area searched was for the employee's exclusive and personal use (factor number 1 above); the

[page 22]

purpose of the search was not work-related (factor number 6 above); and there was no policy putting the employee on notice that her desk might be subject to search (factors number 3 and 5 above). Significantly, the O'Connor Court cited Blok with approval. O'Connor, 480 U.S. at 719.

e. Networks: System Administrators

Case law demonstrates that the courts will examine the totality of the circumstances in determining whether an employee has a reasonable expectation of privacy or whether an employer shares authority over the employee's space and can consent to a search. But applying this employer-consent case law to computer searches can become especially troublesome when the employee's computer is not a stand-alone container, but an account on a large network server. The difficulty is a practical one. In the physical world, individuals often intuitively understand their rights to control physical space and to restrict access by others because they can observe how everyone uses the space. For example, with filing cabinets, employees can see whether they are located in private areas, whether others have access, whether the cabinets are locked, and who has the keys. While explicit company policies certainly help to clarify the situation, employees can physically observe company practices and will probably conclude from their observations that certain property is or is not private.

By contrast, in an electronic environment, employees cannot "see" when a network administrator, supervisor, or anyone else accesses their data. They cannot watch the way people behave with data, as they can with a file cabinet, and deduce from their observations the measure of privacy they ought to expect. As a practical matter, system administrators can, and sometimes do, look at data. But when they do, they leave no physical clues which would tell a user they have opened one of his files. Lacking these physical clues, some users who are unfamiliar with computer technology may falsely but honestly believe that their data is completely private. Will the courts hold this false belief to be one that society is

prepared to recognize as reasonable? Will the courts still find it reasonable, even when a user knows that there are such people as system administrators who are responsible in some fashion for operating and securing the entire network? If so, do users who actually understand the technology and the scope of a system operator's access to data

[page 23] have a lesser expectation of privacy and fewer Fourth Amendment protections than users who are not so well informed? And what happens in the years ahead as our population becomes increasingly computer literate? Of course, these search and seizure questions are not limited to computer networks in the workplace. Universities, libraries, and other organizations, both public and private, may operate computer networks on which users store data which they consider private--either partly or completely. If those networks provide services to the public, they will be controlled by the provisions of 18 U.S.C. 2702, which limits the situations in which a service provider may release the contents of qualifying electronic mail. (For a detailed discussion of this statute, see "STORED ELECTRONIC COMMUNICATIONS," infra p. 85.) But for material which falls outside this statute, the Fourth Amendment analysis discussed above will still apply.

Prosecutors who face these issues at trial should be ready to argue that reasonable network users do, indeed, understand the role and power of system operators well enough to expect them to be able to protect and even restore their files. Therefore, absent some guarantees to the contrary, reasonable users will also expect system administrators to be able to access all data on the system. Certainly, if the system has published clear policies about privacy on the network or has even explained to users that its network administrators have oversight responsibility and control, this will support the position that a system operator's consent to a search was valid. But if the network and its users have not addressed these issues and the situation is ambiguous, the safest course will be to get a warrant. (Of course, if the system administrator does have authority to access and produce a user's files and simply will not do it on request, agents should use a subpoena.)

If agents choose to apply for a warrant and are concerned that a target/user will delete his data before they can execute the search, the agents should consider asking a cooperating system operator to make and keep a backup of the target's data, which they can later procure under the warrant or subpoena. The circumstances of each case will dictate the wisest approach, but agents and prosecutors should explore all these questions before they just ask a system administrator to produce a user's files. [page 24]

F. INFORMANTS AND UNDERCOVER AGENTS

As in other types of investigations, it is often helpful to use

informants or undercover agents to develop evidence. In some cases, of course, they may be of limited value (e.g., a case involving a lone hacker). Additionally, as a matter of policy, there may be restrictions on the type of undercover activities in which agents may engage. For example, the FBI does not access bulletin boards simply to view board activities when there is no reason to believe the board is involved in criminal activity.

Generally speaking, however, the law allows informers to read material on electronic bulletin boards if they have the sysop's permission, explicit or implicit, to access the material on the board. Many BBSs, for example, have parts of the board which are open to the public and which require no password or identification for access. Other boards may have isolated directories, known as sub-boards, that are open only to paying subscribers or trusted members, and those individuals must identify themselves with passwords. Some sysops will ask newcomers to "introduce" themselves and will verify the new user's name, address, and other information before granting access with a password. These introductions should follow the same rules that undercover work has traditionally observed. Law enforcement agents need not identify themselves as such, but they must confine their activities to those that are authorized: they should not break into sections of the board for which they have not been given access. Indeed, the Ninth and Tenth Circuits have both written, in dicta, that an undercover participant must adhere scrupulously to the scope of a defendant's invitation to join the organization. United States v. Aguilar, 883 F.2d 662, 705 (9th Cir. 1989), cert. denied, 498 U.S. 1046 (1991); Pleasant v. Lovell, 876 F.2d 787, 803 (10th Cir. 1989). Thus, an informant or undercover agent must not exceed his authorized access, and having been granted access to some "levels" of the board does not give him permission to break into others.

[page 25]

III. SEIZING HARDWARE

Depending on the facts of the case, the seizure of computer hardware itself can be justified on one of three theories without regard to the data it contains: (1) the hardware is itself contraband; (2) the hardware was an instrumentality of the offense; or (3) the hardware constitutes evidence of an offense. Of course, in many cases, hardware may be seizable under more than one theory. For example, if a hacker uses his computer to insert viruses into other systems, his computer may constitute both an instrumentality of the offense and evidence admissible in court.

As noted above under Definitions, (supra p. 2), hardware is defined as the physical components of a computer system such as the central processing unit (CPU), keyboard, monitor, modem, and printer.

A. THE INDEPENDENT COMPONENT DOCTRINE

We must highlight once again that computer systems are really a combination of connected components (often by wire but increasingly by wireless means). To say that the government has probable cause to seize a "computer" does not necessarily mean it has probable cause to seize the entire computer system (i.e., the computer and all connected peripheral devices). Indeed, each component in a computer system should be considered independently.

In a strictly corporeal world, this doctrine is easy to understand and apply. For example, suppose a defendant stole a television and placed it on a television stand that he lawfully owned. Agents with a warrant for that television would not seize the stand, recognizing that the two items are easily separable and that there is, simply put, no justification for taking the stand.

With computers, the roles of the different attached components are not always separable and it is more difficult to think in such concrete terms. For example, agents with a warrant to seize a target's workstation may discover that the workstation is nothing more than a dumb terminal, and that all the evidence is in the server to which the dumb terminal is connected by wire.

[page 26]

Nonetheless, it is simply unacceptable to suggest that any item connected to the target device is automatically seizable. In an era of increased networking, this kind of approach can lead to absurd results. In a networked environment, the computer that contains the relevant evidence may be connected to hundreds of computers in a local-area network (LAN) spread throughout a floor, building, or university campus. That LAN may also be connected to a global-area network (GAN) such as the Internet. Taken to its logical extreme, the "take it because it's connected" theory means that in any given case, thousands of machines around the world can be seized because the target machine shares the Internet.

Obviously, this is not the proper approach. The better view is to seize only those pieces of equipment necessary for basic input/output (i.e., the computer itself, plus the keyboard and monitor) so that the government can successfully execute the warrant. When agents prepare warrants for other devices, they should list only those components for which they can articulate an independent basis for search or seizure (i.e., the component itself is contraband, an instrumentality, or evidence). Certainly, the independent component doctrine does not mean that connected devices are exempt; it only requires that agents and prosecutors articulate a reason for taking the item they wish to seize. For example, if the defendant has sent letters to the White House threatening the President's life, agents should explain, as a basis for

seizing the target's printer, the need to compare its type with the letter. Additionally, there may be other times when the government should seize peripherals that do not contain evidence but, again, there must be a separate basis for the seizure. See, e.g., "Seizing Hardware and Documentation so the System Will Operate at the Lab," infra p. 62.

B. HARDWARE AS CONTRABAND OR FRUITS OF CRIME

Federal Rule of Criminal Procedure 41(b)(2) authorizes warrants to seize "contraband, the fruits of crime, or things otherwise criminally possessed." The rationale behind such seizures is to prevent and deter crime. See Warden v. Hayden, 387 U.S. 294, 306 n.11 (1967). Often the fruits of crime and

[page 27]

objects illegally possessed will also constitute evidence of a crime, so that they also can be seized to help apprehend and convict criminals (see infra p. 30).

2. Contraband and Fruits of Crime Defined

The fruits of crime include property obtained by criminal activity, United States v. Santarsiero, 566 F. Supp. 536 (S.D.N.Y. 1983) (cash and jewelry obtained by use of a counterfeit credit card), and contraband is property which the private citizen is not permitted to possess, Warden v. Hayden, supra; Aguilar v. Texas, 378 U.S. 108 (1964) (narcotics). Even plans to commit a crime may constitute contraband. Yancey v. Jenkins, 638 F. Supp. 340 (N.D. Ill. 1986).

Of course, many objects which are fruits of crime or illegally possessed are innocent in themselves and can be possessed by at least certain persons under certain conditions. See, e.g. United States v. Truitt, 521 F.2d 1174, 1177 (6th Cir. 1975) (noting that a person legally can possess a sawed-off shotgun if it is properly registered to its owner, though its lawful possession is rare). A court reviewing a seizure under Rule 41(b)(2) will examine whether the circumstances would have led a reasonably cautious agent to believe that the object was a fruit of crime or was illegally possessed. For example, the seizure of jewelry as a fruit of crime in Santarsiero was upheld because a reliable informant had told officers that the suspect had boasted of using counterfeit credit cards to purchase jewelry. 566 F. Supp. at 544-45.

Certainly, there are instances where computer hardware and software are contraband or a fruit of crime. For example, there have been several recent cases involving the theft of computer equipment. Additionally, hackers have been known to penetrate credit reporting companies, illegally obtain credit card numbers, and then order computer equipment with these illegal access devices. In such cases, the equipment that they receive is a product of the fraud and should be seized as such.

[page 28]

C. HARDWARE AS AN INSTRUMENTALITY OF THE OFFENSE

1. Authority for Seizing Instrumentalities

Federal Rule of Criminal Procedure 41(b)(3) authorizes warrants to seize the instrumentalities of crime; that is, "property designed or intended for use or which is or has been used as the means of committing a criminal offense." The historical justification for the government's ability to seize instrumentalities of crime is the prevention of their use to commit future crimes. See Warden v. Hayden, 387 U.S. 294, 306 n.11 (1967); United States v. Boyette, 299 F.2d 92, 98 (4th Cir.) (Sobeloff, C.J., dissenting), cert. denied, 369 U.S. 844 (1962).

2. Instrumentalities Defined

An instrumentality of an offense is any machinery, weapon, instrument, or other tangible object that has played a significant role in a crime. See, e.g., United States v. Viera, 569 F. Supp. 1419, 1428 (S.D.N.Y. 1983) (sophisticated scale used in narcotics trafficking and black light used in counterfeiting currency). Where the object itself is innocent in character, courts will assess its role in the crime to determine whether it was an instrumentality. Compare United States v. Markis, 352 F.2d 860, 864-65 (2d Cir. 1965) (telephone used to take bets by operators of illegal wagering business was an instrumentality because it was integral to the criminal enterprise), vacated without opinion, 387 U.S. 425 (1967), with United States v. Stern, 225 F. Supp. 187, 192 (S.D.N.Y. 1964) (Rolodex file was not instrumentality where it contained names of individuals involved in tax fraud scheme). As stated by the Southern District of New York:

Not every article that plays some part in the commission of the alleged crime is a means of committing it. .... Although it is not necessary that the crime alleged could not have been committed but for the use of the article seized, after a consideration of all the circumstances it must appear that the article played a significant role in the commission of the crime alleged.

[page 29]

Stern, 225 F. Supp. at 192 (emphasis in original).

Before the Supreme Court's decision in Warden v. Hayden, 387 U.S. 294 (1967), courts held that seizable property included instrumentalities, but did not include mere evidence. See generally 3 Wright & Miller, Federal Practice and Procedure: Criminal 2d 664 (1982). In practice, however, judges were reluctant to suppress useful pieces of evidence at

trial, preferring instead to interpret the term "instrumentality" broadly enough to encompass items of evidentiary value. For example, the district court in United States v. Robinson, 287 F. Supp. 245 (N.D. Ind. 1968), upheld the seizure of the following items, all of which connected the defendant to the murder of a federal narcotics agent, as "instrumentalities" of the crime and not "mere evidence": a pair of shoes, a shirt, a jacket, handkerchiefs, spent shell casings, and wet washcloths. Such legal gymnastics were abandoned when the Supreme Court held, in Hayden, that the Fourth Amendment principally protected privacy rights, not property rights, and secured "the same protection of privacy whether the search is for 'mere evidence' or for fruits, instrumentalities or contraband." Hayden, 387 U.S. at 306-07.

Although items that are evidence of crime may now be seized along with instrumentalities, fruits, and contraband, this historical perspective is important for understanding why some early decisions may have categorized evidentiary items as instrumentalities. Moreover, the distinction between "an instrumentality" and "mere evidence" remains critical in computer crime cases because it may determine the government's ability to seize hardware. If a computer and all its peripherals are instrumentalities of a crime, the warrant should authorize the seizure of these items. But if we are seeking the computer only for the documents (mere evidence) it contains, it may be more difficult to justify the seizure or retention of hardware.

Applying the independent component doctrine to the rule permitting seizure of instrumentalities will, in most cases, not be difficult. For example, if an individual engaging in wire fraud printed out thousands of phony invoices on his home computer, it would be reasonable to take the computer, monitor, keyboard, and printer. If the individual electronically mailed these invoices to his victims, it would also be appropriate to seize his external modem (if the modem were internal it would, of course, be seized when the agents took the computer itself). If, instead of using electronic mail, he used a conventional fax machine, it would be reasonable to seize the fax as it, too would have played a significant role in the commission of the offense.

[page 30]

D. HARDWARE AS EVIDENCE OF AN OFFENSE

1. Authority for Seizing Evidence

In 1972, Federal Rule of Criminal Procedure 41(b) was amended to authorize seizing "mere evidence" of a crime. In relevant part, the Rule now states: "A warrant may be issued under this rule to search for and seize any (1) property that constitutes evidence of the commission of a criminal offense...."

2. Evidence Defined

A physical item is evidence if it will aid in apprehending or convicting a person who has committed a crime. The evidence seized need not be admissible at trial.

Courts will evaluate a seizure under this test according to what a reasonable person would believe under the circumstances, and law enforcement officers will not be judged after-the-fact on how helpful the seized evidence actually was in apprehending or convicting a suspect. See Andresen v. Maryland, 427 U.S. 463, 483 (1976) (holding that the "trained special investigator reasonably could have believed" the seized evidence could be used to show criminal intent); United States v. Truitt, 521 F.2d 1174, 1176-78 (6th Cir. 1975) (holding that a reasonably cautious police officer could have believed under the circumstances that a sawed-off shotgun, although legal if registered, was incriminating evidence).

Of course, simply because an item is "evidence of a crime" does not mean that other restrictions may not apply. Law enforcement officials should be aware of other limits imposed by the Constitution, statutes, and regulations upon the seizure of evidence. See, e.g., Guidelines on Methods of Obtaining Documentary Materials Held by Third Parties, 28 C.F.R. 59.1-.6 (governing the application for search warrants for documentary evidence held by non-suspect third parties).

[page 31]

Although computers commonly contain evidence, sometimes they are evidence. If an extortionist sent a letter to his victim with unique print characteristics (e.g., the top half of the letter "W" was missing), his daisy~wheel printer would constitute evidence which could be seized.

E. TRANSPORTING HARDWARE FROM THE SCENE

Whether a computer is seized as contraband, an instrumentality, or evidence, it is important to transport it properly. With some simple computers, moving the equipment is a straightforward proposition. But computer systems are becoming so increasingly complex and diverse that it is harder than ever for technically untrained agents to avoid mistakes. These Guidelines cannot possibly substitute for the expertise that comes from special training courses in seizing, searching, and preserving electronic evidence. Indeed, the discussion that follows is meant only as introduction and orientation to these issues, and not as a comprehensive guide to all the technical contingencies which may arise during a search. The team for a computer-related search should, if possible, include at least one technically trained agent to act as a leader in these areas. Clearly, as complex computer systems become increasingly common, law enforcement agencies will need more trained agents at almost every crime scene. In the meantime, the following discussion may help prosecutors and investigators to anticipate the problems which can confront them.

First, agents must protect the equipment from damage. Second, to the extent they are transporting information storage devices (e.g., hard drives, floppy disks), improper handling can cause loss of data. Third, it may be impossible to make the system work in the field office, laboratory, or courtroom if the seizing agents did not carefully pack and move the computer system so that it can be successfully reassembled later.

Before the search begins, the search leader should prepare a detailed plan for documenting and preserving electronic evidence, and should take time to carefully brief the entire search team to protect both the identity and integrity of all the data. At the scene, agents must remember to collect traditional types of evidence (e.g., latent fingerprints off the keyboard) before touching anything. They must remember, too, that computer data can be destroyed by strong magnetic fields. (Low density magnetic media is more susceptible to such

interference than high density media.) Last, some computer experts will not examine evidence if anyone else has already tried to search or manipulate the data. Their chain-of-custody and integrity-of-evidence procedures will not allow them to examine the computer if its original crime-scene seal has been broken.

The agents executing the actual search must take special precautions when disassembling and packing computer equipment. This careful approach protects not only the hardware items, but also the integrity and accessibility of the data inside. Before disconnecting any cables, it is helpful to videotape or photograph the site (including the screen, if possible, and all wiring connections) and prepare a wiring schematic. This will document the condition of the equipment upon the agents' arrival and show how the system was configured. Agents should disconnect all remote access to the system (e.g., unplug the telephone cord, not the power cord, from the modem) and disconnect network cables from the servers so that no one can alter or erase information during the search. Investigators need to accurately label each cable and the device and port to which the cable connects before disconnecting anything. It is a good idea to attach tags at every connection point on every cable to record all relevant information. It is especially important to label every vacant port as "vacant" so that there is no confusion later. (If vacant ports are not labeled, it is impossible for an expert to tell whether the unlabeled port was in fact vacant, or whether an important label simply fell off.) Once this is done, agents are ready to disassemble, tag and inventory the equipment.

Investigators must determine which drives, disks, and other magnetic media need to be protected. If a hard disk drive is being moved, they must insure that the read/write heads are secured to prevent damage. Some systems secure (park) the heads automatically whenever the machine is not in use, but other systems may require that a specific command be executed or that the heads be secured mechanically. The manufacturer's operating manual should specify the proper procedure for each system.

Agents should protect floppy disk drives according to manufacturer's recommendations. Some suggest inserting a new diskette or piece of cardboard in the drive slot; others do not. (As with hard drives, each manufacturer's instructions may be found in the system manual). Investigators must also label diskettes (either individually or in groups), mark them as evidence and place them in non-plastic evidence containers.

[page 33]

Agents must be conscious of static electricity buildup during the execution of the warrant since static electricity can "zap" a disk and damage data. So can degaussing equipment (an electronic appliance that creates a strong magnetic field and can be used to effectively erase a magnetic tape or disk). A well-known story in law enforcement circles involves a hacker who allegedly magnetized his metal door frame, thus creating a magnetic field that erased magnetic media as agents carried it through the doorway. This story has not been verified and, even if true, such an event is unlikely to occur now because high density media is not easily disrupted by magnetic fields. Nonetheless, a device to measure magnetic fields (a compass or, even better, a gaussmeter) can determine whether such fields exist and, as a general rule, agents should avoid placing magnetic media near any strong magnetic field. Magnetic fields may be created by telephones, radio transmitters, and photocopiers. Additionally, although magnetic media has often been taken through airport metal detectors and X-ray machines without damage, it is wiser not to take magnetic media through these devices. (It is the motor driving the conveyor belt on the X-ray machine, not the fluoroscope itself, that creates the magnetic field which causes the damage.)

Transporting agents should keep all hardware and software in dust-free, climate-controlled environments. Computer-related evidence is sensitive to heat and humidity and should not be stored in the back seat or trunk of a car without special precautions. Temperature extremes may render magnetically stored evidence unreadable, and various types of contamination can damage electronic equipment. A safe range for storing magnetic media is between 40-90F and 20%-80% humidity, free of dust and

tobacco smoke.

[no page 34] [page 35]

IV. SEARCHING FOR AND SEIZING INFORMATION

A. INTRODUCTION

Hardware searches are not conceptually difficult. Like searching for weapons, the items sought are tangible. They occupy physical space and can be moved in familiar ways. Searches for data and software are far more complex. For purposes of clarity, these types of searches must be examined in two distinct groups: (1) searches where the information sought is on the computer at the search scene and (2) searches where the information sought has been stored off-site, and the computer at the search scene is used to access this off-site location.3

In some cases, the distinction is insignificant, and many topics covered in this section apply equally to both types of searches. On the other hand, there are certain unique issues that arise only when the computer is part of a network. For example, since Fed. R. Crim. P. 41(a) requires that a search warrant be issued by a court in the district where the property is located, agents may have to get a second warrant in another district if the target has sent data to a distant computer. See "Describing the Place to be Searched," infra p. 92.

Although "property" is defined in Federal Rule of Criminal Procedure 41(h) to include "documents, books, papers and other tangible objects," (emphasis added), courts have held that intangible property such as information may be seized. In United States v. Villegas, 899 F.2d 1324, 1334-35 (2d Cir.), cert. denied, 498 U.S. 991 (1990), the Second Circuit noted that warrants had been upheld for intangible property such as telephone numbers called from a given phone line and recorded by a pen register, conversations overheard by means of a microphone touching a heating duct, the movement of property as tracked by location-monitoring beepers, and images seized with video cameras and telescopes. The court in Villegas upheld a warrant which authorized agents to search a cocaine factory and covertly take photographs without authorizing the seizure of any tangible objects. But see United States

---

3 Any home PC can be connected to a network simply by adding a modem. Thus, in any ease where a modem is present, agents should consider the possibility that the computer user has stored valuable information at some remote location.

[page 36]

v. Johns, 948 F.2d 599 (9th Cir. 1991), cert. denied, 112 S. Ct. 3046 (1992) (a "sneak and peek" warrant executed without giving notice to the defendants that the search had occurred violated Rule 41(d)).

B. INFORMATION AS CONTRABAND

The same theories which justify seizing hardware--contraband or fruit of crime, instrumentality, or evidence--also apply to seizing information. See "Authority for Seizing Contraband or Fruits of Crime," supra p. 26. Because individuals often obtain copies of software in violation of copyright laws, it may be appropriate to seize that software as well as any documentation (such as photocopied software manuals) because they are likely to be illegally obtained. (Software producers may allow a purchaser to make a backup copy of the software bought, but these copies may not be disseminated because of copyright laws.) Lists of telephone card access codes and passwords for government computer networks may also be considered contraband, because their possession is prohibited by statute if the possessor has the requisite mens rea. 18 U.S.C. 1029(a)(3), 18 U.S.C. 1030(a)(6).

C. INFORMATION AS AN INSTRUMENTALITY

Rule 41(b) broadly defines what may be seized as an instrumentality: any "property designed or intended for use or which is or has been used as the means of committing a criminal offense." Fed. R. Crim. P. 41(b)(3). This includes both tangible and intangible property. See United States v. Villegas, supra, p. 35. Thus, in some cases, informational documents and financial instruments which have been used in the commission of an offense may be seized as instrumentalities of crime. Compare Abel v. United States, 362 U.S. 217, 237-9 (1960) (documents used in connection with suspect's illegal alien status were instrumentalities, including phony birth certificates, bank records,

[page 37]

and vaccination records) with Application of Commercial Inv. Co., 305 F. Supp. 967 (S.D.N.Y. 1969) ($5 million in securities were not instrumentalities where the government suspected improprieties with an $18,000 brokerage account and the securities were at most "incidental" to the offense).

Likewise, investigators should seize objects if they are "designed or intended for use" as instrumentalities. Fed. R. Crim. P. 41(b)(3).

Sometimes an item will obviously fit that description (like software designed to help hackers crack passwords or lists of stolen credit card numbers) but, at other times, it may not be so simple. Even so, as long as a reasonable person in the agent's position would believe the item to be an instrumentality, the courts will probably respect the agent's judgment. This is, after all, the same test used to determine when an object would aid apprehension or conviction of a criminal. See Andresen v. Maryland, 427 U.S. 463, 483 (1976). As such, the particular facts of the case are very important. For example, if an agent investigating the sysop of an illegal bulletin board knows that the board only operates on one personal computer, a second computer sitting in the same room is probably not an instrumentality. But if the agent has heard from a reliable informant that the suspect has boasted about expanding his operation to a second board, that second computer is probably "intended" as an instrumentality, and the agent should take it. Additionally, if the suspect has substantially modified a personal computer to enhance its usefulness for a particular crime (perhaps by installing password-cracking software), an agent might well reasonably believe that the computer and the software was "designed" for criminal activity.

D. INFORMATION AS EVIDENCE

Before the Supreme Court's rejection of the "mere evidence" rule in Warden v. Hayden, 387 U.S. 294, 300-301 (1967), courts were inconsistent in ruling whether records that helped to connect the criminal to the offense were instrumentalities of crime (and thus seizable), or were instead merely evidence of crime (and thus not seizable). Compare Marron v. United States, 275 U.S. 192 (1927) (approving prohibition agent's seizure of bills and ledger books belonging to speakeasy operators as instrumentalities of crime) with United States v. Lefkowitz, 285 U.S. 452 (1932)(disapproving prohibition agent's seizure of papers intended to solicit orders for illegal liquor). Indeed, several courts have concluded that, when it comes to documents, it is impossible to

separate the two categories. See Hayden, 387 U.S. at 302 (stating that the distinction between mere evidence and instrumentalities "is wholly irrational, since, depending on the circumstances, the same `papers and effects' may be `mere evidence' in one case and `instrumentality' in another"); United States v. Stern, 225 F. Supp. 187, 191 (S.D.N.Y. 1964) ("It would be hazardous to attempt any definition [of papers that are instrumentalities of crime and not mere evidence]; we shall not."). Now that evidence of crime may be seized in the same way as instrumentalities of crime, it is useful to acknowledge that, in most instances, documents and other information connecting the criminal to his offense should be

viewed as evidence of the crime, and not as instrumentalities. For example, in United States v. Lindenfield, 142 F.2d 829, 830-32 (2d Cir.), cert. denied, 323 U.S. 761 (1944), the prescription records of a doctor who illegally prescribed morphine to "patients" were classified as evidence, not as instrumentalities.

The prescription records in Lindenfield illustrate the sort of document that may be seized as evidence: records that reveal the operation of the criminal enterprise over time. Other examples include the customer lists of narcotics traffickers, telephone bills of hackers who break into computer networks, and plans for the fraud or embezzlement of corporate and financial targets. This documentary evidence may be in paper or book form, or it may be stored electronically in a computer or on a backup tape. As with other types of evidence, documents may be seized if they aid in showing intent and the absence of mistake on the suspect's part, even though they may not relate directly to the commission of the crime, but to some other similar transaction instead. See Andresen v. Maryland, 427 U.S. 463, at 483-84 (1976)(approving seizure of documents about a second transaction because they showed criminal intent and absence of mistake in the first transaction).

1. Evidence of Identity

Evidence of a crime also includes various types of identification evidence. For example, courts have recognized that clothing seen worn by a criminal during the commission of the offense constitutes evidence of the crime,

because it helps to tie the suspect to the crime. See, e.g., United States v. Korman, 614 F.2d 541, 547 (6th Cir.)(approving the seizure of a green ski jacket as both evidence of and an instrumentality of the crime), cert. denied, 446 U.S. 952 (1980).

Documents that incriminate a suspect's co-conspirators also may be seized as evidence because they help identify other involved parties and connect them with the suspect. See, e.g., United States v. Santarsiero, 566 F. Supp. 536, 544 (S.D.N.Y. 1983) (approving the seizure of the suspect's notebook in a counterfeit credit card investigation where others were working with or purchasing cards from him, and the notebook contained telephone numbers that the investigating officers could reasonably believe would help in identifying and connecting others with the suspect's crimes). In many computer crimes, we have found that hackers work jointly and pool hacking information. In these cases, telephone records may prove this connection. Moreover, agents may seize evidence

that helps identify the occupant of a home or office connected to the crime, where the home or office is used regularly by more than one person. See, e.g., United States v. Whitten, 706 F.2d 1000, 1008-09 (9th Cir. 1983)(approving the seizure of telephone books, diaries, photos, utility bills, telephone bills, personal property, cancelled mail, keys, rent receipts, deeds, and leases that helped establish who owned and occupied premises used for a large scale narcotics operation, where the premises were used by more than one person and the warrant authorized seizing items "indicating the ownership or occupancy of the residence"), cert. denied, 465 U.S. 1100 (1984). As with houses and offices, computers are often used by more than one person, and this sort of evidence may help establish just who used the computer or computers to commit the crime.

2. Specific Types of Evidence

a. Hard Copy Printouts

Any information contained in a computer system may have been printed out by the target of the investigation. Finding a printed copy may be valuable for a number of reasons. First, a printout may display an earlier version of

[page 40]

data that has since-been altered or deleted. Second, in certain electronic environments (such as bulletin boards), individuals may claim to lack knowledge about what information is electronically stored in the computer (e.g., a bulletin board operator may disavow any knowledge that his board contained illegal access codes that were posted and downloaded by others). Finding printed copies in someone's possession may negate this defense. Third, the printouts may tie the crime to a particular printer which, in turn, may be seizable as an instrumentality (e.g., the printouts may reveal that extortionate notes were printed on a certain printer, thus warranting seizure of the printer).

b. Handwritten Notes

Finally, agents should be alert for notes in manuals, on the equipment, or in the area of the computer. These may provide critical keys to breaking passwords, finding the file or directory names of important data, operating the hardware or software, identifying the suspect's electronic or telephone connections with co-conspirators and victims, or finding login names or accounts.

E. PRIVILEGED AND CONFIDENTIAL INFORMATION

1. In General

Warrants to search computers which contain privileged information must meet the same requirements as warrants to search for and seize paper documents under similar conditions; that is, the warrant should be narrowly drawn to include only the data pertinent to the investigation, and that data should be described as specifically as possible. See, e.g. Klitzman v. Krut, 744 F.2d 955 (3d Cir. 1984). Since a broad search of computers used by confidential fiduciaries (e.g., attorneys or physicians) is likely to uncover personal information about individuals who are unconnected with the

[page 41]

investigation, it is important to instruct any assisting forensic computer experts not to examine files about uninvolved third parties any more than absolutely necessary to locate and seize the information described in the warrant.

a. Doctors, Lawyers, and Clergy

Federal law recognizes some, but not all, of the common law testimonial privileges. Fed. R. Evid. 501. Indeed, Congress has recognized a "special concern for privacy interests in cases in which a search or seizure for .... documents would intrude upon a known confidential relationship such as that which may exist between clergyman and parishioner; lawyer and client; or doctor and patient." 42 U.S.C. 2000aa-11(1)(3). At Congress's direction, see 42 U.S.C. 2000aa-11(a), the Attorney General has issued guidelines for federal officers who want to obtain documentary materials from disinterested third parties. 42 U.S.C. 2000aa-11. Under these rules, they should not use a search warrant to obtain documentary materials believed to be in the private possession of a disinterested third party physician, lawyer, or clergyman where the material sought or likely to be reviewed during the execution of the warrant contains confidential information on patients, clients, or parishioners. 28 C.F.R. 59.4(b). A search warrant can be used, however, if using less intrusive means would substantially jeopardize the availability or usefulness of the materials sought; access to the documentary materials appears to be of substantial importance to the investigation; and the application for the warrant has been recommended by the U.S. Attorney and approved by the appropriate Deputy Assistant Attorney General. 28 C.F.R. 59.4(b)(1) and (2).

b. Publishers and Authors

Additionally, Congress has expressed a special concern for publishers and journalists in the Privacy Protection Act, 42 U.S.C. 2000aa. Generally speaking, agents may not search for or seize any "work product materials" (defined by statute) from someone "reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. 2000aa(a). In addition, as an even

[page 42]

broader proposition, government officers cannot search for or seize "documentary materials" (also defined) from someone who possesses them in connection with a purpose to similarly publish. 42 U.S.C. 2000aa(b). These protections do not apply to contraband, fruits of a crime, or things otherwise criminally possessed. 42 U.S.C. 2000aa-7.

Although this provision may seem, at first blush, to have a somewhat limited application for law enforcement, it has emerged as a frequent issue in computer searches. Because even a stand-alone computer can hold thousands of pages of information, it is common for users to mix data so that evidence of crime is commingled with material which is innocuous--or even statutorily protected. And as a technical matter, analysts sometimes cannot recover the electronic evidence without, in some manner, briefly searching or seizing the protected data. Moreover, this problem becomes exponentially more difficult, both legally and practically, if the target computers are part of a network which holds the work of many different people. The larger the network and the more varied its services, the harder it is to predict whether there might be information on the system which could arguably qualify for statutory protection. (This complex area of the law is discussed in detail at "THE PRIVACY PROTECTION ACT, 42 U.S.C. 2000aa," infra p. 72. It is critical that prosecutors and agents read this section and the statute with care before undertaking a search which may intrude on protected materials.)

2. Targets

If the person who holds the documents sought is not "disinterested" but a target of the investigation, the rules are understandably different. In those cases, agents may get a warrant to search the files for confidential information (regardless of whether that information is technically "privileged" under Federal law), but the warrant should be drawn as narrowly as possible to include only information specifically about the case under investigation.

When the target of an investigation has complete control of the computer to be searched (such as a stand-alone PC), it may be difficult to find

all the evidence without examining the entire disk drive or storage diskettes. Even in situations like these, it may be possible to get other people in the suspect's office to help locate the pertinent files without examining everything. When a

[page 43]

computer must be removed from the target's premises to examine it, agents must take care that other investigators avoid reading confidential files unrelated to the case. Before examining everything on the computer, analysts should try to use other methods to locate only the material described in the warrant. Finally, as experts comb for hidden or erased files or information contained between disk sectors, they must continue to protect the unrelated, confidential information as much as possible.

3. Using Special Masters

In rare instances, the court may appoint a special master to help search a computer which contains privileged information. See, e.g., DeMassa v. Nunez, 747 F.2d 1283 (9th Cir. 1984). A neutral master would be responsible to the court, and could examine all the documents and determine what is privileged. If the court appoints a master, the government should ask for a neutral computer expert to help the master recover all the data without destroying or altering anything. In cases like these, the computer expert needs detailed instructions on the search procedures to be performed. In no event should the target of the search or his employees serve as the master's computer expert.

F. UNDERSTANDING WHERE THE EVIDENCE MIGHT BE: STAND- ALONE PCs, NETWORKS AND FILE-SERVERS, BACKUPS, ELECTRONIC BULLETIN BOARDS, AND ELECTRONIC MAIL

1. Stand-Alone PCs

When searching for information, agents must not overlook any storage devices. This includes hard drives, floppy disks, backup tapes, CD-ROMs4,

[page 44]

WORM drives 5, and anything else that could hold data. In addition, notwithstanding the high-tech nature of computer searches, investigators must remember basic evidentiary techniques. If identification is an issue, they should look for fingerprints or other handwritten notes and labels that may help prove identity. If data is encrypted, a written copy of the password is clearly important.

---

4 CD-ROM stands for Compact Disk--Read Only Memory. Much like a compact disk for music, it allows the user to search for and read information without being able to alter it.

5 WORM stands for Write Once Read Many. The user can write large amounts of information to a platter (a large disk); but once written, the platter can only be read, not altered.

a. Input/Output Devices: Do Monitors, Modems, Printers, and Keyboards Ever Need to be Searched?

Prosecutors must always keep in mind the independent component doctrine (supra p. 25); that is, there must be a basis for seizing each particular item. If agents are only searching for information, it may be senseless to seize hardware that cannot store information.

That said, it is important to remember that information can be retrieved from many hardware devices, even those not normally associated with a storage function. Generally speaking, input and output (I/O) devices such as keyboards, monitors, and printers do not permanently store data. Most data is stored on devices such as hard drives, CD-ROMs, and floppy disks. By contrast, I/O devices are used to send data to, and receive data from, the computer. Once the computer is turned off, I/O devices do not store information. For example, when a computer is turned off, the information on the screen is lost unless it has been saved to a storage device.

However, there are significant exceptions to this general rule. A trained computer specialist, using specialized techniques, may find data or other evidence even on I/O devices. The following list is not all-inclusive, but rather offers some examples of I/O devices that may provide useful evidence even after they have been turned off.

(1) Laser printers -- It may be possible to search for images of the last page printed on laser printers. This technique requires planning because the expert must examine the printer before it is moved. If this type of evidence may be needed, a computer expert must be ready at the

scene with the necessary equipment. Additionally, paper containing information may still be inside a laser printer due to a paper jam that was not cleared.

(2) Hard disk print buffers -- Some laser printers have five- or

ten-megabyte hard drives that store an image before it prints, and the information will stay on the drive until the printer runs out of memory space and writes over it. One example of a printer that may have an internal hard drive is the Qume 1000 Color Printer. An expert would be able to search the hard drive for information sent to and stored by that printer.

(3) Print Spooler Device -- This device holds information to be printed. The spooler may be holding a print job if the printer was not ready to print when the print command was given (e.g., the printer was not turned on or was out of paper). This device should be handled at the scene since the information will be lost when power is disrupted.

(4) Ribbon printers -- Like old typewriter ribbons, printer ribbons contain impressions from printed jobs. These impressions can be recovered by examining the ribbon.

(5) Monitors -- Any burning of the screen phosphorus may reveal data or graphics commonly left on the screen.

(6) Keyboards -- Although they do not normally store information, some unusual keyboards are actually computer workstations and may contain an internal diskette drive.

(7) Hard Cards -- These appear to be a typical function board but they function like a hard disk drive and store information.

(8) Scanner -- Flatbed type scanners may have hard paper copy underneath the cover.

(9) Fax machines -- Although some kinds of stand-alone fax machines simply scan and send data without storing it, other models can store the data (e.g., on a hard drive) before sending it. Significantly, the data remains in the machine's memory until overwritten. Some fax machines contain two or more megabytes of memory--enough to hold hundreds of pages of information.

[page 46] b. Routine Data Backups

Even on stand-alone systems, computer users often make backup copies of files to protect against hardware failure or other physical disruptions. If the computer has any sort of failure which destroys the original copy of data or programs (e.g., a hard disk failure), the data can then be restored from the backups. How often backups are made is solely up to the user. As a practical matter, however, most computer-literate users will back up data regularly since mechanical failures are not uncommon and it

is often difficult and time~-consuming to recreate data that has been irretrievably lost. Backup copies can be made on magnetic tape, disks, or cartridges.

2. Networked PCs

Increasingly, computers are linked with other computers. This can be done with coaxial cable in a local area network, via common telephone lines, or even through a wireless network, using radio frequency (RF) communications. Due to this interconnectivity, it has become more important than ever to ascertain from sources or surveillance what type of system agents will encounter. Without knowing generally what is there before the search, investigators could end up with nothing more than a "dumb terminal" (no storage capability) connected to a system which stores the files in the next county or state. It would be akin to executing a search warrant for a book~making operation on a vacant room that only has a phone which forwards calls to the actual operation site. During the planning stage of a search, the government must consider the possibility of off-site storage locations.

The following are systems or devices which make it possible for a suspect to store data miles, or even continents, away from her own computer:

FILE SERVER: A file server is a computer on a network that stores the programs and data files shared by the users of the network. A file server acts like a remote disk drive, enabling someone to store information on a computer system other than his own. It can be located in another judicial district from the target machine. [page 47]

ELECTRONIC MAIL: Electronic mail provides for the transmission of messages and files between computers over a communications network. Sending information in this way is similar in some ways to mailing a letter through the postal service. The messages are sent from one computer through a network to the electronic address of another specific computer or to a series of computers of the sender's choice. The transmitted messages (and attached files) are either stored at the computer of the addressee (such as someone's personal computer) or at a mail server (a machine dedicated, at least in part, to storing mail). If the undelivered mail is stored on a server, it will remain there until the addressee retrieves it. When people "pick up" e-mail from the mail server, they usually receive only a copy of their mail, and the stored message is maintained in the mail server until the addressee deletes it (some systems allow senders to delete mail on the server before delivery). Of course, deleted mail may sometimes be recovered by undeleting the message (if not yet overwritten) or by obtaining a backup copy (if the server was backed up before the message was deleted).

ELECTRONIC BULLETIN BOARD SYSTEMS (BBS): A bulletin board system is a computer dedicated, in whole or in part, to serving as an electronic meeting place. A BBS computer system may contain information, programs, and e-mail, and is set up so that users can dial the bulletin board system, read and leave messages for other users, and download and upload software programs for common use. Some BBSs also have gateways which allow users to connect to other bulletin boards or networks. A BBS can have multiple telephone lines (so that many people can use it at the same time) or a single line where a user's access is first-come, first-served. BBSs can have several levels of access, sometimes called "sub-boards" or "conferences." Access to the different conferences is usually controlled by the system operator with a password system. A single user may have several different passwords, one for each different level or conference. A user may store documents, data, programs, messages, and even photographs in the different levels of the BBS.

A bulletin board system may be located anywhere telephone lines go. Therefore, if a suspect may have stored important information on a BBS, a pen register on the suspect's phone may reveal the location of these stored files. Agents must be careful, though, because sysops have been known to forward incoming calls through a simple phone in one spot to

their BBS computers somewhere else. Sometimes these calls hop between houses, and sometimes, between jurisdictions. Investigators cannot assume that the phone number called by the suspect is always the end of the line.

VOICE-MAIL SYSTEMS: A voice-mail system is a complex phone answering machine (computer) which allows individuals to send and receive telephone voice messages to a specific "mailbox" number. A person can call the voice-mail system (often a 1-800 number) and leave a message in a particular person's mailbox, retrieve messages left by other people, or transfer one message to many different mailboxes in a list. Usually, anyone can leave messages, but it takes a password to pick them up or change the initial greeting. The system turns the user's voice into digital data and stores it until the addressee erases it or another message overwrites it. Criminals sometimes use voice mailboxes (especially mailboxes of unsuspecting people, if the criminals can beat the mailbox password) as remote deaddrops for information which may be valuable in a criminal case. Voice mailboxes are located in the message system computer of the commercial vendor which supplies the voice-mail service, or they can be found on the computer at the location called. Voice mail messages can be written on magnetic disk or remain in the

computer's memory, depending on the vendor's system.

Of course, all networked systems, whether data or voice, may keep routine and disaster backups.

a. Routine Backups

Making backups is a routine, mandatory discipline on multi-user systems. On larger systems, backups may be created as often as two to three times per working shift. Usually backups are made once per day on larger systems and once per week on smaller ones. Backups are usually stored in a controlled environment to protect the integrity of the data (e.g., locked in a file cabinet or safe). The system administrators will usually have written procedures which set out how often backup copies will be made and where they will be kept. Backups for large systems are often stored at remote locations.

[page 49]

b. Disaster Backups

These are additional backups of important data meant to survive all contingencies, such as fire, flood, etc. As extra protection, the data is stored off-site usually in another building belonging to the business or in rented storage space. It would be unusual to find the disaster backups near the routine backups or original data. Again, these copies can be stored on diskettes, magnetic tape, or cartridge.

G . SEARCHING FOR INFORMATION

1. Business Records and Other Documents

Obtaining records from a multi-user computer system raises certain issues that are uncommon in the paper world. When dealing with papers stored in filing cabinets, agents can secure the scene and protect the integrity of the evidence by physically restricting access to the storage container and its papers. Electronic records are, of course, easier to alter or destroy. More important, such alteration or destruction may occur while the agent is looking at a copy of the document on A workstation terminal. Therefore, it is important to control remote access to data while the search is being conducted. This can often be done by prohibiting access to the file or file server in question, either by software commands or by physically disconnecting cables. This should only be done by an expert, however, because altering the system's configuration may have significant unintended results.

If the system administrator is cooperating with investigators, the task becomes much easier, and agents should use the least intrusive means possible to obtain the data (e.g., a request, grand jury subpoena, or administrative subpoena). Of course, if the entire business is under investigation or there is reason to believe that records may be altered or destroyed, a search warrant should be used.

[page 50]

2. Data Created or Maintained by Targets

Targets of criminal investigations, particularly computer crimes, may have data on a multi-user computer system. Where the target owns or operates the computer system in question, it is safest to use warrants, although subpoenas may be appropriate in the right case.

Where the target does not control the system but merely has data on it, the sysop may be willing to provide the requested data assuming he has the authority to do so. Never forgetting the legal restraints of 18 U.S.C. 2702 (see "Stored Electronic Communications," infra p. 85), the sysop can, as a practical matter, probably retrieve the needed data rather easily. Ordinarily, a multi-user computer system will have specific accounts assigned to each user or groups of users. While the various "users" may not be able to get into each others' files, the system operator (like a landlord with passkeys) can usually examine and copy any file in the computer system. (Typically, the sysop has what is called "superuser" authority or "root" access.)

Some systems, by their rules, may prohibit the system managers or operators from reading files in specific data areas or may expressly limit the purposes for which sysops may exercise their access. In those cases, sysops may insist on a court order or subpoena. If, on the other hand, users have consented to complete sysop access in order to use the system, a request to the sysop for the information may be all that is required. In either event, rarely will it be wise for investigating agents to search large computer systems by themselves. Without the sysop's help, it may be difficult (if not impossible) for agents to comb a multi-user computer system the way they search file cabinets for paper records.

When using a subpoena with a future return date, agents should specifically ask for the computerized records as they exist at time of service, and state clearly that service of the subpoena obliges the recipient to preserve and safeguard the subpoenaed information by making a copy. Investigators should explain that even if the recipient contests the subpoena, he must not only copy the data "as is," but must

also confirm to the agent that the copy has been made. The subpoena should also say that failure to preserve the subpoenaed information may subject the recipient to sanctions for contempt. In some

[page 51]

circumstances, a "forthwith subpoena" may even be appropriate. If all this is not done, the data may be altered or erased--deliberately, accidentally, or in the normal course of business--before the return date on the subpoena.

3. Limited Data Searches

Once analysts have determined the operating system and have taken precautions to protect the integrity of the data, they will select tools to aid in the search. Using specially designed software called "utilities" will greatly help, because analysts can tailor the search to look for specified names, dates, and file extensions. They can scan disks for recently deleted data and recover it in partial or sometimes complete format. They can also identify and expose hidden files. In some cases, analysts may find files that are not in a readable format; the data may have been compressed to save space or encrypted to control access to it. Here again, utility packages will help recover the data. In designing the data search, they might use a variety of utilities. Some are off~the-shelf software available from most computer retailers. But utility software can also be custom-made, especially designed to perform specific search functions that are specified in standard laboratory procedures. Obviously, agents should rely upon experts for this kind of analysis. (See APPENDIX C, p. 143, for a list of federal sources for experts.)

There are several reasons why analysts will probably want to do a limited rather than a complete search through the data. First of all, the law in general prefers searches of all things--computer data included--to be as discrete and specific as possible. Second, the warrant may specify particular files, directories, or sub-directories, or certain categories of data. Finally, even if the facts of a case give an analyst free rein to search all the data, the economies of scale usually require a more systematic approach. At the least, analysts should plan for a methodical inventory of directories and sub-directories and prepare to document all the steps taken in the search. Because data is so easy to alter or destroy, analysts must have a careful record so that their efforts can be re~created for a court. In examining the data, analysts will probably have to do some sorting--examining things that could be relevant and by-passing the unrelated items. Only rarely will they be allowed to or even want to read everything on the computer system being searched. Even

so, caution is advised, because directory headings and file names may often be misleading.

[page 52]

In addition to searching by file, sub-directory, or directory, the power of the computer allows analysts to design a limited search in other ways as well. Computer experts can search data for specific names (like names of clients, co~conspirators, or victims), words (like "drugs," "tax," or "hacking"), places (either geographic locations or electronic ones), or any combination of them. As legal researchers know, if the keyword search is well defined, it can be the most efficient way to find the needle in the haystack. But unless analysts are working from a tip and know how the data is organized, there will probably be some trial and error before they can find the key words, names, or places. In addition, technical problems may complicate a keyword search. For example, encryption, compression, graphics, and certain software formatting schemes may leave data difficult to search in this fashion.

In the list of files contained in a directory or sub-directory, there will be other kinds of information that may indicate whether a particular file should be searched. The names of files in a directory often carry extensions that indicate what sort of file is or what it does. These file extensions are often associated with common applications software, such as spreadsheets (that could hold accounting data), databases (that can have client information), word processing (which could hold any sort of alphanumeric text), or graphics. There will also be a date and time listed for every file created. Although this information can easily be altered and may be misleading, in some cases it may accurately reflect the last time the file was revised.

Further, the kind of software found loaded on a computer may reveal how the computer has been used. If there is communications software, for example, the computer may have been used to send incriminating data to another computer system at another location. A modem or other evidence of remote access should also tip off the searcher to this possibility, which may expand the investigation and create a need for a new warrant. For example, the original search may disclose phone bills indicating frequent long-distance calls to one particular number. If a call to this number reveals a modem tone, then further investigation would be warranted.

Clearly, the person conducting a computer search should have high-level technical skills to ensure success. Moreover, a well-meaning investigator with amateur skills could inadvertently, but irretrievably, damage the data. When in doubt, rely only on experts.

[page 53]

4. Discovering the Unexpected

a. Items Different from the Description in the Warrant

The Fourth Amendment requires specific descriptions of the places, people, and things to be searched as well as the items to be seized. Specificity has two aspects--particularity and overbreadth. "Particularity" is about detail: the warrant must clearly describe what it seeks. "Breadth" is about scope: the warrant cannot include items for which there is no probable cause. Together, the particularly and breadth limitations prevent general searches of a person's properly. Thus, generic classifications in a warrant are acceptable only when a more precise description is not possible. In Re Grand Jury Subpoenas, 926 F.2d 847, 856-7 (9th Cir. 1991).

Despite defense objections, the court upheld the seizure of computer disks not named in the warrant in United States v. Musson, 650 F. Supp. 525, 532 (D. Colo. 1986). The warrant in that case authorized agents to seize various specific records, and the court reasoned that because of the changing technology, the government could not necessarily predict what form the records would take. See also United States v. Reyes, 798 F.2d 380, 383 (10th Cir. 1986); United States v. Lucas, 932 F.2d 1210, 1216 (8th Cir.), cert. denied, 112 S. Ct. 399 (1991). In these days, the safest course is always to assume that particular, clearly described "records" or "documents" may be in electronic form and to provide for this possibility in the warrant. (See "SAMPLE COMPUTER LANGUAGE FOR SEARCH WARRANTS," APPENDIX A, p. 125.)

Other courts, however, have suppressed the results of search warrants which broadly covered electronic "records" in form, but were too vague about their content. In Application of Lafayette Academy, Inc., 610 F.2d 1 (1st Cir. 1979), the court struck a warrant which expressly authorized the seizure of computer tapes, disks, operation manuals, tape logs, tape layouts, and tape printouts. Although the warrant specified that the items must also be evidence of criminal fraud and conspiracy, that limit on content was not sufficiently particular to save the evidence. Id. at 3. See also Voss v. Bergsgaard, 774 F.2d 402, 404-5 (10th Cir. 1985).

[page 54]

b. Encryption

If agents have authority to search the data in a computer or on a disk and find it has been encrypted, how should they proceed--both legally and

practically?

Although an encrypted computer file has been analogized to a locked file cabinet (because the owner is attempting to preserve secrecy), it is also analogous to a document written in a language which is foreign to the reader. As both of these metaphors demonstrate, the authority granted by the warrant to search for and seized encrypted information also brings the implied authority to decrypt: to "break the lock" on the cabinet or to "translate" the document. Indeed, a warrant to seize a car and its contents implicitly authorizes agents to unlock it.

Of course, the rule may be different if the search is based upon consent. A court might well find that a target who has encrypted his data and has not disclosed the necessary password has tacitly limited the scope of his consent. In that case, the better practice is to ask explicitly for consent to search the encrypted material, as well as the password. If the target refuses, agents should obtain a warrant for the encrypted data.

In United States v. David, 756 F. Supp. 1385 (D. Nev. 1991), the defendant was cooperating with the government by giving them drug-dealing information from encrypted files in his computer memo book. During one interview, the agent learned the defendant's password by standing over his shoulder and watching as he typed it. Later, when the defendant stopped cooperating and started destroying information in the notebook, the agent seized it and used the defendant's password to access the remaining information. The court reasoned that the agent's learning the password was like his picking up the key to the container. When the defendant withdrew his consent to give more information from the memo book, the act which required a warrant was looking inside the container--whether locked or unlocked--not the acquisition or even the use of the key. If the agent did not have authority to search the data, then knowing the password would not confer it. Id. at 1391. Conversely, if the agent does have a warrant for the data, she may break the "lock" to search it. For more comment on the consent issues in the David case, see the discussion at p. 14.

[[page 55]

As a practical matter, getting past the encryption may not be easy, but there are several approaches to try. First of all, the computer crime lab or the software manufacturer may be able to assist in decrypting the file. Investigators should not be discouraged by claims that the password "can't be broken," as this may simply be untrue. Some can be done easily with the right software. If that fails, there may be clues to the password in the other evidence seized--stray notes on hardware or desks; scribbles in the margins of manuals or on the jackets of disks. Agents

should consider whether the suspect or someone else will provide the password if requested. In some cases, it might be appropriate to compel a third party who may know the password (or even the suspect) to disclose it by subpoena (with limited immunity, if appropriate).

H. DECIDING WHETHER TO CONDUCT THE SEARCH ON-SITE OR TO REMOVE HARDWARE TO ANOTHER LOCATION

It is possible for analysts to search for electronic evidence in several places: on-site, at an investigative agency field office, or at a laboratory. The key decision is whether to search at the scene or somewhere else, since an off~-site search will require packing and moving the property and may constitute a greater intrusion on the property rights of the computer owner/user.6 In addressing this issue, it is necessary to consider many factors such as the volume of evidence, the scope of the warrant, and the special problems that may arise when attempting to search computers.

Although it may, practically speaking, be necessary to remove the computer in order to search it, that logistical reality does not expand the theoretical basis of probable cause. This is a completely separate issue, and agents must not write broad warrants simply because, in reality, it will be necessary to seize the entire filing cabinet or computer. Rather, they should draft the warrant for computer records as specifically as possible (akin to a search warrant papers in a file cabinet) by focusing on the content of the record. Then, as a separate logical step, they should address the practical aspects of each case: whenever searching data "containers" on site would be unreasonable, agents should explain in the affidavit why this is true and ask for

permission to seize the containers in order to find the relevant documents. (See "DRAFTING A WARRANT TO SEIZE INFORMATION: Describing the Items to be Seized," infra p. 97.) (If the particular computer storage devices which contain the evidence may also hold electronic mail protected by 18 U.S.C. 2701, et seq., see STORED ELECTRONIC COMMUNICATIONS," infra p. 85. If they may contain material covered by the Privacy Protection Act, 42 U.S.C. 2000aa, see "THE PRIVACY PROTECTION ACT," infra p. 72.)

1. Seizing Computers because of the Volume of Evidence

Since any document search can be a time-consuming process, cases discussing file cabinet searches are helpful. Although not technically complex, it can take days to search a file cabinet, and courts have

sustained off-site searches when they are "reasonable under the circumstances." The key issues here are: (1) how extensive is the warrant and (2) what type of place is to be searched.

---

6. If hardware is going to be removed from the site, refer to the suggestions on packing and moving hardware, supra p. 31.

a. Broad Warrant Authorizes Voluminous Seizure of Documents

In determining whether agents may take documents from the scene for later examination, they must consider the scope of the warrant. When the warrant directs agents to seize broad categories of records, or even all records (because the suspect's business is completely criminal or infected by some pervasive, illegal scheme), then it is not difficult to argue all papers and storage devices should be seized. In these cases, courts have supported the carting off of whole file cabinets containing pounds of unsorted paper. U.S. Postal Service v. C.E.C. Services, 869 F.2d 184, 187 (2d Cir. 1989); United States v. Sawyer, 799 F.2d 1494, 1508 (11th Cir. 1986), cert. denied sub nom. Leavitt v. U.S. , 479 U.S. 1069 (1987). "When there is probable cause to seize all [items], the warrant may be broad because it is unnecessary to distinguish things that may be taken from things that must be left undisturbed." U.S. v. Bentley, 825 F.2d 1104, 1110 (7th Cir.), cert. denied, 484

[page 57]

U.S. 901 (1987). In such cases, it is not necessary to carefully sort through documents at the scene to insure that the warrant has been properly executed.

This rationale has been extended to computers. In U.S. v. Henson, 848 F.2d 1374 (6th Cir. 1988), cert. denied, 488 U.S. 1005 (1989), agents searched several used car dealerships for evidence of an interstate odometer roll-back scheme. The warrant authorized agents to seize, among other things, "modules, modems and connectors, computer, computer terminals, hard copy user documentation pertaining to files and/or programs, cables, printers, discs, floppy discs, tapes, vendor phone numbers, all original and backup tapes and discs, any other informational data input, all vendor manuals for hardware and software, printouts...." Id. at 1382. The warrant did not require on-site sorting, and the defendants later accused agents of going on a "seizing frenzy." The court, however, sustained the search, observing that the extensive seizures were authorized by the warrant, and the warrant was broad

because so was the criminality. The court relied on the rule of reasonableness in concluding that officers were right not to try to sort through everything at the scene. Since the extensive seizure of records was authorized by the terms of the warrant, it was inevitable that the officers would seize documents that were not relevant to the proceedings at hand. We do not think it is reasonable to have required the officers to sift through the large mass of documents and computer files found in the Hensons' office, in an effort to segregate those few papers that were outside the warrant.

Id. at 1383-4 (emphasis added).

Although the Henson defendants argued that agents seized items not covered by the warrant, this did not invalidate the search. As noted by the court,

A search does not become invalid merely because some items not covered by a warrant are seized.... Absent flagrant disregard for the limitations of a search warrant, the items covered by the warrant will be admissible.

Id. at 1383 (citations omitted). See also U.S. v. Snow, 919 F.2d 1458, 1461 (10th Cir. 1990).

[page 58]

The Eleventh Circuit expressed a similar rule of reasonableness in United States v. Wuagneux, 683 F.2d 1343, 1353 (11th Cir. 1982), cert. denied, 464 U.S. 814 (1983). In Wuagneux, a dozen agents searched the records of a business for a day and a half, and seized between 50,000 and 100,000 documents (approximately one to two percent of those on the premises). Defendants complained that the agents should not have removed whole files or folders in order to take a particular document, but the court disagreed: "To require otherwise `would substantially increase the time required to conduct the search, thereby aggravating the intrusiveness of the search,' " citing United States v. Beusch, 596 F.2d 871, 876-7 (9th Cir. 1979). The Eighth Circuit reached the same conclusion in Marvin v. U.S. , 732 F.2d 669 (8th Cir. 1984), where agents searched a clinic for financial information related to tax fraud. The agents seized many files without examining the contents at the scene, intending to copy and sort them later. Although the agents seized some files that were completely outside the warrant, the district court's remedy, upheld on appeal, was to order return of the irrelevant items. The agents' decision not to comb through all the files at the scene, the court noted, was "prompted largely by practical considerations and time constraints." Id. at 675. Accord Naugle v. Witney, 755 F. Supp. 1504, 1516 (D. Utah 1990)(Removing an entire filing cabinet, including items not described in the warrant,

was reasonable since the alternative would require officers to remain on the premises for days, a result less reasonable and more intrusive.)

b. Warrant is Narrowly Drawn but Number of Documents to be Sifted through is Enormous

The more difficult cases are those in which the sought-after evidence is far more limited and the description in the warrant is (and should be) more limited as well. "When the probable cause covers fewer documents in a system of files, the warrant must be more confined and tell the officers how to separate the documents to be seized from others." United States v. Bentley, supra, at 1110.

The problem of the narrowly drawn, tightly focused warrant is illustrated by U.S. v. Tamura, 694 F.2d 591 (9th Cir. 1982). Because agents knew exactly what records they sought at a particular business, they were able (and it was reasonable for them) to draft the warrant very specifically. But it

[page 59]

was much easier to describe the records than to find them, especially when the company employees refused to help. In the end, the agents simply took all the records including eleven boxes of computer printouts, 34 file drawers of vouchers, and 17 drawers of cancelled checks. Unlike most other cases that address these issues, this court faced a seizure where most of the documents taken were outside the warrant. It concluded, therefore, that "the wholesale seizure for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as `the kind of investigatory dragnet that the Fourth Amendment was designed to prevent.'" Id. at 595 (citations omitted). Although the court found reversal was not compelled (because the government had been "motivated by considerations of practicality"), it also found this a "close case." Their advice for law enforcement is concrete:

In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the Government and law enforcement officials generally can avoid violating Fourth Amendment rights by sealing and holding the documents pending approval by a magistrate of a further search, in accordance with the procedures set forth in the American Law Institute's Model Code of Pre-Arraignment Procedure. If the need for transporting the documents is known to the officers prior to the search, they may apply for specific authorization for large-scale removal of material, which should be granted by the magistrate issuing the warrant only where on-site sorting

is infeasible and no other practical alternative exists.

Id. at 595-6 (footnote omitted).

c. Warrant Executed in the Home

When a search is conducted at a home instead of a business, courts seem more understanding of an agent's predilections to seize now and sort later. In United States v. Fawole, 785 F.2d 1141, 1144 (4th Cir. 1986), ten agents had searched the defendant's home for three and a half hours removing, among other things, 350 documents. Almost half of those papers were in a briefcase, which the agents seized without sorting. Although many things in the briefcase

[page 60]

were outside the scope of the warrant, the court found that, under the circumstances, the seizure did not amount to a general, exploratory rummaging in a person's belongings.

Even more extensive were the seizures in United States v. Santarelli, 778 F.2d 609 (11th Cir. 1985). In that case, agents searched the home of a suspected loanshark, confiscating the entire contents of a four-drawer file cabinet. In the end, they left with eight large boxes of items which they inventoried at the local FBI office. When the defendant objected to this process, the court strongly disagreed:

Given the fact that the search warrant entitled the agents to search for documents .... it is clear that the agents were entitled to examine each document in the bedroom or in the filing cabinet to determine whether it constituted evidence.... It follows that Santarelli would have no cause to object if the agents had entered his home to examine the documents and remained there as long as the search required. The district court estimated that a brief examination of each document would have taken several days. Under these circumstances, we believe that the agents acted reasonably when they removed the documents to another location for subsequent examination.... [T]o require an on-premises examination under such circumstances would significantly aggravate the intrusiveness of the search by prolonging the time the police would be required to remain in the home.

Id. at 615-6 (citation omitted).

d. Applying Existing Rules to Computers

Clearly, the Tamura court could not have anticipated that the explosion

in computers would result in the widespread commingling of documents. While computers are often set up with directories and subdirectories (much like a file cabinet is set up with file folders), many users put data on disks in random fashion. Thus, a particular letter or file could be anywhere on a hard disk or in a box of floppies.

[page 61]

Most important, all of the file-cabinet cases discussed above implicitly rely on the premise that "documents" are readily accessible and ascertainable items; that any agent can find them and (unless the subject is quite technical) can read, sort, and copy those covered by warrant. The biggest problem in the paper cases is time, the days it takes to do a painstaking job. But computer searches have added a formidable new barrier, because searching and seizing are no longer as simple as opening a file cabinet drawer. When agents seize data from computer storage devices, they will need technical skill just to get the file drawer open. While some agents will be "computer literate," only a few will be expert; and none can be expert on every sort of system. Courts have not yet addressed this reality. In the meantime, search warrant planning in every computer case should explore whether agents will ask for off-site search authority in the warrant application.

2. Seizing Computers because of Technical Concerns

a. Conducting a Controlled Search to Avoid Destroying Data

The computer expert who searches a target's computer system for information may need to know about specialized hardware, operating systems, or applications software just to get to the information. For example, an agent who has never used Lotus 1-2-3 (a spreadsheet program) will not be able to safely retrieve and print Lotus 1-2-3 files. If the agent entered the wrong computer command, he could unwittingly alter or destroy the data on the system. This sort of mistake not only alters evidence, but could create problems for the system's owner as well. Since it is the government's responsibility to recover evidence without altering data, the safest course is to rely on experts working in controlled environments.

Additionally, savvy computer criminals may know how to trip-wire their computers with "hot keys" or other self-destruct programs that could erase vital evidence if the system were examined by anyone other than an expert. For example, a criminal could write a very short program that would cause the computer to demand a password periodically and, if the correct password is not entered within ten seconds, it would destroy data automatically. In some cases,

[page 62]

valuable evidence has been lost because of the way the computers were handled. Therefore, this concern may make it doubly important to remove the computers, unless an expert determines that an on-site search will be adequate.

Quite obviously, some computers (such as large mainframes) are not easily moved. And some defendants will no doubt argue that if the government can search a mainframe computer on site, it can search PCs on site as well. Even so, the test should not be what is arguably possible, but rather what is the most reasonable, most reliable, and least intrusive way to search each system. The fact that mainframes may pose unique problems should not lead courts to adopt impractical rules for other searches.

In sum, there is ample authority to justify removing computer systems (or the relevant parts of them) to a field office or laboratory in order to search them for information. This is especially true where the warrant is broad, an on-site search will be intrusive, or technical concerns warrant moving the system to a lab. This will not always be the case, however, and agents and their experts should explore searching on site (or making exact copies to search later) whenever it is appropriate. Before agents ask for authority to seize any hardware for an off-site data search, they should analyze the reasons and set them out clearly for the magistrate.

b. Seizing Hardware and Documentation so the System Will Operate at the Lab

With an ever-increasing array of computer components on the market--and with existing hardware and software becoming obsolete--it may be impossible to seize parts of a computer system (e.g., the CPU and hard drive) and operate them at the laboratory. In fact, there may be times when agents will need to seize every component in the computer system and later have a laboratory computer specialist determine whether or not each piece can be returned. Many hardware incompatibilities exist (even within a given computer family such as IBM-compatible PCs), and the laboratory experts may need to properly re-configure the system back at the lab in order to read data from it.

[page 63]

Peripherals such as printers and special input and display devices may be necessary to operate and display certain software applications. Agents should attempt to learn as much about the system to be searched as possible so that appropriate seizure decisions can be made. If certain

peripherals must be seized to insure that the data can be retrieved from storage devices, this should be articulated in the warrant affidavit and covered in the warrant. Then an expert should examine the seized equipment as soon as practicable to determine whether the peripheral devices need to be retained. This approach relies completely on the facts of each case. It will seem reasonable and temperate when the I/O devices seized are essential, but not when the items seized are commercially available and the only justification for the seizure/retention is convenience and not necessity. If in doubt, agents should seek permission to seize the peripherals, and then insure a prompt review at the lab.

Similarly, when agents search and seize a computer system, they should ask for authority to seize any documentation that explains the hardware and software being seized. Documentation found at the scene may be a key in re~assembling the computer, operating it, or using the software on the machine properly. If the computer's user is experienced, he may have customized the software, and the documentation may be required to retrieve data. Although a computer lab may have or be able to obtain many standard varieties of documentation, some of it may not be easily available for purchase. As with hardware or software, the documentation should not be seized unless needed and, if seized, should be returned when no longer required.

I. EXPERT ASSISTANCE

1. Introduction

While planning is important to the success of any search, it is critical in searching and seizing information from computers. Agents should determine, to the extent possible, the type of computer involved, what operating system it uses, and whether the information sought can be accessed by, or is controlled by, a computer literate target.

[page 64]

Answering these questions is key, because no expert can be expert on all systems. Mainframes, for example, are made by various companies (e.g., IBM, DEC, Cray) and often run unique, proprietary operating systems. Even the PC market offers significantly different hardware/software configurations. Although the most common desk-top computer is an IBM or IBM-compatible system, it runs a range of operating systems including DOS (with or without Windows), OS/2, and UNIX. Apple Computers are also popular and run their own unique operating system.

Computer literate targets may attempt to frustrate the proper execution of a search warrant. For example, an ingenious owner might have installed

hidden commands that could delete important data if certain start-up procedures are not followed. If this might be the case, experts will take special precautions before the search: they will, for example, start (or "boot") the computer from a "clean" system diskette in a floppy drive, not from the operating software installed on the system. These hidden traps, as well as passwords and other security devices, are all obstacles that might be encountered in a search.

In sum, since computer experts cannot possibly be expert on all systems, it is important lo have the correct expert on the scene. Knowing the type of computer to be searched, and the type of operating system being used, will allow the appropriate expert to be selected. This, in turn, will streamline the search process, since the expert may be familiar with the software and file structures on the target machine.

2. Finding Experts

Most situations will require an expert to retrieve, analyze, and preserve data from the computers to be searched. Oftentimes the job may not be so complex: the records may be stored with a standard brand of software using the DOS (Disk Operating System) format. Some of the most common software programs are WordPerfect (for text), Lotus (for spreadsheets), and dBase (for databases). If it is more complicated than this, however, only an expert in the hardware and software at hand should do the work.

[page 65]

To determine what type of expert will be needed, agents should get as much information about the targeted system as possible. Sources like undercover agents, informants, former employees, or mail covers can provide information about the system at the search site. Once the computer systems and software involved have been identified, an appropriate expert can be found from either the federal or private sector. Ultimately, the expert must use sound scientific techniques to examine any computer evidence.

a. Federal Sources

The best place to find an expert may be in the investigating agency itself. Many federal agencies have experienced people on staff who can help quickly when the need arises, and the list at APPENDIX C provides contact points for various agencies. If the investigating agency lacks an expert in the particular system to be searched, other federal agencies may be able to assist. The trick, of course, is to find the expert while planning for the search and not to start looking after the agents execute

the warrant. Prosecutors must allow time to explore the federal network and find the right person.

Most of the federal agencies that routinely execute search warrants for computer evidence have analysts at central laboratories or field experts who can search the seized computer evidence. Many of them will also work on evidence from other federal or state agencies as time permits. It is important to call early to get specific instructions for handling the evidence, and these experts can provide other technical assistance as well. For example, there are many kinds of software (both government and private) which will help process evidence, break passwords, decrypt files, recover hidden or deleted data, or assist investigators in other important ways. Because these utilities are constantly changing, it is important to consult with experts who have them and know how to use them.

Each agency organizes its computer experts differently. For example, the Computer Analysis and Response Team (CART) is a specialized team within the central FBI Laboratory in Washington, D.C., that examines various types of computer evidence for FBI agents nationwide. The IRS, on the other hand, has about seventy decentralized experts, called Seized Computer Evidence Recovery (SCER) Specialists who work in controlled environments

[page 66]

across the country. Almost every IRS District has at least one SCER Specialist, and many have two. The Drug Enforcement Administration's forensic computer experts are also experienced in all phases of computer operations related to criminal cases, including data retrieval from damaged media and decryption. The U.S. Secret Service has approximately twelve special agents who are members of the Electronic Crimes Special Agent Program (ECSAP). These agents are assigned to field offices on a regional basis and are trained in the area of computer investigations and computer forensics. (For a list of federal sources for computer experts, see APPENDIX C, p. 143.)

b. Private Experts

Whatever the source of a private expert, the affidavit should ask permission to use non-law-enforcement personnel during the execution of the search warrant. The issuing magistrate should know why an expert is needed and what his role will be during the search. Agents must carefully monitor the expert to insure that he does not exceed the limits described in the search warrant. Certain experts--those not familiar with the judicial system--are not likely to be expert on how to execute a search warrant, protect chain-of~-custody, or resolve search issues that may

affect the evidence's admissibility at trial. Thus, a private expert should be paired with an experienced agent every step of the way. In addition, the expert's employment contract should address confidentiality issues, and include a non-disclosure clause and a statement of Privacy Act restrictions. If the contracting agency is the IRS, pay special note to Internal Revenue Code provisions at 26 U.S.C. 6103, which address rules for confidentiality and nondisclosure of tax return information.

(1) Professional Computer Organizations

Many professional computer organizations have members who are experts in a wide variety of hardware and software. Computer experts from the government are a good source for finding a private expert, for the organizations and contacts between them change almost as fast as the technology. Also, one advantage of using a professional organization as the source of an expert is that

these organizations usually have members who work routinely with federal or state law enforcement and are therefore familiar with handling evidence and testifying.

(2) Universities

Another source for experts is a university, especially for high-tech crimes involving rare kinds of hardware or software. The academic environment attracts problem-solvers who may have skills and research contacts unavailable in law enforcement.

(3) Computer and Telecommunications Industry Personnel

In some cases, the very best expert may come from a vendor or service provider, particularly when the case involves mainframes, networks, or unusual systems. Many companies such as IBM and Data General employ some experts solely to assist various law enforcement agencies on search warrants.

(4) The Victim

Finally, in some circumstances, an expert from the victim organization may be the best choice, especially if the hardware configuration or software applications are unique to that organization. Agents and prosecutors must, of course, be sensitive to potential claims of bias. Many relevant issues, such as estimates of loss, may pose a considerable gray area. Even if the victim-expert is completely dispassionate and

neutral in her evaluation, her affiliation with and loyalty to the victim organization may create a bias issue later at trial.

[page 68]

3. What the Experts Can Do

a. Search Planning and Execution

Agents and prosecutors who anticipate searching and seizing computers should include a computer expert in the planning team as early as possible. Experts can help immeasurably in anticipating the technical aspects of the search. This not only makes the search smoother, it is important information for designing the scope of the warrant. In particular, if agents can give the expert any information about the target's specific computer system, the expert may be better able to predict which items can be searched at the scene, which must be seized for later analysis, and which may be left behind.

Further, if the computer system is unusual or complex, technical experts can be invaluable help at the scene during the search. Particularly when evidence resides on computer networks, backup tapes, or in custom-tailored systems, the evidence will be safest in the hands of an expert.

b. Electronic Analysis

The experts will examine all the seized computer items (so long as they are properly preserved and sealed) and will recover whatever evidence they can. Most forensic computer examiners will perform at least the following: (1) make the equipment operate properly; (2) retrieve information; (3) unblock "deleted" or "erased" data storage devices; (4) bypass or defeat passwords; (5) decipher encrypted data; and (6) detect the presence of known viruses.

The data to be searched can consist of hundreds or even thousands of files and directories. In some cases, there will be evidence in most of the files seized, and in others, only a small fraction of them. Once the analyst has protected the original data from change, she must begin to search for the relevant material.

[page 69]

A good first step is to print out a directory of the information

contained on a hard drive or floppy disk. Directories give valuable information about what is in the files, when they were created, and how long they are. Of course, analysts will not entirely trust file names, as hackers have been known to hide highly incriminating material in files with innocuous names and misleading dates.

Once the analyst has printed a directory, he will probably log onto the hard or floppy drive and look at each file, noting on the printed directory (or a separate log sheet if available) the type of information in each file and whether it appears relevant. Relevant files can be copied onto a separate disk or printed out in hard copy. It is a good idea always to review files from bit-stream copies (which record each separate bit of information, including hidden files) or in "read only" mode so that the reviewer can read the document but cannot edit it. This way, the agents can later testify that the seized material could not have been mistakenly altered during the review. Of course, there is more than one "right way" to analyze electronic evidence, and experts must deal with the circumstances of each case. Ultimately the analyst must adhere to sound scientific protocols in recovering and examining computer-related evidence, and keep clear and complete records of the process.

c. Trial Preparation

Computer forensic experts can help prosecute the case with advice about how to present computer-related evidence in court. Many are experienced expert witnesses and they can (1) help prepare the direct case; and (2) anticipate and rebut defense claims. In addition, computer experts can assist prosecutors in complying with the new federal rules pertaining to expert witnesses, Fed. R. Evid. 16(a)(1)(E) and 16(b)(1)(C), effective December 1, 1993. Under these rules, the government must provide, upon request, a written summary of expert testimony which it intends to use during its case in chief. There is a reciprocal requirement for the summary of defense expert witness testimony, as long as the defense has requested a summary from the government, and the government has complied.

d. Training for Field Agents

Before a computer case ever arises, experts can train agents and prosecutors about computer search problems and opportunities. They can teach investigators how to preserve and submit computer evidence for examination, and many will also provide field support as time permits.

[page 71]

V. NETWORKS AND BULLETIN BOARDS

A. INTRODUCTION

Electronic Bulletin Board Services (BBSs) are computers set up to serve in the electronic world as places where users can post and read messages--much like traditional bulletin boards. In addition, however, a BBS may also permit users to communicate via private electronic mail, to engage in "chat sessions" (real-time conversations where the "speakers" talk by using their keyboards instead of their voices), to upload and download files, and to share information on topics of common interest (e.g., a newsletter on stamp collecting). A sysop runs the bulletin board, and BBS users access it with their computers over regular telephone lines.

Some bulletin boards, known as "pirate bulletin boards," are maintained for illegal purposes such as distributing copyrighted software, credit card numbers, telephone access codes, and pornography. A BBS dedicated to phone fraud is also called a "phone phreaker board," and those which distribute child pornography and adult obscenity are called, not surprisingly, "porn boards." The illegal material on these boards is not protected by the First Amendment since such items are "fruits of crime" and "contraband" and do not convey any thought, opinion, or artistic expression. Nor can these operations claim some sort of "press protection" for publishing these items, since the Constitution does not shield the press against laws of general applicability. In short, the First Amendment is not a license to commit crimes. See Securities and Exchange Commission v. McGoff, 647 F.2d 185 (D.C. Cir.), cert. denied, 452 U.S. 963 (1981); Cf. Pell v. Procunier, 417 U.S. 817, 833-5 (1974)(the right to speak and publish does not carry an unrestrained right to gather information; a prison may restrict the press's access to its inmates in accord with the state's legitimate incarceration policy objectives).

It gets more complex, however, because many bulletin boards are not devoted solely to illegal activities, but are hybrid boards: they contain both illegal and legal material. To complicate matters further, the legitimate material on the board (or stored on the same computer which runs the board) may be statutorily protected. For example, some private electronic mail may be covered under 18 U.S.C. 2701, et seq., Stored Wire

[page 72]

and Electronic Communications. (For further discussion, see "STORED ELECTRONIC COMMUNICATIONS," infra p. 85). Even more difficult, some material may be specifically protected from search and seizure by a complex statute called the Privacy Protection Act, 42 U.S.C. 2000aa. In order to understand the scope and intricacy of this statute and how it might apply to computer searches, it helps to begin with the case which prompted it.

B. THE PRIVACY PROTECTION ACT, 42 U.S.C. 2000aa

1. A Brief History of the Privacy Protection Act

On April 9, 1971, nine police officers in California responded to Stanford University Hospital to disperse a large group of demonstrators. The demonstrators resisted, and they ultimately attacked and injured all nine officers. Two days later, on April 11, The Stanford Daily, a student newspaper, carried articles and photographs devoted to the student protest and the clash between these protestors and the police. Believing that The Stanford Daily might possess additional photographs that would identify other protestors, the police sought and obtained a search warrant to search the newspaper's offices.

A month after the search, The Stanford Daily brought a civil action alleging violations of the First, Fourth and Fourteenth Amendments. In support of their claims, the plaintiffs alleged that (1) the Fourth Amendment forbade the issuance of search warrants for evidence in the possession of those not suspected of criminal activity and (2) the First Amendment prohibited the use of search warrants against members of the press and, instead, required the use of subpoenas duces tecum. Zurcher v. Stanford Daily, 436 U.S. 547 (1978). The Supreme Court disagreed with both claims, holding that the use of a search warrant, even for the pursuit of "mere evidence," was permitted on both non~suspect third parties and members of the news media.

[page 73]

In response to Zurcher, Congress passed the Privacy Protection Act of 1980, 42 U.S.C. 2000aa (hereinafter the PPA). The purpose of this legislation, as stated in the Senate Report, is to afford "the press and certain other persons not suspected of committing a crime with protections not provided currently by the Fourth Amendment." S. Rep. No. 874, 96th Cong., 2d Sess. 4 (1980). As the legislative history indicates,

the purpose of this statute is to limit searches for materials held by persons involved in First Amendment activities who are themselves not

suspected of participation in the criminal activity for which the materials are sought, and not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation.7 Id. at 11.

The PPA protects two classes of materials--defined as "work product materials" and "documentary materials"--by restricting beyond the existing limits of the Fourth Amendment when government agents can get warrants to search for or seize them.

It is important to note that, although victims of a search which violates the PPA may not move to suppress the results, the statute does create civil remedies. Moreover, the PPA specifically precludes the government from asserting a good faith defense to civil claims, so in this respect 2000aa is a strict liability statute.

2. Work Product Materials

In general terms, the first category of protected material covers original work in the possession of anyone (including authors and publishers) who intends (from an objective view) to publish it. In construing this statute, the exact language of the definitions is important. Specifically, "work product materials" are defined in 42 U.S.C. 2000aa-7(b) as

7 The Department had previously promulgated regulations on issuing subpoenas directly to members of the news media or indirectly for their telephone toll records. The regulations also addressed interrogating, indicting, or arresting members of the press. See 28 C.F.R. 50.10.

materials, other than contraband or the fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or which is or has been used, as the means of committing a criminal offense, and--

(1) in anticipation of communicating such materials to the public, are prepared, produced, authored, or created, whether by the person in possession of the materials or by any other person;

(2) are possessed for the purposes of communicating such materials to the public; and

(3) include mental impressions, conclusions, opinions, or theories of the

person who prepared, produced, authored, or created such material.

When "work product materials" are involved, Title 42, Section 2000aa(a) provides that:

Notwithstanding any other law, it shall be unlawful for a government officer or employee, in connection with the investigation or prosecution of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce. . (emphasis added). . .[unless]

(1) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate: Provided, however, That a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or withholding of such materials or the information contained therein (but such a search or seizure may be conducted under the provisions of this paragraph if the offense consists of the receipt, possession, or communication of information relating to the national defense, classified information, or restricted data under the provisions of section 793, 794, 797, or

[page 75]

798 of Title 18, or section 2274, 2275 or 2277 of this title, or section 783 of Title 50); or

(2) there is reason to believe that the immediate seizure of such materials is necessary to prevent the death of, or serious bodily injury to, a human being.

Thus, under 2000aa(a), there are three situations in which government agents may search for or seize these materials without running afoul of the statute. First, the definition itself specifically excludes contraband or the fruits or instrumentalities of a crime. 42 U.S.C. 2000aa-7(b). As the drafting Committee noted,

[T]hese kinds of evidence are so intimately related to the commission of a crime, and so often essential to securing a conviction, that they should be available for law enforcement purposes, and, therefore, must fall outside the no search rule that is applied to work product.

S. Rep. 96-874, 96th Cong., 2d Sess. 17, reprinted in 1980 U.S. Code

Cong. & Admin. News 3964. In BBS cases, the most common objects of the warrant--stolen access codes, child pornography, and illegally copied software--would clearly fall within the contraband exclusion, so the PPA would not affect a warrant drawn for these materials.

In addition, as quoted above, the PPA creates two exceptions to the general prohibition against seizing "work product." One excepts situations in which life and limb are at stake. The other applies when (1) the work product is evidence of crime, and (2) the person who possesses the materials probably committed it. Even so, this evidence-of-crime exception does not apply if the particular crime "consists of the receipt, possession, communication or withholding of such material...." unless the work product was classified or restricted, and the offense is specifically listed in the PPA. 42 U.S.C. 2000aa(a)(1) and (b)(1). This general evidence-of-crime exception was intended to

codify a core principle of this section, which is to protect from search only those persons involved in First Amendment activities who are themselves not implicated in the crime under investigation, and not to shield those who participate in crime.

[page 76]

H.R. Rep. No. 1064, 96th Cong., 2d Sess. 7. To trigger the exception, however, law enforcement officials are held to a higher-than-usual requirement: they must show probable cause to believe the person who holds the evidentiary materials is a suspect of the crime--the same showing of cause required for an arrest warrant. S. Rep. No. 874, 96th Cong., 2d Sess. 11, reprinted in 1980 U.S. Code Cong. & Admin. News 3950, 3957.

It may, of course, be difficult to invoke this evidence-of-crime exception, particularly at early stages of the investigation. As the Supreme Court noted in Zurcher (and a number of commentators have reiterated since), a search warrant is often most useful early in an investigation when agents have probable cause to believe there is evidence on the premises, but are not ready to arrest any particular person. See Zurcher v. Stanford Daily, 436 U.S. at 561; Testimony of Richard J. Williams, Vice President, National District Attorney's Association, in Hearing before the Committee on the Judiciary, United States Senate, 96th Cong., 2d Sess. on S. 115, S. 1790, and S. 1816 (Mar. 28, 1980) Serial No. 96-59, at 152-3.

The receiving-stolen-property exemption--which prevents agents from using the evidence-of-crime exception when the crime is receipt, possession,

communication, or withholding of the same work product materials--was included to prevent law enforcement officials from classifying work product as "stolen goods" to justify seizing it. The Committee report gave as its primary example the case of a reporter who receives an under-the-table copy of a corporate memo discussing a defective product. Knowing the report to be stolen, the reporter might be guilty of receiving or possessing stolen property and thus unprotected by the PPA.

The Committee believed that it would unduly broaden the suspect exception to use the reporter's crime of simple "possession" or "receipt" of the materials (or the similar secondary crimes of "withholding" or "communicating" the materials) as a vehicle for invoking the exception when the reporter himself had not participated in the commission of the crimes through which the materials were obtained

H. Rep. No. 1064, 96th Cong., 2d Sess. 7 (emphasis added). In light of Congress's stated concern, perhaps this counter-exception does not apply when anything more than simple possession is involved: that is, possession is combined with the mens rea necessary to constitute some other offense (e.g.,

[page 77]

possession with intent to defraud). See 18 U.S.C. 1029(a)(3) (making it a crime to "knowingly and with intent to defraud" possess fifteen or more devices which are counterfeit or unauthorized access devices); 18 U.S.C. 1030(a)(6) (making it a crime to "knowingly and with intent to defraud" traffic in any password or similar information through which a computer may be accessed without authorization).

3. Documentary Materials

In addition to protecting work product, the PPA covers a second, larger class of items called "documentary materials." The statute defines this term in extraordinarily broad fashion--a definition which covers almost all forms of recorded information which are "... possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication...." 42 U.S.C. 2000aa(b) (emphasis added). Specifically, "documentary materials" encompass

materials upon which information is recorded, and includes, but is not limited to, written or printed materials, photographs, motion picture films, negatives, video tapes, audio tapes, and other mechanically, magnetically or electronically recorded cards, tapes, or discs, but does not include contraband or the fruits of a crime or things otherwise

criminally possessed, or property designed or intended for use, or which is or has been used as, the means of committing a criminal offense.

42 U.S.C. 2000aa-7(a).

As with "work product materials," the statute excludes from the definition of "documentary materials" any items which are contraband or the fruits or instrumentalities of a crime. 42 U.S.C. 2000aa-7(a). Further, the two exceptions to the work-product search prohibition, discussed above, also apply to searches for documentary materials: they may be searched and seized under warrant in order to (1) prevent death or serious injury; or (2) to search for evidence of crime held by a suspect of that crime. (This last exception includes all its attendant internal exemptions, examined above, relating to crimes of possession or receipt.)

[page 78

Additionally, the PPA allows agents to get a warrant for documentary materials under two more circumstances found at 42 U.S.C. 2000aa(b):

(3) there is reason to believe that the giving of notice pursuant to a subpena duces tecum would result in the destruction, alteration, or concealment of such materials; or

(4) such materials have not been produced in response to a court order directing compliance with a subpena duces tecum, and--

(A) all appellate remedies have been exhausted; or

(B) there is reason to believe that the delay in an investigation or trial occasioned by further proceedings relating to the subpena would threaten the interests of justice.

In drawing these additional exceptions, Congress anticipated some of the factors a court might consider in determining whether relevant documentary materials could be lost to the government. These factors include whether there is (1) a close relationship (personal, family, or business) between the suspect and the person who holds the material, or (2) evidence that someone may hide, move, or destroy it. S. Rep. 96-874, 96th Cong., 2d Sess. 13, reprinted in U.S. Code Cong. & Admin. News 3950, 3959-60.

4. Computer Searches and the Privacy Protection Act

The Privacy Protection Act only applies to situations where law enforcement officers are searching or seizing (1) work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication; or (2) documentary materials possessed by a person in connection with a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication. 42 U.S.C.

[page 79]

2000aa(a) and (b). Before the computer revolution, the statute's most obvious application was to traditional publishers, such as newspaper or book publishers. The legislative history makes clear, however, that the PPA was not intended to apply solely to the traditional news media but was meant to have a more sweeping application. As then-Assistant Attorney General for the Criminal Division Phillip B. Heymann testified:

While we considered the option of a press-only bill, this format was rejected partially because of the extreme difficulties of arriving at a workable definition of the press, but more importantly because the First Amendment pursuits of others who are not members of the press establishment are equally as important and equally as susceptible to the chilling effect of governmental searches as are those of members of the news media.

H. Rep. No. 1064, 96th Cong., 2d Sess., Transcript of Statement on File, at 4.

With the widespread proliferation of personal computers, desktop publishing, and BBS services, virtually anyone with a personal computer and modem can disseminate to other members of the public (especially those who have appropriate hardware and software) a "newspaper ... or other similar form of public communication." Thus, the scope of the PPA may have been greatly expanded as a practical consequence of the revolution in information technology--a result which was probably not envisioned by the Act's drafters.

Before searching any BBS, therefore, agents must carefully consider the restrictions of the PPA, along with its exceptions. Additionally, they should include any information bearing on the applicability of this statute (and its many exceptions and sub-exceptions) in the warrant affidavit. That said, it is also important to recognize that not every sysop who possesses information necessarily has an intent to disseminate it to the public. Nor is every BBS engaged in a "similar form of public communication."

a. The Reasonable Belief Standard

When addressing work product materials, the statute, by its terms, only applies when the materials are possessed by a person "reasonably believed

[page 80]

to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. 2000aa(a). In non~computer contexts, the courts have concluded that it is not enough just to possess materials a professional reporter might possess. In addition, there must be some indication the person intended to disseminate them. In Lambert v. Polk County, Iowa, 723 F. Supp. 128 (S.D. Iowa 1989), for example, the plaintiff Lambert captured a fatal beating on videotape. Police investigating the incident seized the tape from Lambert and, shortly thereafter, Lambert contracted to sell the tape to a local television station. After the police refused to relinquish the tape, the television station and Lambert sued for injunctive relief claiming, among other things, a violation of 42 U.S.C. 2000aa. While the district court granted relief on other grounds, it held that neither the television station nor Lambert was likely to prevail on a 42 U.S.C. 2000aa claim. The television station was not the aggrieved party, and "there was nothing about the way Lambert presented himself [to the officers] that would have led them to reasonably believe that Lambert's purpose was to make a dissemination of the videotape to the public." Lambert, 723 F. Supp. at 132. But cf. Minneapolis Star & Tribune Co. v. United States, 713 F. Supp. 1308 (D. Minn. 1989)(plaintiffs from whom videotapes were seized at robbery scene were successful in PPA claim because agents apparently had independent knowledge that plaintiffs represented the established media).

The reasonable belief standard was also important in the district court opinion in Steve Jackson Games v. United States, 816 F. Supp. 432 (W.D. Tex. 1993), appeal filed on other grounds, (Sept. 17, 1993). To understand the scope of this opinion, it is important to put it in the context of its facts. In early 1990, the United States Secret Service began investigating potential federal computer crimes under 18 U.S.C. 1030. The Secret Service learned that a Bell South computer system had been invaded, and that the computer hackers were attempting to decrypt passwords which would allow them into computer systems belonging to the Department of Defense.

During the course of this investigation, the Secret Service received information implicating an individual who was employed by Steve Jackson Games, a Texas company that published books, magazines, box games, and

related products. Steve Jackson Games used computers for a variety of business purposes, including operating an electronic bulletin board system ("BBS"). The Secret Service was informed that the suspect was one of the sysops of the Steve Jackson Games BBS, and that he could delete any documents or information in the Steve Jackson Games computers and bulletin

[page 81]

board. Even so, none of the other sysops nor the company itself was ever a suspect in the investigation.

On February 28, 1990, the Secret Service obtained a federal warrant to search the offices of Steve Jackson Games and to seize various computer materials. The warrant covered:

Computer hardware * * * and computer software * * * and written material and documents relating to the use of the computer system, documentation relating to the attacking of computers and advertising the results of computer attacks * * *, and financial documents and licensing information relative to the computer programs and equipment at [the company's offices] which constitute evidence, instrumentalities and fruits of federal crimes, including interstate transportation of stolen property (18 U.S.C. 2314) and interstate transportation of computer access information (18 U.S.C. 1030(a)(6)). This warrant is for the seizure of the above described computer and computer data and for the authorization to read information stored and contained in the above described computer and computer data.

The Secret Service executed the warrant on March 1, 1990. The agents seized two of thirteen functioning computers, and one other computer that was disassembled for repair. The Secret Service also seized a large number of floppy disks, a printer, other computer components, and computer software documentation. Steve Jackson Games immediately requested the return of the seized materials, but the agency retained most of the materials for several months before returning them. No criminal charges were brought as a result of this investigation.

In May 1991, plaintiffs (Steve Jackson Games; the company's owner and sole shareholder, Steve Jackson; and several individual users of the company's BBS) filed suit against the Secret Service and the United States, alleging violations of the Privacy Protection Act. They also claimed violations of the Stored Electronic Communications Statute, discussed in greater detail at "STORED ELECTRONIC COMMUNICATIONS," infra p. 85.

Following a bench trial, the court determined that the defendants had violated the Privacy Protection Act. The court held that the materials seized by the Secret Service (in particular, the draft of a book about to be published)

[page 82]

included "work product materials" and "documentary materials" protected by the Privacy Protection Act. The court decided that seizing these materials did not immediately violate the statute, however, because at the time of the seizure, the agents did not (in the language of the statute) "reasonably believe[]" that Steve Jackson Games "ha[d] a purpose to disseminate to the public a news~paper, book, broadcast, or other similar form of public communication * * * ." This was true even though "only a few hours of investigation" would have revealed it. Id. at 440 n.8. However, the court held that a violation did occur on the day after the search when at least one agent learned the materials were protected by the statute and failed to return them promptly.

b. Similar Form of Public Communication

As noted above, the PPA applies only when the materials are possessed by a person reasonably believed to have a purpose to disseminate to the public "a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. 2000aa (emphasis added). Not every BBS will satisfy this standard. For example, a BBS that supplies unauthorized access codes to a small group of phone phreakers is not disseminating information to the public, nor is it engaging in a form of public communication similar to a newspaper. (Of course, the contraband exception will probably also apply in such a case).

The exact scope of the PPA remains uncertain, and the recent opinion in Steve Jackson Games does not clarify the issue. There the court found a cognizable PPA violation arising from the Secret Service's search and prolonged seizure of the successive drafts of a book Steve Jackson was soon to publish. But, just as important, the court did not hold that seizing the Steve Jackson BBS likewise violated the statute. Instead, the court held that "[i]n any event, it is the seizure of the 'work product materials' that leads to the liability of the United States Secret Service and the United States in this case." 816 F. Supp at 441. Indeed, one of the attorneys who represented Steve Jackson Games reached a similar conclusion:

Though the results in the SJG case were very good on balance, a couple of major BBS issues were left for better resolution on another day.... [One issue] is the finding that SJG was a

[page 83]

'publisher' for purposes of the PPA. This holding ... leaves the applicability of the PPA largely undetermined for other BBS'. Steve Jackson Games was a print publisher, and its computers were used to support the print publishing operation. What about BBS' that publish their information in electronic form only? What about BBS' that do not publish anything themselves in the traditional sense, but host public conferences? The SJG case simply does not give guidance on when a non-printing BBS qualifies as a publisher or journalistic operation for purposes of PPA protection. Rose, Steve Jackson Games Decision Stops the Insanity, Boardwatch, May 1993, at 53, 57.

c. Unique Problems: Unknown Targets and Commingled Materials

Applying the PPA to computer BBS searches is especially difficult for two reasons. First, early in an investigation, it is often impossible to tell whether the BBS sysop is involved in the crime under investigation. But unless agents have probable cause to arrest the sysop at the time of the search, the evidence-held-by-a-target exception in 42 U.S.C. 2000aa would not apply.

Second, because most computers store thousands of pages of information, targets can easily mix contraband with protected work product or documentary materials. For example, a BBS trafficking in illegally copied software (which, along with the computers used to make the copies, is subject to forfeiture) may also be publishing a newsletter on stamp collecting. If agents seized the computer (or even all the data), the seizure would necessarily include both the pirated software and the newsletter. Assuming the stamp-collectors' newsletter was completely unrelated to the criminal copyright violations and also that it qualified as a "similar form of public communication," the seizure might violate the plain wording of the PPA.

There are, as yet, no cases addressing the status of PPA-protected materials which are commingled with contraband or evidence of crime. However, in construing the Fourth Amendment, the courts have recognized that there is sometimes no practical alternative to seizing non-evidentiary items and sorting them out later. See National City Trading Corp. v. United States, 635

[page 84]

F.2d 1020 (2d Cir. 1980)(space used by a law office and by a targeted business operation was so commingled that the entire suite, really being

one set of offices, was properly subject to search); United States v. Hillyard, 677 F.2d 1336, 1340 (9th Cir. 1982)("Cases may arise in which stolen goods are intermingled with and practically indistinguishable from legitimate goods. If commingling prevents on site inspection, and no practical alternative exists, the entire property may be seizable, at least temporarily."); United States v. Tropp, 725 F. Supp. 482, 487-88 (D. Wyo. 1989)("Some evidence not pertinent to the warrant was seized ... only because it had been commingled or misfiled with relevant documents. That evidence was returned.... In sum, the search warrant comported with the mandate of the Fourth Amendment and the search conducted pursuant thereto was not unreasonable."). (For a more extensive discussion of commingled materials and off-site searches, see "DECIDING WHETHER TO CONDUCT THE SEARCH ON-SITE OR TO REMOVE HARDWARE TO ANOTHER LOCATION," supra p. 55.) Of course, these commingling cases involve the Fourth Amendment, not 42 U.S.C. 2000aa, and it remains to be seen whether these holdings will apply to the Privacy Protection Act

5. Approval of Deputy Assistant Attorney General Required

On September 15, 1993, Deputy Attorney General Philip B. Heymann issued a memorandum which requires that all applications for a warrant issued under 42 U.S.C. 2000aa(a) must be authorized by the Assistant Attorney General for the Criminal Division (AAG), upon the recommendation of the U.S. Attorney or (for direct Department of Justice cases) the supervising Department of Justice attorney.

On December 9, 1993, Jo Ann Harris, the Assistant Attorney General (AAG) for the Criminal Division, delegated this authority by memorandum to the Deputy Assistant Attorneys General of the Criminal Division. There are emergency procedures for expediting the approval in cases which require it. All requests for authorization--emergency or routine--should be directed to the Chief, Legal Support Unit of the Office of Enforcement Operations in the Criminal Division (202-514-0856).

If agents or prosecutors are planning a search and seizure of electronic evidence in a case in which the PPA may apply, we urge them to contact the

Computer Crime Unit (202-514-1026) immediately to discuss the investigation and any new legal developments in this area.

C. STORED ELECTRONIC COMMUNICATIONS

There are special statutory rules protecting some electronic

communications in electronic storage. Anyone who provides an electronic communication service or remote computing services to the public, is prohibited by 18 U.S.C. 2702 from voluntarily disclosing the contents of the electronic communications it stores or maintains on the service. A "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system. 18 U.S.C. 2711(2).

It is not entirely clear what sorts of electronic communications services will be found to provide "public" service. Generally speaking, "public" means available to all who seek the service, even if there is some requirement, such as a fee. It is probably safe to assume that any service permitting "guest" or "visitor" access is "public." On the other hand, the term should not be read to cover business networks open only to employees for company business. If that business network is connected to the Internet (an extensive world-wide network), it may be part of a "public" system, but this does not necessarily mean that the corporate LAN (local-area network) becomes a "public" service.

There are several important exceptions to 2702's non-disclosure rule, including (1) a provision under 18 U.S.C. 2702(b)(3) allowing a person or entity to disclose the contents of a communication with the lawful consent of the originator, an addressee, or the intended recipient of such communication (or the subscriber in the case of a remote computing service), and (2) a provision under 18 U.S.C. 2702(b)(6) allowing disclosure to a law enforcement agency if the contents were inadvertently obtained and appear to pertain to the commission of a crime.

For the government to obtain access to a "stored electronic communication," it must follow the dictates of 18 U.S.C. 2703, which sets out different rules depending upon how long the particular communication has been in electronic storage. That section provides that "a governmental entity

[pshr 86]

may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage ... for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent state warrant." 18 U.S.C. 2703(a) (emphasis added). If the information has been stored for more than 180 days, prosecutors may use either a Rule 41 search warrant (without notice to the customer or subscriber) or an administrative subpoena, grand jury subpoena, trial subpoena, or a court order pursuant to 18 U.S.C. 2703(d) (with notice to the customer or subscriber).

The two terms underlined above merit further discussion. First of all, it is important to note that not all electronically stored communications are covered by this section. The electronic communication must be transmitted on a system that affects interstate or foreign commerce, 18 U.S.C. 2510(12), and must be in electronic storage. "Electronic storage" means any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof or any backup of this communication. 18 U.S.C. 2510(17).

To understand the importance of this definition, it is critical to know how electronic mail works. Generally speaking, e-mail messages are not transmitted directly from the sender's machine to the recipient's machine; rather, the e-mail message goes from the sending machine to an e-mail server where it is stored (i.e., kept in "electronic storage"). A message is then sent from the server to the addressee indicating that a message for the addressee has been stored. The actual message remains on the server, however, until the addressee retrieves it by having a copy sent to his machine. Often, both the sender and receiver can delete the e-mail from the server.

Section 2703 protects the electronic communication while it is stored in the server in this intermediate state.8 Once a message is opened, however, its storage is no longer "temporary" nor "incidental to. . .transmission," and it thus takes on the legal character of all other stored data. Therefore, the statute

[page 87]

8 When a sysop backs up the mail server to protect against system failure, all e-mails stored on the server will be copied. Thus, if the e-mail is later deleted from the server, the backup copy remains. The statute protects this copy as well. 18 U.S.C. 2510(17)(B).

does not apply to all stored communications, such as word processing files residing on a hard drive, even when these files were once transmitted via e~-mail.

The other highlighted term--"require the disclosure"--seems to suggest that 2703 only applies when the government seeks to compel the service provider to produce the electronic mail, not when government agents actually seize it. With this in mind, the statute's cross-reference to Rule 41 is confusing, because Rule 41 authorizes the government to "seize" items, not to "require [their] disclosure." To speak in terms of requiring the disclosure of electronic mail, rather than of seizing it, seems to connote a process of serving subpoenas, not of executing

warrants.

On the other hand, Congress may have simply assumed that most system providers would be disinterested in the "search," and that, as a practical matter, the service provider would actually retrieve and turn over to the government those files of suspect-users listed in the warrant. In mentioning Rule 41, Congress may not have been focusing on who would actually do the retrieval, but rather on what level of proof would be required before electronic communications in electronic storage could be procured for a criminal investigation. Therefore, the statute's references to warrants and Rule 41 seem designed to insure that, no matter who actually searches the system, the government will be held to a probable-cause standard--even if the system provider would have been just as willing to honor a subpoena. See H.R. Rep. No. 647, 99th Cong., 2d Sess., at 68 ("The Committee required the government to obtain a search warrant because it concluded that the contents of a message in storage were protected by the Fourth Amendment.... To the extent that the record is kept beyond [180 days] it is closer to a regular business record maintained by a third party and, therefore, deserving of a different standard of protection.").

Indeed, it is entirely reasonable to read this statute as Congress's effort to regulate primarily the duties of service providers to protect the privacy of their subscribers in regard to all third parties, including law enforcement. The statute may not have fully contemplated those cases in which the system provider (rather than the subscriber) is, or may be, implicated in the criminal investigation.

There is, unfortunately, no case law clearly addressing this issue. In a recent civil suit, the government was held liable for seizing electronic mail on

an electronic bulletin board service (BBS), even though the agents had a valid warrant.9 Steve Jackson Games. Inc. v. U.S. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), appeal filed on other grounds, (Sept. 17, 1993). In that case, plaintiffs sued following a search by the Secret Service of computers and other electronic storage devices which belonged to the company. (For a more complete description of the facts of the case, see the discussion at p. 80.) One of the computers seized by the Secret Service was the computer used by Steve Jackson Games to operate its BBS. The hard disk of the BBS computer contained a number of private e-mail messages, some of which had not yet been accessed by their addressees. The district court found that the Secret Service read e-mail messages on the computer and subsequently deleted certain information and

communications, either intentionally or accidentally, before returning the computer to Steve Jackson Games. Id. at 441. Here, the court held that the Secret Service "exceeded the Government's authority under the statute" by seizing and examining the contents of "all of the electronic communications stored in the [company's] bulletin board" without complying with the statute's requirements for government access. The court's opinion never addressed, however, the interplay between 2703 and Rule 41, so it sheds no light on the proper interpretation of 2703(a). In fact, the court never cited 2703(a) at all. Instead, the court discussed the requirements of 2703(d), a provision that allows the government to get a court order, upon a showing that the communication sought is relevant to a legitimate law enforcement inquiry, when the communication has been in storage more than 180 days or is held by a remote computing service. (The court did not find how long the searched communications were in storage, but did hold that Steve Jackson was a remote computing service.) Even under this lesser standard-- 2703(a) requires a search warrant based upon probable cause--the court held that the government's search was improper, noting that the government did not advise the magistrate, by affidavit or otherwise, that the BBS contained private electronic communications between users, nor how the disclosure of the contents of those communications related to the investigation.

In most cases, of course, the electronic communications sought will be in storage 180 days or less, and, therefore, may be obtained "only pursuant to a warrant." 18 U.S.C. 2703(a)(emphasis added). When preparing a warrant to

9 Pursuant to 18 U.S.C. 2707(d), a good faith reliance on a court warrant is a complete defense to any civil action. The court summarily rejected the defense, stating that it "declines to find this defense by a preponderance of the evidence in this case." Id. at 443.

[page 89]

search a computer, investigators should specifically indicate whether there is electronic mail on the target computer. If the agents intend to read those electronic communications, the warrant should identify whose mail is to be read, and establish that those electronic communications are subject to search under Fed. R. Crim. P. 41(b) (Search and Seizure, Property Which May Be Seized With a Warrant).

[no page 90]

[page 91]

VI. DRAFTING THE WARRANT

A. DRAFTING A WARRANT TO SEIZE HARDWARE

If a computer component is contraband, an instrumentality of the offense, or evidence, the focus of the warrant should be on the computer component itself and not on the information it contains. The warrant should be as specific as possible about which computer components to seize and, consistent with other types of warrants, it should describe the item to be seized in as much detail as possible, especially if there may be two or more computers at the scene. Include, where possible, the manufacturer, model number, and any other identifying information regarding the device. (For further information, see "SAMPLE COMPUTER LANGUAGE FOR SEARCH WARRANTS," APPENDIX A, p. 125.)

It may also be appropriate-to seek a "no-knock" warrant in cases where knocking and announcing may cause (1) the officer or any other individual to be hurt; (2) the suspect to flee; or (3) the evidence to be destroyed. (See "Seeking Authority for a No-Knock Warrant," infra p. 100.)

In computer cases, the evidence is especially perishable, and agents should never underestimate the subjects of the investigation. They may be knowledgeable about telecommunications and may have anticipated a search. As a result, computers and memory devices on telephone speed dialers may be "booby-trapped" to erase if they are improperly entered or if the power is cut off.

[page 92]

B. DRAFTING A WARRANT TO SEIZE INFORMATION

1. Describing the Place to be Searched

Until recently, when a warrant specified where a search was to occur, the exercise was bound by physical laws: agents took objects they could carry from places they could touch. But computers create a "virtual" world where data exists "in effect or essence though not in actual fact or form." The American Heritage Dictionary, (2d ed. 1983).

Rule 41(a) failed to anticipate the creation of this "virtual" world. By its very terms, a warrant may be issued "for a search of property ... within the district." Specifically, it provides that,

Upon the request of a federal law enforcement officer or an attorney for the government, a search warrant authorized by this rule may be issued (1) by a federal magistrate, or a state court of record within the

federal district, for a search of property or for a person within the district and (2) by a federal magistrate for a search of property or for a person either within or outside the district if the property or person is within the district when the warrant is sought but might move outside the district before the warrant is executed.

Fed. R. Crim. P. 41(a)(emphasis added).

In a networked environment, however, the physical location of stored information may be unknown. For example, an informant indicates that the business where he works has a duplicate set of books used to defraud the Internal Revenue Service. He has seen these books on his computer terminal in his Manhattan office. Based upon this information, agents obtain a warrant in the Southern District of New York authorizing a search for, and seizure of, these records. With the informant's help, agents access his computer workstation, bring up the incriminating documents, and copy them to a diskette.

[page 93]

Unfortunately, unbeknownst to the agents, prosecutor, or informant, the file server that held those documents was physically located in another office, building, district, state, or country.10

There are, under Rule 41, at least three variations on this problem. First, information is stored off-site, and agents know this second site is within the same district. Second, information is stored off-site, but this second site is outside the district. Third, information is stored off-site, but its location is unknown.

a. General Rule: Obtain a Second Warrant

Whenever agents know that the information is stored at a location other than the one described in the warrant, they should obtain a second warrant. In some cases, that will mean going to another federal district--nearby or across the country. If the data is located overseas, the Criminal Division's Office of International Affairs (202-514-0000) and our foreign law enforcement counterparts can assist in obtaining and executing the foreign warrant. The Computer Crime Unit (202-514-1026) can help in expediting international computer crime investigations.

b. Handling Multiple Sites within the Same District

Assuming that the server was simply in another office on the same floor, the warrant might well be broad enough to cover the search. Indeed, even with physical searches, courts have sometimes allowed a second but

related search to be covered by one warrant. In United States v. Judd, 687 F. Supp. 1052, 1057-9 (N.D. Miss. 1988), aff'd 889 F.2d 1410 (5th Cir. 1989), cert. denied,

10 In this example, the storage of information in an out-of-district server was fortuitous; i.e., a product of the network architecture. In fact, hackers may deliberately store their information remotely. This allows them to recover after their personal computers fail (essentially by creating off-site backup copies). Additionally, if agents seize a hacker's personal computer, no evidence will be found, and the hacker can still copy or destroy the remotely stored data by accessing it from another computer.

[page 94]

494 U.S. 1036 (1989), the FBI executed a search warrant for records at Address #1, and learned that additional records were located at Address #2. Without obtaining a second warrant, and relying only on the first, the agents entered Address #2 and seized the additional records.

The district court framed the question like this: was the partially incorrect description in the warrant sufficient to include both business addresses, which in this case, happened to be in the same building? The court held that since Address #2 was "part" of Address #l, and since they were both used for the business pursuits of the same company, the search was proper. See also United States v. Prout, 526 F.2d 380, 388 (5th Cir.) (search of adjacent separate apartment that was omitted from the warrant was proper), cert. denied, 429 U.S. 840 (1976).

It becomes more problematic when the server is in another building, one clearly not described in the warrant. In situations where a second warrant was not obtained, there is still an argument that remotely accessing information from a computer named in the warrant does not violate Fourth Amendment law. See discussion of United States v. Rodriguez, infra.

c. Handling Multiple Sites in Different Districts

What if, unbeknownst to the agents executing the search warrant, the property seized was located in another district? Although the defense could argue that the court lacked jurisdiction to issue the warrant, the agents executing the warrant never left the district in which the warrant was issued. Moreover, in some cases, it may be difficult, if not impossible, to ascertain the physical location of a given file server and obtain the evidence any other way. In these cases, prosecutors should

argue that the warrant authorized the seizure.

If agents have reason to believe the second computer may be in a different district, however, the issue should be addressed with the magistrate. While some courts may strictly construe the language of Rule 41 and require data to be retrieved only from the district where it permanently resides, other courts may follow the logic of the recent Second Circuit case United States v. Rodriguez, 968 F.2d 130 (2d Cir.), cert. denied, 113 S. Ct. 140 (1992). Although that case addressed the issue of "place" under the wiretap statute (18

[page 95]

U.S.C. 2518) and not under Rule 41, the constraints of the statute were quite similar. ("Upon such application the judge may enter an ex parte order ... approving interception ... within the territorial jurisdiction of the court in which the judge is sitting.... ")

In Rodriguez, the Second Circuit held that a wiretap occurs in two places simultaneously: the place where the tapped phone is located and the place where law enforcement overhears it. If those two places are in different jurisdictions, a judge in either one can authorize the interception. In this case, the DEA was tapping several phones in New York from its Manhattan headquarters. In addition, they tapped a phone in New Jersey by leasing a phone line from the service carrier and running it to the same New York office from which they monitored all the calls on all the lines. The court cited "sound policy reasons" for allowing one court to authorize all the taps, since all the reception and monitoring occurred in that same jurisdiction.

If the DEA can lease a phone line running from New Jersey to New York in order to consolidate its efforts, courts may also find it completely reasonable lo conclude that computer network data searches, like telecommunications interceptions, can occur in more than one place.

d. Information at an Unknown Site

Unfortunately, it may be impossible to isolate the location of information. What then? Does a warrant authorizing the search and seizure of one computer automatically allow agents to search and seize any data that it has sent to other computers? If the original warrant does not allow investigators to physically enter another building and search another computer, does it permit them to "go" there electronically, using as their vehicle only the computer that they have been authorized to search? What if the other computer is physically located in another district? Finally, if the warrant does not authorize seizing the off-site

data (no matter how it is obtained), are there circumstances under which it could be taken without a warrant?

If agents have reason to believe there is off-site storage but no way to identify the site, they should tell the magistrate. Of course, the standard to use in evaluating a description in the warrant is whether "the description is such

[page 96

that the officer with a search warrant can, with reasonable effort ascertain and identify the place intended." Steele v. United States, 267 U.S. 498, 503 (1925). See also United States v. Darensbourg, 520 F.2d 985, 987 (5th Cir. 1975), quoting United States v. Sklaroff, 323 F. Supp. 296, 321 (S.D. Fla. 1971).

Drawing upon Steele, it may be prudent for the warrant to specifically include any data stored off-site in devices which the subject computer has been configured by its operator to readily access, and which have been regularly used as a component of the subject computer. This is more likely to be upheld if the government has reason to believe the suspect is using an off-site computer and has no way to determine where it is, either geographically or electronically, until the suspect's computer is examined. In such cases, the affidavit should indicate why a complete address is not available, including any attempts that have been made to get the information (e.g., informants, undercover agents, pen registers, electronic or video surveillance) on the subject computer. It will be important to show a clear relationship between the computer described in the warrant and the second computer at the different location. If the second computer is somewhere in the same district, that also holds the second data search closer to the physical terms of Rule 41.

e. Information/Devices Which Have Been Moved

What happens if the targets: (1) move computers and storage devices (disk drives, floppies, etc.) between two or more districts (e.g., a laptop computer); or (2) transmit data to off-site devices located in another district?

Under Rule 41(a)(2), a magistrate in one district can issue a warrant to be executed in another district provided the property was "within" District A when the warrant was issued. Again, this rule is relatively easy to apply when physical devices are the object of the search. But how does that rule apply to electronic data? If a suspect creates data in District A and uploads11 that data

11 "Upload" means to transfer data from a user's system to a remote computer system. Wehster's, supra. Of course, only a copy is transferred, and the original remains on the user's machine. It may be significant to search for the uploaded data even if the original has been seized. For example, the user may have altered the original.

[page 97]

to a computer in District B, has he "moved" it between districts, thus authorizing a District A magistrate to issue a warrant for a search of the District B computer, even though the District B computer was never physically transported from or even located in District A?

The key to resolving these issues is understanding what agents are seizing. If they are going to seize the computer hardware in District B to get the data, they must get a warrant in District B (after all, the District B computer was never moved). If agents are simply copying data, however, it could be argued that the data uploaded from District A to District B is property that has been moved. Since the item to be seized is data and not its storage device, the "within the district" requirement is fulfilled.

2. Describing the Items to be Seized

When the evidence consists of information in a computer system, but the computer itself is not an instrumentality of the offense or otherwise seizable, the hardware is simply a storage device. First and foremost, all technical matters aside, searching the computer is conceptually similar to searching a file cabinet for papers. One important difference is that while the storage capacity of a file cabinet is limited, the storage capacity of computers continues to increase. A standard 40-megabyte hard drive contains approximately 20,000 pages of information, and 200+ megabyte drives are already quite common. Therefore, although the computer itself is no more important to an investigation than the old cabinet was, the technology may complicate enormously the process of extracting the information.

Bearing this analogy in mind, if agents have probable cause only for the documents in the computer and not for the box itself, they should draft the warrant with the same degree of specificity as for any other document or business record in a similar situation. For example, the detail used to describe a paper sales receipt (for a certain product sold on a certain date) should not be any less specific merely because the record is electronic.

As with other kinds of document cases, the breadth of a warrant's authority to search through a suspect's computer will depend on the breadth of the criminality. Where there is probable cause to believe that an enterprise

[page 98]

is pervasively illegal, the warrant will authorize the seizure of records (both paper and electronic) far more extensively than if probable cause is narrow and specific. "When there is probable cause to seize all [items], the warrant may be broad because it is unnecessary to distinguish things that may be taken from things that must be left undisturbed." United States v. Bentley, 825 F.2d 1104, 1110 (7th Cir.), cert. denied, 484 U.S. 901 (1987). But by the same token, "[w]hen the probable cause covers fewer documents in a system of files, the warrant must be more confined and tell officers how to separate documents to be seized from others." Id. at 1110. See also Application of Lafayette Academy, Inc., 610 F.2d 1 (lst Cir. 1979). There is nothing about the nature of searching for documents on a computer which changes this underlying legal analysis. Each warrant must be crafted broadly or specifically according to the extent of the probable cause, and it should focus on the content of the relevant documents rather than on the storage devices which may contain them.

The difficulties arise when, armed with a narrow and specific warrant, agents begin the search. If agents know exactly what they are looking for (a certain letter; a voucher filed on a particular date), it may be simple enough to state it in the warrant. But because computers, like file cabinets, can store thousands of pages of information, the specific letter may be much easier to describe than to find. Some may argue, with good reason, that the sheer volume of evidence makes it impractical to search on site. (For a more extensive discussion of these issues, see "DECIDING WHETHER TO CONDUCT THE SEARCH ON-SITE OR TO REMOVE HARDWARE TO ANOTHER LOCATION," supra p. 55.)

Even so, the volume-of-evidence argument, by itself, may not justify seizing all the information storage devices--or even all of the information on them--when only some of it is relevant. In In Re Grand Jury Subpoena Duces Tecum Dated November 15. 1993, 846 F. Supp. 1 1 (S.D.N.Y. 1994), the district court applied a similar analysis to a grand jury subpoena for digital storage devices. In that case, the government had subpoenaed the central processing units, hard disks, floppy disks, and any other storage devices supplied by the target corporation ("X Corporation") to specified officers and employees of the corporation. Of course, these storage devices also contained unrelated information, including some that was quite personal: an employee's will and individual

financial records and information. When "X Corporation" moved to quash the subpoena, the government acknowledged that searching the storage devices by 'key word' would identify the relevant documents for the grand jury's investigation. Even so, prosecutors continued to argue for

[page 99]

enforcement of the subpoena as written, particularly because the grand jury was also investigating the corporation for obstruction of justice. In quashing the subpoena, the judge clearly distinguished between documents or records and the computer devices which contain them.

The subpoena at issue here is not framed in terms of specified categories of information. Rather, it demands specified information storage devices.... Implicit in [an earlier case] is a determination that subpoenas properly are interpreted as seeking categories of paper documents, not categories of filing cabinets. Because it is easier in the computer age to separate relevant from irrelevant documents, [the] ontological choice between filing cabinets and paper documents has even greater force when applied to the modern analogues of these earlier methods of storing information.

Although the judge found that investigating the corporation for "obstruction and related charges indeed justifies a commensurately broader subpoena ...," he declined to modify, rather than quash, the subpoena at issue because "this Court does not have sufficient information to identify relevant documents (including directory files)...." The court's reference to directory files seems to imply that the directory would necessarily list everything in the storage device--which is, of course, not true. A directory would not display hidden, erased, or overwritten files which could still be recoverable by a computer expert. Perhaps the judge's conclusion might have been different if the government had proceeded by search warrant rather than subpoena. In any case, it is interesting to note that the court, in trying to find a balance, suggested that when a grand jury suspects "that subpoenaed documents are being withheld, a court-appointed expert could search the hard drives and floppy disks."

3. Removing Hardware to Search Off-Site: Ask the Magistrate for Explicit Permission.

Because the complexities of computer data searches may require agents to remove computers from a search scene, agents and prosecutors should anticipate this issue and, whenever it arises, ask for the magistrate's express

[page 100]

permission. Obviously, the more information they have to support this decision, the better--and the affidavit should set out all the relevant details. It will be most important to have this explicit permission in the warrant for those cases where (as in Tamura, supra p. 58) agents must seize the haystack to find the needle.

If the original warrant has not authorized this kind of seizure, but the agent discovers that the search requires it, she should return to the magistrate and amend the warrant, unless exigencies preclude it.

4. Seeking Authority for a No-Knock Warrant

a. In General

Under 18 U.S.C. 3109, an agent executing a search warrant must announce his authority for acting and the purpose of his call. See, e.g., United States v. Barrett, 725 F. Supp. 9 (D.D.C. 1989)("Police, search warrant, open up"). This knock-and-announce requirement, although statutory, has been incorporated into the Fourth Amendment, United States v. Bustamante-Gamez, 488 F.2d 4, 11-12 (9th Cir. 1973), cert. denied, 416 U.S. 970 (1974), and therefore a statutory violation may also be a constitutional one. United States v. Murrie, 534 F.2d 695, 698 (6th Cir. 1976); United States v. Valenzuela, 596 F.2d 824, 830 (9th Cir.), cert. denied, 441 U.S. 965 (1979). The knock~-and-announce rule is designed to reduce the possibility of violence (the occupant of the premises may believe a burglary is occurring), reduce the risk of damage to private property (by allowing the occupant to open the door), protect the innocent (the agent may be executing the warrant at the wrong location), and symbolize the government's respect for private property.

Of course, if no one is present, there is no one to notify, and agents can search the place without waiting for its occupant. United States v. Brown, 556 F.2d 304 (5th Cir. 1977). The knock-and-announce requirement also does not apply when the door is open. United States v. Remigio, 767 F.2d 730 (10th Cir.), cert. denied, 474 U.S. 1009 (1985). It is unclear whether the rule applies to businesses, as different courts have reached different conclusions.

[page 101]

Cf. United States v. Agrusa, 541 F.2d 690 (8th Cir. 1976)(3109 applies to businesses), cert. denied, 429 U.S. 1045 (1977), with United States v. Francis, 646 F.2d 251 (6th Cir.)(3109 applies only to dwellings), cert. denied, 454 U.S. 1082 (1981).

After knocking and announcing, agents must give the occupants a reasonable opportunity to respond, although exigent circumstances may justify breaking in without an actual refusal. Compare United States v. Ruminer, 786 F.2d 381 (10th Cir. 1986)(break-in authorized where police waited five seconds and saw people running in house), with United States v. Sinclair, 742 F. Supp. 688, 690-1 (D.D.C. 1990)(one- to two-second delay, even with noise inside, was insufficient to warrant break-in).

Moreover, exigent circumstances may justify forcible entry without "knocking and announcing" at all. Circumstances are exigent if agents reasonably believe that giving notice to people inside could cause (1) the officer or any other individual to be hurt; (2) a suspect to flee; or (3) the evidence to be destroyed. Additionally, investigators need not knock and announce when it would be a "useless gesture" because the people inside already know their authority and purpose.

b. In Computer-Related Cases

In many computer crime cases, the primary concern will be preserving the evidence. Technically adept suspects may "hot-wire" their computers in an effort to hide evidence. Although there are many ways to do this, two more common practices involve "hot keys" and time-delay functions. A "hot key" program is designed to destroy evidence, usually by overwriting or reformatting a disk, when a certain key is pressed.12 Thus, when officers knock at the door and announce their presence, the subject of the search can hit the key that activates the program. A time-delay function is a program that monitors the keyboard to determine whether the user has pressed any key. If no key is

12 Of course, the fact that this occurs does not mean the evidence cannot he salvaged. Experts can often recover data which has been deleted or overwritten.

pressed within a certain period of time, such as 30 seconds, the program activates and destroys data. A target may, therefore, answer the door slowly and attempt to delay the agent's access to the machine.

These problems, which may be present in every computer crime investigation, are not, standing alone, sufficient to justify dispensing with the knock-and-announce rule. Most courts have required agents to state specifically why these premises or these people make it either dangerous or imprudent to knock and announce before a search. See United States v. Carter, 566 F.2d 1265 (5th Cir. 1978)(someone inside yelled

"It's the cops" and the agent, who had a warrant to search for heroin, heard running inside), cert. denied, 436 U.S. 956 (1978); United States v. Stewart, 867 F.2d 581 (10th Cir. 1989)(collecting cases). But cf. United States v. Wysong, 528 F.2d 345 (9th Cir. 1976)(mere fact that police knew defendant was trafficking in an easily destroyable liquid narcotic created exigent circumstance that justified entry without knocking and announcing).

In short, most cases hold that agents must have some reasonable, articulable basis to dispense with the knock-and-announce requirement. Moreover, in light of the salutary purposes served by the rule, they should have very good reasons before deviating from it. In appropriate cases, however, a no-knock warrant should be obtained. In deciding whether to seek a no-knock warrant, agents should consider, among other things: (1) what offense is being investigated (is it a narcotics case where the subjects may be armed, or is it non-violent hacking?); (2) is there information indicating evidence will be destroyed (in one recent hacker case, the targets talked about destroying evidence if raided by the police); (3) the age and technical sophistication of the target; and (4) whether the target knows, or may know, he is under investigation.

[page 103]

VII. POST-SEARCH PROCEDURES

A. INTRODUCTION

As noted above, the government is permitted to search for and to seize property that is contraband, evidence, or an instrumentality of the offense. The law does not authorize the government to seize items which do not have evidentiary value, and generally agents cannot take things from a search site when their non-evidentiary nature is apparent at the time of the search.

With computer crimes, however, it is not always possible to examine and separate wheat from chaff at the search location. There may be thousands of pages of data on the system; they may be encrypted or compressed (and thus unreadable); and searching computers frequently requires expert computer skills and equipment. All these factors contribute to the impracticality of on-site processing. Accordingly, agents will often seize evidentiary materials that are mixed in with collateral items. (See "DECIDING WHETHER TO CONDUCT THE SEARCH ON-SITE OR TO REMOVE HARDWARE TO ANOTHER LOCATION," supra p. 55.)

For several reasons, it is important to separate evidence (and contraband, fruits, and instrumentalities) from irrelevant items. First,

as noted above, the law does not generally authorize seizing non-evidentiary property. But to the extent agents sort and return these materials after a search, the courts are less likely to require that large amounts of data be sorted at the scene. Put another way, if law enforcement authorities routinely retain boxes of property that are not evidence, the courts surely will become less sympathetic in those cases where it is, in fact, appropriate to seize entire systems and analyze them later at the lab.

A second reason to promptly sort seized evidence is that the process will help to organize the investigation. Agents and prosecutors will obviously want to focus on the evidence when preparing complaints or indictments. Getting a handle on the items that advance the case will help agents assess quickly and accurately where the case should go. As much as overbroad seizures offend the

[page 104]

law, they are just as bad for the investigation. Investigators should cull out the things that do not help the case right away to avoid endlessly sifting through unimportant materials as the investigation progresses.

Procedures for sorting, searching, and returning seized items will depend in part upon the type of evidence involved. There are, however, certain basic concepts that apply across the board. The basics include the following.

B. PROCEDURES FOR PRESERVING EVIDENCE

1. Chain of Custody

Computer evidence requires the same chain of custody procedures as other types of evidence. Of course, the custodian must strictly control access and keep accurate records to show who has examined the evidence and when. (For a further discussion of this issue, see "EVIDENCE: Chain of Custody," infra p. 119.)

2. Organization

As with other parts of the investigation, the sorting process should be as organized as possible. If there are only a few agents involved, each with discrete tasks, the job is likely to be quick and efficient. Many agents, unsure of their tasks, are more likely to misplace or overlook evidence. An organized review process, which is part of a larger, well-briefed search plan, is also easier to describe and defend in court.

[page 105]

3. Keeping Records

Agents should always document their investigative activities. This allows other agents and attorneys to keep track of complex investigations, and will help the case agent reconstruct the sorting process at a later time if necessary. A log should be kept that describes each item seized, whether it was examined, and whether it contained evidence.

When items are returned, a receipt should set out: (a) a clear description of the item, (b) the person who received it (with a signature and identification), and (c) when the item was released. It often makes sense to return all items at one time rather than to do it piecemeal. Also, it is a good idea to keep photographs of the property returned in order to avoid disputes.

4. Returning Seized Computers and Materials

Once agents have removed the computer system from the scene, an expert should examine the seized material as soon as practicable. This examination may be conducted by a trained field office agent, a special agent sent to the field office for this purpose, or by a properly-qualified private expert. Some agencies may require that the computer system be shipped to a laboratory. Each agency should establish and follow a reasonable procedure for handling computerized evidence.

Once the analyst has examined the computer system and data and decided that some items or information need not be kept, the government should return this property as soon as practicable. The courts have acknowledged an individual's property interest in seized items, and the owner of seized property can move the court for a return of property under Fed. R. Crim. P. 41(e). That remedy is available not only when the search was illegal, but also if the person simply alleges a "deprivation of property by the Government." In Re Southeastern Equipment Co. Search Warrant, 746 F. Supp. 1563 (S.D. Ga. 1990).

[page 106]

Agents and prosecutors must remember that while a computer may be analogous to a filing cabinet for the agents who search it, it is much more to most computer users. It can be a data processor, graphics designer, publisher, and telecommunications center. Courts will no doubt recognize the increasingly important role computers play in our society,

and the public's extensive reliance on these computers to support the way we live and do business. As a result, law enforcement should be prepared to look carefully at the circumstances of each case and to seize computers only as needed, keeping them only as necessary.

a. Federal Rules of Criminal Procedure: Rule 41(e)

While computer-owners may be especially eager for return of their hardware, software, data, and related materials, the issue of whether to retain or return lawfully seized property before trial is not unique to computers. Rule 41(e) of the Federal Rules of Criminal Procedure sets out the standards and procedures for returning all property seized during the execution of a search warrant. The Rule, in general, provides that a party who is "aggrieved by an unlawful search and seizure or by the deprivation of property" may file a motion for the return of the property on the ground that the party is entitled "to lawful possession of the property." 13

A Rule 41(e) motion for return of property can be made either before or after indictment. However, a district court's jurisdiction over a pre-indictment motion is more limited than if the indictment has been returned. Pre-indictment remedies are equitable in nature and must only be exercised with "caution and restraint." Floyd v. United States, 860 F.2d 999, 1003 (10th Cir. 1988). The Tenth Circuit, the only Circuit to address this issue, held that two conditions must be satisfied before a district court may assume jurisdiction over a pre~indictment Rule 41(e) motion: "a movant must demonstrate that being deprived

13 Rule 41(e) does not distinguish according to how the property was used in the offense; thus, a computer used as an instrumentality of an offense (e.g., to duplicate copyrighted software or hack into other systems) is not treated differently for Rule 41 analysis from a computer used as a "storage cabinet" for documents. Of course the government's interest in seizing and keeping the computer in each case is different and, thus, from a realistic standpoint, how the computer was used in the offense is important in determining whether to retain or return it.

of actual possession of the seized property causes 'irreparable injury' and must be otherwise without adequate remedy at law." Matter of Search of Kitty's East, 905 F.2d 1367, 1371 (1Oth Cir. 1990).

Because of the paucity of cases in this area, it is very difficult to say what facts will satisfy this two-part test. However, the reported decisions do offer guidance in responding to a request for the return of

seized property. The Tenth Circuit in Kitty's East held that the "irreparable injury" element is not satisfied by the threat of an imminent indictment. 905 F.2d at 1371, citing Blinder, Robinson & Co. v. United States, 897 F.2d 1549, 1557 (1Oth Cir. 1990). The appellate court in Kitty's East upheld the district court's decision to take jurisdiction because the nature of the seized materials--pornographic videotapes--invoked the First Amendment right of free speech. "Although the interests of the commercial speech at issue here may not equate with those of political speech, we agree that the special protections of the First Amendment justified the exercise of equitable jurisdiction in this case." Id. Conversely, the Blinder court rejected the movant's contention that it was irreparably injured by the government's failure to return original documents: "[T]he record strongly suggests that [the movant] is able to operate with photocopies of the documents seized by the government and either has copies or can make copies of all the property that the government seized." Blinder, 897 F.2d at 1557.

Once jurisdiction has been established, Rule 41(e), according to the Tenth Circuit, requires the party to also show that the retention of the property by the government is unreasonable:

Reasonableness under all of the circumstances must be the test when a person seeks to obtain the return of property. If the United States has a need for the property in an investigation or prosecution, its retention of the property generally is reasonable. But, if the United States' legitimate interests can be satisfied even if the property is returned, continued retention of the property would become unreasonable.

Id., quoting Committee Note to 1989 Amendment at 30, 124 F.R.D. at 428.

As described, the Kitty's East court initially held the district court had properly exercised jurisdiction over the motion because of the possibility that the movant's First Amendment rights would be impaired. However, the court then denied the Rule 41(e) motion for the return of the seized property. The

[page 108]

court held that Kitty's East failed to demonstrate that it was aggrieved by an unreasonable retention of the property:

With regard to the videotapes seized, Kitty's has made no argument that the seizure has precluded all exhibition or rental of the videotapes in question. Kitty's First Amendment rights are not sufficiently infringed by the government's seizure for evidence of a few copies of a limited number of videotapes to be 'aggrieved' under Rule 41(e).... Further,

return of the videotapes would pose too great a risk of loss of potential evidence. As the Supreme Court has noted, 'such films may be compact, readily transported for exhibition in other jurisdictions, easily destructible, and particularly susceptible to alteration by cutting and splicing critical areas of film.' We hold therefore, that the government's retention of no more than two evidentiary copies of each film is reasonable and does not 'aggrieve' Kitty's under Rule 41(e).

905 F.2d at 1376 (citations omitted).

In United States v. Taft, 769 F. Supp. 1295, 1307 (D. Vt. 1991) the court relied on Kitty's East to deny a motion for the return of two firearms which had been legally seized by the government during the execution of a search warrant. Moreover, the court refused to second guess the government about the evidentiary value of the guns: "[H]aving decided that the government legally seized the two firearms, this court will not opine as to the evidentiary value of the guns in the instant prosecution for cultivation of marijuana."

The decisions addressing Rule 41(e) impose a heavy burden on a party seeking the return of property, including computers, lawfully seized by the government. However, unless there is a reason not to do it, agents should explore giving the computer owner copies of the computer disks seized--even when Rule 41(e) does not require it. This is especially true if the owner needs the data to run a business. Of course, if the information stored on the disks is contraband or if copying the information would jeopardize the investigation, agents should not make copies for the owner.

Similarly, if the owner of a seized computer needs it for business, there may be intermediate solutions. For example, using careful scientific protocols and keeping exacting records, an analyst can make printouts from the hard drives to have "original" records to admit in court. Following the same process, the analyst can then make a mirror image (or "bit-stream") data copy

[page 109]

of the hard drives for later analysis. Before returning the computers, agents should explain the printout and copying processes used, and give the defense an opportunity to object to the integrity and admissibility of the printouts and copies at that time. Best practice is to ask the defense counsel to sign an explicit waiver of those issues at the time the computer is returned and to stipulate that printouts and electronic copies will be admissible under Fed. R. Evid. 1001. (For a more extensive discussion of admitting electronic evidence, see "EVIDENCE," infra p.

113.) If the defense refuses to concede the accuracy and admissibility of the printouts and copies, the government should keep the computer. (For a form "Stipulation for Returning Original Electronic Data," see APPENDIX A, p. 135).

b. Hardware

In deciding whether to retain hardware, agents should consider several factors. Aspects that weigh in favor of keeping hardware include: (1) the hardware was used to commit a crime, was obtained through criminal activity, or is evidence of criminal activity, (2) the owner of the hardware would use it to commit additional crimes if it were returned, (3) the hardware is unique and is either essential for recovering data from storage devices or difficult to describe without the physical item present in court, and (4) the hardware does not serve legitimate purposes. Factors that weigh in favor of returning hardware include: (1) a photograph of the hardware would serve the same evidentiary purpose as having the machines in court, (2) the hardware is an ordinary, unspecialized piece of equipment such as a telephone, (3) the hardware is used primarily for legal purposes, and (4) the hardware is unlikely to be used criminally if returned.

Although the result will depend on the precise facts of each case, some basic principles are clear. Where hardware was used to commit a crime (instrumentality) or is the proceeds of crime (fruit) and it belongs to the suspect, agents should generally keep it. When the hardware clearly is not evidence of a crime (e.g. an electronic wristwatch which turns out to have no memory), it should generally be returned.

[page 110]

The difficult situations arise when hardware was only tangential in the crime, played primarily a non-criminal role, or does not belong to the suspect. In these cases, agents and prosecutors must balance the government's need to retain the original items against the property owner's interest in getting them back. In any case, aggrieved property owners can ask the court to order the government to return even lawfully-seized items. See Fed. R. Crim. P. 41(e).

c. Documentation

Warrants often include computer books, programming guides, user manuals and the like. These items may have evidentiary significance in several ways: they may be proprietary (e.g. telephone company technical manual for employees); they may indicate that software, hardware, or the manuals themselves were obtained illegally; they may be necessary for searching a

particular, customized machine also covered by the warrant; or they may contain handwritten notes about how the subject used the machine. In this case, agents should treat the books and manuals as evidence and retain them.

Very often, however, books and manuals are not unique. Most of the time, they will be publicly available user guides without significant handwritten notes. They may be convenient references for investigators, but they do not add anything that could not be commercially purchased. In such cases, Rule 41(e) does not require subjects to supply such equipment or technical information, so these items (if they contain no evidence) should be returned.

d. Notes and Papers

Notes and papers often contain extremely valuable information like passwords, login sequences, and other suspects' telephone numbers or names. Notes also tend to be rather cryptic, so agents will not always know right away what they are. Accordingly, it may be appropriate to retain notes and papers until they can be carefully examined, but agents should return records that are clearly not evidence or instrumentality.

[page 111]

e. Third-Party Owners

The retain-or-return question is particularly delicate when the evidence (usually hardware) belongs to innocent third parties. While the government is clearly entitled to seize evidence no matter who owns it, Rule 41(e) of the Federal Rules of Criminal Procedure recognizes that the property owner may move for return of unreasonably held items. See Fed. R. Crim. P. 41(e) advisory committee note (1989)("reasonableness under all of the circumstances must be the test when a person seeks to obtain the return of property"). The committee notes further point out that the government's legitimate interests can often be satisfied "by copying documents or by conditioning the return on government access to the property at a future time." Id.

When a third party claims ownership, it is important to evaluate competing claims before deciding what to do. The worst solution is to return property to someone who later turns out not to have been the rightful owner. Thus, whenever it is appropriate to return property, agents must verify ownership with documents or other reliable evidence. If in doubt, it is best to retain the item and let the aggrieved parties assert their various claims in court. This way, the government will not become embroiled in complicated ownership investigations, and will not

release property to the wrong party. [no page 112] [Page 113]

VIII. EVIDENCE

A. INTRODUCTION

Although the primary concern of these Guidelines is search and seizure, the ultimate goal is to obtain evidence admissible in court. From the moment agents seize electronic evidence, they should understand both the legal and technical issues that this sort of evidence presents under the Federal Rules of Evidence.

It can be especially confusing to think about digital proof because, both in our current discussions and in early cases, legal analysts have tended to treat "computer evidence" as if it were its own separate, overarching evidentiary category. Of course, in some very practical ways electronic evidence is unique: it can be created, altered, stored, copied, and moved with unprecedented ease, which creates both problems and opportunities for advocates. But in many important respects, "computer evidence," like any other, must pass a variety of traditional admissibility tests.

Specifically, some commentary is not very clear whether admitting computer records requires a "best evidence" analysis, an authentication process, a hearsay examination, or all of the above. Advocates and courts have sometimes mixed, matched, and lumped these ideas together by talking simply about the "reliability" or "trustworthiness" of computer evidence in general, sweeping terms, rather than asking critically whether the evidence was "trustworthy" in all required aspects.

Part of the reason for this is probably that the first computer evidence offered in court was information generated by businesses. Long before most people used computers in their homes, telephone companies and banks were using them to record, process, and report information that their businesses required. Not surprisingly, many of the early decisions link computer evidence with the business records exception to the hearsay rule. Of course, that exception--which is meant to address a substantive hearsay problem--also includes a sort of internal authentication analysis. (Fed. R. Evid. 803(6)

[Page 114]

requires a showing that a record was made "at or near the time by, or from information transmitted by, a person with knowledge. . .").

But "computer evidence" as we know it today covers the universe of documentary materials, and is certainly not limited to business records.

Computer evidence may or may not contain hearsay statements. It will always need to be authenticated in some way. And data that has been produced, processed, and retrieved under circumstances other than the discipline of a business probably will not contain the qualities that make electronic evidence "reliable" as a business record. Even business records, themselves, may require a closer look, depending on what the proponent wants to do with them at trial.

The key for advocates will be in understanding the true nature of each electronic exhibit they offer or oppose: for what purpose and by what process (both human and technological) was it created? And what specific issues of evidence (rules of form? rules of substance?) does that particular electronic item raise?

B. THE BEST EVIDENCE RULE

One of the issues that investigators and lawyers sometimes cite as troublesome in working with electronic evidence turns out, on examination, to be a largely surmountable hurdle: the "best evidence rule." This rule provides that "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress." Fed. R. Evid. 1002.

The impact of this rule is softened considerably by its reference to other rules. Indeed, Fed. R. Evid. 1001 makes clear in two separate provisions that when it comes to electronic documents, the term "original" has an expansive meaning. First of all, Fed. R. Evid. 1001(1) defines "writings and recordings" to explicitly include magnetic, mechanical, or electronic methods of "setting down" letters, words, numbers, or their equivalents. Clearly, then, when someone creates a document on a computer hard drive, for example, the electronic data stored on that drive is an admissible writing. A proponent could obviously offer it to a court by producing the hard drive in court and displaying

it with a monitor. But that somewhat cumbersome process is not the only choice. In telling us what constitutes an "original" writing or recording, Fed. R. Evid. 1001(3) says further that "[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" Thus, so long as they are accurate, paper printouts from electronic storage devices qualify as "originals" under the rule, and there is clearly no evidentiary need to haul computer equipment into a courtroom simply to

admit a document--although there sometimes may be tactical reasons for doing so.

But even having set up that inclusive definition of "original" writing, the Federal Rules go much further to relax the common law standard. Fed. R. Evid. 1003 provides that "[a] duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." Therefore, unless authenticity or some "unfairness" is at issue, courts may freely admit duplicate electronic documents. "Duplicate" is defined in Fed. R. Evid. 1001(4) as "a counterpart produced by the same impression as the original ... by mechanical or electronic re-recording ... or by other equivalent techniques which accurately reproduces (sic) the original." Many investigative agencies analyze data evidence from exact electronic copies (called "bit-stream" copies) made with commercial or custom-made software. So long as the copies have been properly made and maintained, the Federal Rules allow judges to accept these copies (or expert opinions based on them) as readily as the originals.

Thus, the Federal Rules have, despite their nod to the best evidence rule, made way for a lively courtroom use of electronic evidence in all its many forms. Questions of admissibility turn not on whether the data before a court is on a hard drive, a duplicate floppy disk, or a printout of either one. Instead, courts must ask whether the original data is authentic and whether any copies offered are accurate.

C. AUTHENTICATING ELECTRONIC DOCUMENTS

Of course, every time trial lawyers offer any piece of evidence, they must be ready to show that, as the authentication rule, Fed. R. Evid. 901(a),

[Page 116]

states, "the matter in question is what its proponent claims." Clearly, there are many ways to do this, including the ten illustrations offered by Fed. R. Evid. 901 (b).

1. "Distinctive" Evidence

One of the most common methods for authenticating evidence is to show the item's identity through some distinctive characteristic or quality. Indeed, the authentication requirement of Fed. R. Evid. 901(a) is satisfied if an item is "distinctive" in its "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken

in conjunction with circumstances." Fed. R. Evid. 901(b)(4). In fact, it is standard practice to use this method to authenticate some kinds of evidence which may now be digitally created, stored, and reproduced. For example, attorneys offering photographs into evidence invariably just ask a "witness with knowledge" (under Fed. R. Evid. 901(b)(1)) whether a particular photo is "a fair and accurate representation" of something or someone. But should the process of authenticating photographs recognize that, with the advent of digital photography, it is now possible to alter an electronic image without leaving a trace? Consider the following example.

Agents and prosecutors were shown a photograph of a body--twisted on the floor, a gaping wound in the chest. Across the room, on the floor, was a large pistol. On the white wall above the victim's body, scrawled in the victim's own blood, were the words, "I'll kill again. You'll never catch me."

Unlike conventional photographs, however, this picture was not created with film, but with a digital camera. The entire picture was made up of binary digits, ones and zeros, which could be altered without detection. So two law enforcement agents, using commercially available software, started rearranging the digits. They "cleaned" the wall, removing the bloody words. They closed the chest wound, choosing instead to have blood trickling from the victim's temple. Last, they moved the gun into the victim's hand. The case was now solved: the report would claim, and the photograph would "prove," the victim committed suicide.

[Page 117]

This was, of course, only a demonstration, which took place in the summer of 1991 at a meeting of the Federal Computer Investigations Committee. The Committee had been established by a handful of federal and state law enforcement personnel who were among the first to appreciate how emerging technologies were both providing new opportunities for criminals and creating new challenges for law enforcement officials. For this group, the point of this demonstration was apparent: not only could ordinary photographs not be trusted in the same old way to be reliable, but an ordinary agent might be duped if he or she were not technologically astute enough to realize the potential for sophisticated digital alteration. The key, of course, is that there is no negative, and the alteration leaves no tracks.

Nor will these authenticity problems be limited to photographs. For example, some package delivery services now allow recipients to sign for their packages on a hand-held device which creates a digital copy of the recipient's signature. Although this makes it easy to transfer the

information to a computer, it also enables the computer to recreate the signature. If the hand~held device measures and records the pressure applied by the signer and if the computer reprints that signature with an ink-based printer, the computer~-generated copy will look absolutely authentic--even to the author.

Despite these examples, there will be many times when electronic evidence--whether photographs or documents--will indeed be identifiable based on distinctive characteristics alone. An eyewitness can just as easily identify a digital photograph of a person as he could a conventional photo. The question for both judge and jury will be the witness's ability and veracity in observing and recalling the original person, photo, scene, or document with which he compares the in-court version. The fact that it is possible to alter a photo--for example, to extend the skid marks at an accident scene--is far less significant if the authenticating witness is independently sure from observing the site that the skid marks were, in fact, ten feet long. Similarly, the recipient of a discarded electronic ransom note may recall the content of the original note well enough to authenticate a printout from the accused's computer.

But to the extent that in-court photos or documents support incomplete or fading witness memories--or even substitute for witness memory altogether--lawyers must realize that "distinctive characteristics" in electronic evidence may be easy to alter, and may not, depending on the circumstances, satisfy a court. What witness can independently verify the distinctive accuracy of long lists of names or numbers? Can he say that a digital photo is "a fair and accurate

representation of a crime scene" in all details--no matter how minor they may have seemed at the time? While he will probably be able to remember whether there was a knife sticking out of a body, will he be able to verify the precise location of a shoe across the room? An eyewitness who picked out the defendant at a line-up should be able to look at a photograph of the array and find the defendant again. But can she say for sure, when testifying at a hearing on defendant's motion to suppress an allegedly suggestive line-up, that all the other people in the picture are exactly as she saw them? Has there been no mustache added in this picture, no height or weight changed in any way? And although the recipient of a ransom note may well be able to recall the exact words of the note, will he recall the type face?

It is important to remember that the traditional process of authenticating an item through its uniqueness often carries an unspoken

assumption that the thing--the murder weapon, the photo, or the letter, for example--is a package deal. It either is or is not the thing the witness remembers. Thus, if the witness can identify particular aspects of the item with certainty (such as the content of the ransom note), the other aspects (such as the type face) usually follow along without much debate. Of course, there are times, even with conventional photography, when an authenticating witness will be asked about internal details: "When you saw the crime scene at 5:30, were the shoes both on the right side of the room?" In those circumstances, attorneys and judges naturally tend to be more exacting in establishing that the witness can authenticate not only part of the package, but all the parts that matter.

But with digital photography, this rather minor problem of authentication takes on a new life. Depending on the way electronic evidence has been produced, stored, and reproduced, the collection of ones and zeros that constitutes the "package" of the photograph is infinitely and independently variable--not by moving shoes at the crime scene, but by changing any digits at any time before the exhibit photo is printed. Perhaps judges will find themselves admitting digital photographs and documents based on "distinctive characteristics" if a witness with knowledge can identify and authenticate the item in all relevant detail. But that, of course, requires a judge to know in advance which details will be relevant to the case and which are insignificant. If the characteristic that makes the item distinctive is not the same one that makes it relevant, judges might and should be wary about admitting digital

[Page 119]

evidence in this way. Even if judges are satisfied, attorneys who cross examine an authenticating witness on minute details of digital photographs may affect the witness's credibility with the jury, especially if the attorney shows how easily the evidence could be altered.

One of the potential solutions to this problem which arises from the nature of electronic evidence may actually be electronic: digital signatures. The Digital Signature Standard, proposed by the National Institute of Standards and Technology (NIST) in the Department of Commerce, would allow authors to encrypt their documents with a key known only to them. Assuming the author has not disclosed his password to others, this identifying key could serve as a sort of electronic evidence seal. In that event, the signature would be just the kind of distinctive characteristic the rules already recognize.

For the time being, however, most computer evidence can still be altered

electronically--in dramatic ways or in imperceptible detail--without any sign of erasure. But this does not mean that electronic evidence, having become less distinctive, has become any less admissible. It simply may require us to authenticate it in other ways.

2. Chain of Custody

When prosecutors present evidence to a court, they must be ready to show that the thing they offer is the same thing the agents seized. When that evidence is not distinctive but fungible (whether little bags of cocaine, bullet shell casings, or electronic data), the "process or system" (to use the language of Fed. R. Evid. 901(b)(9)) which authenticates the item is a hand-to-hand chain of accountability.

Although courts generally have allowed any witness with knowledge to authenticate a photograph without requiring the photographer to testify, that may not suffice for digital photos. Indeed, judges may now demand that the proponent of a digital picture be ready to establish a complete chain of custody --from the photographer to the person who produced the printout for trial. Even so, the printout itself may be a distinctive item when it bears the authenticator's initials, or some other recognizable mark. If the photographer takes a picture, and then immediately prints and initials the image that becomes

[Page 120]

an exhibit, the chain of custody is just that simple. But if the exhibit was made by another person or at a later time, the proponent should be ready to show where the data has been stored and how it was protected from alteration.

3. Electronic Processing of Evidence

When data goes into computers, there are many methods and forms for getting it out. To the extent that computers simply store information for later retrieval, a data printout may qualify as an original document under Fed. R. Evid. 1001(3). Where the computer has merely acted as a technological file cabinet, advocates must be ready to authenticate the in-court version of the document as genuine, but the evidentiary issues (at least those connected to the computer) do not pertain to the substance or content of the document.

But in many cases, attorneys want to introduce evidence that the computer has not only stored, but has also processed in some fashion. If the computer, its operating system, and its applications software have reorganized the relevant information--by comparing, calculating,

evaluating, re-grouping, or selectively retrieving--this processing has altered at least the form of the information, and probably the substance as well.

The fact that the computer has changed, selected, or evaluated data naturally does not make the resulting product inadmissible, but it does require another analytical step. The computer processing itself often creates a new meaning, adds new information--which is really the equivalent of an implicit statement. If an advocate wishes to introduce this processed product, he usually offers it for the truth of the conclusion it asserts. For example, when the telephone company compiles raw data into a phone bill for a subscriber, the bill is literally a statement: "The following long distance calls (and no others) were placed from your phone to these numbers on these days and times."

If the computer has created a hearsay statement by turning raw evidence into processed evidence, its proponent should be ready to show that the process is reliable. Computers process data in many different ways by running programs, which can be commercially or privately written. Any of these programs can contain logical errors, called "bugs," which could significantly affect the accuracy of the computer process. And even if there is no error in

the code, a technician may run the program in a way that creates a false result. For example, a particular computer search program may be "case sensitive," which means that the upper- and lower-case versions of any given letter are not interchangeable. If an author working in WordPerfect (a popular word~-processing program), searches a document for the word "Evidence," the computer will not find the word "evidence," because the letter "e" was not capitalized. What does it mean, then, when the computer reports that the word was "not found"? Under what circumstances should a computer's conclusion be admissible in court?

Consider a failure-to-file tax case. If a prosecutor asks the IRS to search its databanks to see whether a taxpayer filed a return in a particular year, the IRS may give her two very different products. If the taxpayer filed electronically, the IRS can produce either an original document from its computers (a printout of the filing) or an admissible duplicate in the form of an electronic copy. In that case, the IRS computers simply acted as storage cabinets to hold and reproduce the information that was entered by the taxpayer. Tax return in; tax return out.

But if, on the other hand, the IRS searches its databanks and finds

nothing, the IRS's negative report is clearly a hearsay statement which results from a computer process--the electronic search for the taxpayer's tax return. The hearsay rule (Fed. R. Evid. 803(10)) allows the absence of a public record to be shown by testimony "that diligent search failed to disclose the record ...." But testimony in what form? Will the negative computer report suffice, or should the technician who ran the search testify? Must the technician explain not only what keystrokes he entered to conduct the search, but also establish the error-free logic of the program he used? Must he know not only that the program searches for both lower- and upper-case versions of the taxpayer's name, but also exactly how it accomplishes that task? While the absence of a record is often admitted in evidence, prosecutors can expect that as attorneys become more computer-literate, defense counsel will raise new challenges in this area. Indeed, the accuracy or inaccuracy of the IRS's negative report rests on many different components, including the reliability (both human and technical) of the computer process.

Certainly, the mathematical validity of any program is a question of fact--a question which the opponent of a piece of processed evidence should have an opportunity at some point to explore and to contest. Similarly, the methods and safeguards involved in executing the program must also be fair ground for

[Page 122]

analysis and challenge. While it would clearly be both unnecessary and burdensome to prove every step of a computer process in every case, courts must also be ready to look behind these processes when the facts warrant. As lawyers and judges learn more about all the variables involved in creating evidence through computer processing, this area may become a new battleground for technical experts.

D. THE HEARSAY RULE

Most agents and prosecutors are familiar with the business records exception to the hearsay rule. Fed. R. Evid. 803(6). Generally speaking, any "memorandum, report, record, or data compilation" (1) made at or near the time of the event, (2) by, or from information transmitted by, a person with knowledge, is admissible if the record was kept in the course of a regularly conducted business activity, and it was the regular practice of that business activity to make the record.

A business computer's processing and re-arranging of digital information is often part of a company's overall practice of recording its regularly conducted activity. Information from telephone calls, bank transactions, and employee time sheets is regularly processed, as a fundamental part of

the business, into customer phone bills, bank account statements, and payroll checks. Logic argues that if the business relies on the accuracy of the computer process, the court probably can as well.

This is different, however, from using a company's raw data (collected and stored in the course of business, perhaps) and electronically processing it in a new or unusual way to create an exhibit for trial. For example, banks regularly process data to show each account-holder's transactions for the month, and most courts would readily accept that monthly statement as a qualifying business record. But may a court presume a similar regularity when the same bank runs a special data search for all checks paid from the account-holder's account over the past year to an account in Switzerland? In this case, even though the report was not made at or near the time of the event, the document is probably admissible as a summary under Fed. R. Evid. 1006. That rule allows courts to admit a "chart, summary, or calculation" as a substitute for "voluminous writing, recordings, or photographs." Nonetheless,

[Page 123]

other parties still have the right to examine and copy the unabridged original data, and to challenge the accuracy of the summary. Of course, this also opens the way to challenges of any computer process which created the summary.

In most other respects, of course, the hearsay rule operates with computer evidence exactly as it does with any other sort of evidence. For instance, statements for purposes of medical treatment, vital statistics, or statements against interest may all qualify as exceptions to the hearsay rule, whether they are oral, written, or electronic. Clearly, an electronic statement against interest must also be authenticated properly, but it does not fail as hearsay. Conversely, a correctly authenticated electronic message may contain all sorts of hearsay statements for which there are no exceptions.

The key is that computer evidence is no longer limited to business records, and the cases that carry that assumption are distinguishable when advocates work with other kinds of electronic evidence. But even with business records, a trial lawyer well versed in the technological world who knows how to ask the right questions may find that the "method or circumstances of preparation indicate lack of trustworthiness," under Fed. R. Evid. 803(6), to such a degree that a court will sustain, or at least consider, a challenge to the admissibility of the evidence. Computers and their products are not inherently reliable, and it is always wise to ask, in any particular case, what computers do and how they do it.

[no page 124] [Page 125]

IX. APPENDICES

APPENDIX A: SAMPLE COMPUTER LANGUAGE FOR SEARCH WARRANTS

IT IS ESSENTIAL to evaluate each case on its facts and craft the language of the warrant accordingly. Computer search warrants, even more than most others, are never one-size-fits-all products. The following paragraphs are a starting point for recurring situations, but may be adjusted in infinite ways. If you have any questions about tailoring an affidavit and warrant for your case, please call the Computer Crime Unit at 202-514-1026 for more suggestions.

Your affiant knows that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime, and/or (2) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security devices which are (1) instrumentalities, fruits, or evidence of crime, or (2) storage devices for information about crime.

1. Tangible Objects

a. Justify Seizing the Objects

Explain why, in this case, the tangible computer items are instrumentalities, fruits, or evidence of crime--independent of the information they may hold.

[Page 126]

Your affiant knows that [subject's] regional offices concertedly and systematically supplied various specialized computer programs to its individual local offices. These computer programs were designed to manipulate data in ways which would automatically add a few pennies to the amount billed to customers for each transaction. By using this specially designed program in its computers, the [subject] was able to commit a pervasive and significant fraud on all customers which would be very difficult for any one of them to detect.

* * * * * * *

or * * * * * * *

Your affiant knows that [subject] accessed computers without authority from his home by using computer hardware, software, related documentation, passwords, data security devices, and data, more specifically described as follows: [ ].

* * * * * * *

and

* * * * * * *

As described above, the [subject's] computer hardware, software, related documentation, passwords, data security devices, and data were integral tools of this crime and constitute the means of committing it. As such, they are instrumentalities and evidence of the violations designated. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them.

b. List and Describe the Objects

The tangible objects listed below may be named and seized as the objects of the search when they are, themselves, instrumentalities, fruits, or evidence of crime. Depending on the facts of the case, the list may be long or very

[Page 127]

short. The affidavit should describe the specific tangible objects with as much particularity as the facts allow. The following paragraphs are designed to be expansive and all-inclusive for those cases in which the government has probable cause to search and seize all computer hardware, software, documentation, and data security devices (including passwords) on site. However, most cases will call for a much more limited list

(1) Hardware

Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, memory typewriters, and self~-contained

"laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices), peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

(2) Software

Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating

[Page 128]

systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

(3) Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

(4) Passwords and Data Security Devices

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

2. Information: Records, Documents, Data

For clarity, most "information" warrants need one paragraph listing all the kinds of evidence they seek (content). Then they need a separate paragraph detailing all the various forms this evidence could take, so it is clear that all forms apply to all records. Most warrants will need another section (in appropriate cases) explaining why agents need to seize data storage devices for

[Page 129]

off-site searches. It may also be necessary to ask the magistrate for permission to take some peripheral hardware and software even though it does not directly contain evidence.

a. Describe the Content of Records, Documents, or other Information

If the object of the search is information which has been recorded in some fashion (including digital form), it is important to begin with the content of the record and not with its form. Depending on the case, the probable cause may be limited to one very specific document or extend to every record in a wholly criminal enterprise. Describe the content of the document with the same specificity and particularity as for paper records.

Based on the facts as recited above, your affiant has probable cause to believe the following records are located at [the suspect's] residence and contain evidence of the crimes described:

A letter dated July 31, 1991 from [the suspect] to his mother.

Tax records and all accompanying accounts, records, checks, receipts, statements, and related information for tax year 1991.

Lists of illegal or unauthorized access codes or passwords, including (but not limited to) telephone, credit card, and computer access codes.

All records relating to [the suspect's] drug trafficking, including (but not limited to) lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions; any information related to sources of narcotic drugs (including names, addresses, phone numbers, or any other identifying information); any information recording [the suspect's]

[Page 130]

schedule or travel from 1988 to present; all bank records, checks, credit card bills, account information, and other financial records.

b. Describe the Form which the Relevant Information May Take

If you know the records are stored on a computer or in some other digital form, you should limit the scope of the search to digital records. If you cannot determine in advance the form of the records (or if the records are in several different forms) the following language is a starting point. BUT BE SURE TO ELIMINATE ANYTHING WHICH DOES NOT APPLY TO YOUR CASE. Once again, because cases which have nothing else in common may all have digital evidence, the following list is extremely broad. For example, in child pornography or counterfeiting cases, the non-digital evidence may be photographs, films, or drawings. But in drug cases, tax cases, or computer crimes, the agents may not be searching for graphics or other pictures.

The terms "records," "documents," and "materials" include all of the foregoing items of evidence in whatever form and by whatever means such records, documents, or materials, their drafts, or their modifications may have been created or stored, including (but not limited to) any handmade form (such as writing, drawing, painting, with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs, or any information on an electronic or magnetic storage device, such as floppy diskettes, hard disks, backup tapes, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

[Page 131]

c. Electronic Mail: Searching and Seizing Data from a BBS Server under 18 U.S.C. 2703

In some situations, you may know or suspect that the target's computer is the server for an electronic bulletin board service (BBS). If you need to seize the computer, the data on it, or backups of the data, consider the applicability of 18 U.S.C. 2703. (See "STORED ELECTRONIC COMMUNICATIONS," supra p. 85.) If the statute applies and there is or may be qualifying e-mail on the computer, consider whether the government has probable cause to believe that all or any of it is evidence of crime.

Your affiant has probable cause to believe that [the suspect]'s computer operates, in part, as the server (or communications center) of an electronic bulletin board service ("BBS"). This BBS [appears to] provide[s] "electronic communication service" to other persons, and [may] contain[s] their "electronic communications," which may have been in "electronic storage" on [the suspect's] computer for less than 180 days (as those terms are defined in 18 U.S. C. 2510). The affiant is aware of the requirements of Title 18 U.S.C. 2703 describing law enforcement's obligations regarding electronic communications in temporary storage incident to transmission, as defined in that statute.

(1) If All the E-Mail is Evidence of Crime

If the whole BBS is dedicated to criminal enterprise (such as a specialty "porn board" or "pirate board"), the facts may support searching and seizing all the e-mail, including the electronic mail which qualifies under the statute.

[Your affiant, as an undercover subscriber and user of (the suspect's) BBS network, has learned that it is dedicated to exchanging illegal copies of computer software and stolen access codes among users. All users are asked to furnish pirated software products and active access codes (phone cards, credit cards, PBX codes, and computer passwords) in return for the privilege of illegally downloading from the BBS other illegal software or codes they may choose. Your affiant has used the electronic mail services of the BBS, and knows

that the subscribers use it primarily to share information about other sources of illegal software and about how to use stolen access codes and computer passwords. Thus, your affiant has probable cause to believe that any electronic mail residing on the system contains evidence of these illegal activities.]

(2) If Some of the E-Mail is Evidence of Crime

If you have probable cause to believe that there will be evidence of crime in the e-mail of some users and not others, the affidavit and warrant should distinguish and describe which will be searched and seized and which will not. In most cases like this, the government will be focusing on the electronic communications of the suspect/sysop's co-conspirators. The affidavit should identify the particular individuals, if possible (by name or "hacker handle"), so that data analysts will know which e-mail to search and which to leave unopened. In

some cases, the government may have probable cause to search e-mail from some "sub-boards" of the BBS, but not from others. In other cases, the magistrate may allow the government to run "string searches" of all the e-mail for certain specified key words or phrases. There are too many variations in these cases to draft useful models, but the wisest course is to address this issue in the affidavit and set out a search and seizure plan which the magistrate can approve. Please call the Computer Crime Unit (202-514~-1026) for more specific assistance.

(3) If None of the E-Mail is Evidence of Crime

In some cases. the suspect's criminal uses of his computer are quite separate from and coincidental to his using it as the server for a BBS. For example, a sysop who runs a legal bulletin board from his home may also use the same computer to store personal copies of child pornography, or records of his drug-dealing business, or a death-threat letter to the President of the United States. None of these criminal uses has anything to do with the legal (and perhaps statutorily protected) private electronic communications of his BBS subscribers--except for the fact that they reside on the same computer system.

[Page 133]

And even when this computer system clearly is an instrumentality of the suspect/sysop's crime, the government may be obliged to protect the unrelated, qualifying e-mail of innocent third parties and set it aside, unopened. In any event, the government should consider and address this issue with the magistrate and devise a plan which will work in the case at hand. Call the Computer Crime Unit for more help.

d. Ask Permission to Seize Storage Devices when an Off~-Site Search is Necessary

Based upon your affiant's knowledge, training and experience, and consultations with [NAME AND QUALIFICATIONS OF EXPERT], your affiant knows that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

1) The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine

all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

2) Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence

[Page 134]

and to recover even "hidden," erased, compressed, password~-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

e. Ask Permission to Seize, Use, and Return Auxiliary Items, as Necessary

In cases where you must seize hardware, software, documentation, and data security devices in order to search and seize the data for which you have probable cause, ask the magistrate's permission in the affidavit. The language which follows is general and will be most applicable to computers which are not part of an extensive network. Of course, if you have specific information in your case to support seizing auxiliary items (e.g., the computer hardware is rare; the operating system is custom-designed), cite those factors rather than using the general description which follows.

Based upon your affiant's knowledge, training and experience, and [NAME AND QUALIFICATIONS OF EXPERT], your affiant knows that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

The peripheral devices which allow users lo enter or retrieve data from the storage devices vary widely in their compatibility with other

hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re~configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and

[Page 135]

hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices.

If, after inspecting the l/O devices, software, documentation, and data security devices, the analyst determines that these items are no longer necessary to retrieve and preserve the data evidence, the government will return them within a reasonable time.

f. Data Analysis Techniques

Data analysts may use several different techniques to search electronic data for evidence or instrumentalities of crime. These include, but are not limited to the following: examining file directories and subdirectories for the lists of files they contain; "opening" or reading the first few "pages" of selected files to determine their contents; scanning for deleted or hidden data; searching for key words or phrases ("string searches").

3. Stipulation for Returning Original Electronic Data

In some cases, you may want to return data storage devices which contain original electronic evidence to the suspect and keep "bit-stream" or "mirror-image" copies for processing and for use at trial. For example, the suspect may be a large business which employs many innocent people and which needs its computers and data in order to run the business and pay the employees. If you do wish to return the equipment and data before trial, consider using some version of the following stipulation to avoid evidentiary issues. Of course, whether the copies are, indeed, "exact" copies is a question of fact, and the defense will have to satisfy itself that the government's copying process was accurate. But if, after exploring the issue, the defense refuses to

[Page 136]

sign a stipulation and cannot be satisfied about the reliability of the

duplicates, you will probably need to keep the originals. (See "Returning Seized Computers and Materials," supra p. 105, and "EVIDENCE," supra p. 113.) (For a form stipulation, see p. 137.)

[Page 137]

UNITED STATES DISTRICT COURT

In the Matter of the Search of ____

STIPULATION OF THE PARTIES.

It is hereby stipulated and agreed between ____ and ____ as an individual and as an agent for ____ that:

(1) the electronic information contained on the [Bernoulli 90-MB disk, number ____] is a complete, exact, and accurate duplicate of the electronic information contained on [the hard drive of an IBM personal computer, serial number ____] [the hard drive of a personal computer identified as "Fred's" by an evidence tag attached to the top of the CPU cover, said personal computer bearing no serial number or other identifying information] [a floppy disk marked with an evidence sticker as "item number ____, and bearing the initials "_ _ _"]; which computers/floppy disk were/was seized from ____ on ____, 199_, by agents of the ____.

(2) the electronic information contained on the [Bernoulli 90-MB disk, number ____] accurately reproduces the original data described above as of____, 199_.

Assistant U.S. Attorney Defendant

Agency Attorney

[No page 138] [Page 139]

APPENDIX B: GLOSSARY14

BBS -- See "Electronic Bulletin Board Systems."

CD ROM -- CD ROM stands for Compact Disk Read-Only Memory. CD ROMs store and read massive amounts of information on a removable disk platter or solid state storage chip. Unlike the data on hard drives and diskettes, data on CD ROMs can only be read--not altered--by the user. Also called "firmware."

CPU-- The central processing unit.

DATA -- "A formalized representation of facts or concepts suitable for communication, interpretation, or processing by people or automated means." The term "data" is often used to refer to the information stored in the computer.

DOCUMENTATION -- Documents that describe technical specifications for computer-related products and how to use hardware components and/or software applications.

ELECTRONIC BULLETIN BOARD SYSTEMS (BBS) -- A bulletin board system is a computer dedicated, in whole or in part, to serving as an electronic meeting place. A BBS computer system may contain information, programs, and e-mail, and is set up so that users can dial the bulletin board system, read and leave messages for other users, and download and upload software programs for common use. A BBS can have multiple telephone lines (so that many people can use it at the same time) or a single line where a user's access is first-come, first-served. BBSs can have several levels of access, sometimes called "sub-boards" or "conferences." Access to the different conferences is controlled by the system operator with a password system. A single user may have several different passwords, one for each different level or conference. A user may store documents, data, programs, messages, and even photographs in the different levels of the BBS. A bulletin board system may be located anywhere telephone lines go.

14 All quotations in this Glossary are taken from Webster's Dictionary of Computer Terms (3d ed. 1988).

ELECTRONIC MAIL -- Electronic mail provides for the transmission of messages and files between computers over a communications network. Sending information in this way is similar in some ways to mailing a letter through the postal service. The messages are sent from one computer through a network server to the electronic address of another specific computer or to a series of computers of the sender's choice. The transmitted messages (and attached files) are either stored at the computer of the addressee (such as someone's personal computer) or at the mail server (a machine dedicated, at least in part, to storing mail), and will remain there until the addressee retrieves the mail from the server. When people "pick up" e-mail from the mail server, they usually receive only a copy of their mail, and the stored message is maintained in the mail server until the addressee deletes it. (Some systems allow senders to delete mail on the server before delivery.) Of course, deleted mail may sometimes be recovered by "undeleting" the message (if not yet

overwritten) or by obtaining a backup copy (if the server was backed up before the message was deleted).

FAX PERIPHERAL -- A device, normally inserted as an internal card, that allows the computer to function as a fax machine. (An abbreviation of "facsimile.")

FILE SERVER -- A file server is a computer on a network that stores the programs and data files shared by the users of the network. A file server is the nerve center of the network, and also acts as a remote disk drive, enabling users to store information. It can be physically located in another judicial district from the suspect's machine.

FLOPPY DISK DRIVE -- A drive that reads from or writes to separate diskettes which the user inserts. Information is stored on the diskettes themselves, not on the drive.

HARD DISK DRIVE -- A storage device based on a fixed, permanently mounted disk drive. It may be either internal (part of the computer itself) or external (a separate but connected component). Both applications and data may be stored on the disk.

HARDWARE -- "The physical components or equipment that make up a computer system..." Examples include keyboards, monitors, and printers.

[Page 141]

INPUT/OUTPUT DEVICE -- A piece of equipment which sends data to, or receives data from, a computer. Keyboards, monitors, and printers are all common I/O devices.

LASER DISK -- Similar to a CD ROM drive but uses lasers to read and sometimes write information.

MODEM -- A device ("modulate/demodulate") which allows one computer to communicate with another computer, normally over standard telephone lines. It converts the computer's digital information to analogue signals for outgoing telephone transmission, and reverses the conversion for incoming messages. Modems may be either part of (internal) or external to the computer.

MOUSE -- A pointing device that controls input by moving a cursor or other figure on the screen. Normally, the user points to an object on the screen and then presses a button on the mouse to indicate her selection.

NETWORK -- "A system of interconnected computer systems and terminals."

PRINTER -- A number of technologies exist, using various techniques. The most common types of computer printers are:

1. Band - a rotating metal band is impacted as it spins;

2. Daisy wheel - a small print wheel containing the form of each character rotates and hits the paper, character by character;

3. Dot matrix - characters and graphics are created by pins hitting the ribbon and paper;

4. Ink jet - injects (sprays) ink onto the paper;

5. Laser - electrostatically charges the printed page and applies toner;

6. Plotter - moves ink pens over the paper surface, typically used for large engineering and architectural drawings.

7. Thermal - a hot printer head contacts special paper that reacts to heat.

[Page 142]

SCANNER -- Any optical device which can recognize characters on paper and, using specialized software, convert them into digital form.

SERVER -- See "File Server."

SOFTWARE -- "The programs or instructions that tell a computer what to do." This includes operating system programs which control the basic functions of the computer system (such as Microsoft's Disk Operating System--"MS-DOS"--that controls IBM-compatible PCs) and applications programs which enable the computer to produce useful work (e.g., a word processing program such as WordPerfect).

SYSOP -- See "System Administrator."

SYSTEM ADMINISTRATOR -- The individual responsible for assuring that the computer network is functioning properly. He is often responsible for computer security as well.

SYSTEM OPERATOR -- See "System Administrator."

VOICE-MAIL SYSTEMS -- A voice-mail system is a complex phone answering machine (run by a computer) which allows individuals to send and receive

telephone voice messages to a specific "mailbox" number. A person can call the voice-mail system (often a 1-800 number) and leave a message in a particular person's mailbox, retrieve messages left by other people, or transfer one message to many different mailboxes in a list. Usually, anyone can leave messages, but it takes a password to pick them up or change the initial greeting. The system turns the user's voice into digital information and stores it until the addressee erases it or another message overwrites it. Criminals sometimes use voice mailboxes (especially, if they can beat the password, those of unsuspecting people) as remote deaddrops for information that may be valuable in a criminal case. The server for the voice mailboxes is usually located in the message system computer of the commercial vendor which supplies the voice-mail service. Sometimes it can be found on the customer~-organization's computer server at the location called. Voice mail messages can be written on magnetic disk or remain in the computer's memory, depending on the vendor's system.

[No page 142] [Page 143]

APPENDIX C: FEDERAL EXPERTS FOR COMPUTER CRIME INVESTIGATIONS

The following is a list of some federal resources in alphabetical order:

1. Bureau of Alcohol, Tobacco, and Firearms Forensic Science Laboratory 1401 Research Blvd. Rockville, MD 20850 301-217-5717

2. Drug Enforcement Administration Chief, Technical Operations Section 8199 Backlick Road Lorton, VA 20079 703-557-8250

3. Federal Bureau of Investigation Computer Crime Squad Washington Metropolitan Field Office 7799 Leesburg Pike Suite 200, South Tower Falls Church, VA 22043 202-324-9164

4. Federal Bureau of Investigation Laboratory Division 9th and Pennsylvania Ave., N.W. Washington, DC 20535 202-324-3000

5. Internal Revenue Service SCER Program Coordinator Criminal Investigation Division CI:R:I Room 2246 1111 Constitution Ave., N.W. Washington, DC 20224 202-535-9130

[Page 144]

United States Air Force Computer Crime Division Office of Special Investigations HQ AFOSI/IVSC Bolling Air Force Base Washington, DC 20332-6001 202-767-5847

United States Secret Service Electronic Crimes Branch 1310 L Street, N.W. Washington, DC 20005 202-435-7700

[Page 145]

APPENDIX D:

COMPUTER SEARCH AND SEIZURE WORKING GROUP

The following agencies and individuals contributed to these guidelines.
* Designates those no longer in government service.

United States Department of Defense

United States Air Force

Computer Crime Division Office of Special Investigations HQ AFOSI/IVSC Bolling AFB Washington, DC 20332-6001 202-767-5847

Jim Christy, Chief

United States Department of Justice

Criminal Division

Kevin Di Gregory, Deputy Assistant Attorney General

Robert Litt, Deputy Assistant Attorney General

[Page 146] General Litigation and Legal Advice Section 1001 G Street, N.W., Suite 200 Washington, DC 20001 202-514-1026

Mary C. Spearing, Chief Scott Charney, Chief, Computer Crime Unit Martha Stansell-Gamm, Working Group Chair Laura Blumenfeld William D. Braun William C. Brown Elena Duarte Gerald Grzenda Annette Long Stevan Mitchell Michael J. Rhim Daniel Schneider Joshua Silverman Phillip Talbert * Peter Toren George Toscas Candice Will Paula Wolff

Office of Professional Development and Training 1001 G Street, N.W., Suite 250 Washington, DC 20001 202-514-1323

Debra Crawford

[Page 147]

Drug Enforcement Administration

Criminal Law Section Office of the Chief Counsel 700 Army Navy Drive, West Bldg. Arlington, VA 22202 202-307-8014

Greg Mitchell

Federal Bureau of Investigation

Computer Analysis and Response Team Laboratory Division, Room 3218 9th and Pennsylvania Ave., N.W. Washington, DC 20535 202-324-2104

Steve McFall, Chief Mike Noblett

Computer Crime Squad Washington Metropolitan Field Office 7799 Leesburg Pike Suite 200, South Tower Falls Church, VA 22043 202-324-9164

James Settle, Chief *

[Page 148]

Tax Division

Criminal Law Section Main Justice Bldg., Room 4625 10th and Constitution Ave., N.W. Washington, DC 20530 202-514-2832

Tony Whitledge

United States Attorneys Offices

Northern District of California 450 Golden Gate Ave., 11th Floor Box 36055 San Francisco, CA 94102 415-556-4229

Robert K. Crowe

Southern District of California 940 Front St., Room 5-N-I9 San Diego, CA 92189-0150 619-557-6962

Mitchell D. Dembin

Northern District of Georgia Richard Russell Bldg., Room 1800 75 Spring Street Atlanta, GA 30335 404-331-6954

Kent Alexander, United States Attorney Randy Chartash

[Page 149]

Southern District of New York One St. Andrews Plaza New York, NY 10007 212-791-0055

Steve Fishbein *

Eastern District of Virginia 600 E. Main St., Suite 1800 Richmond, VA 23219 804-771-2186

Win Grant

United States Department of the Treasury

Bureau of Alcohol, Tobacco, and Firearms

Forensic Science Laboratory 1401 Research Blvd. Rockville, MD 20850 301-217-5717

John Minsek

Systems Operation/Software Engineering Support Branches 650 Massachusetts Ave., N.W., Room 6004 Washington, DC 20226 202-927-6095

Dan Lofton Michael Park

[Page 150]

Internal Revenue Service

Criminal Investigation Division 1111 Constitution Ave., N.W., Room 2246 Washington, DC 20224 202-535-9130

Timothy Whitley, Senior Analyst

Criminal Investigation Training Federal Law Enforcement Training Center Building 69, Third Floor Glynco, GA 31524 912-267-2378

Dan Duncan, Attorney Chuck Rehling, Special Agent

Seized Computer & Evidence Recovery Specialists Computer Investigative Specialists 515 N. Sam Houston Pkwy., East Mail Stop 9123 NW Houston, TX 77060 713-878-5897

Ken Scales, Special Agent

United States Customs Service

Office of Investigative Programs Special Investigations Division 1301 Constitution Ave., N.W., Room 6130 Washington, DC 20229 202-377-9283

John Seither, Senior Special Agent

[Page 151]

United States Secret Service

Electronic Crimes Branch Financial Crimes Division 1310 L Street, N.W., Room 200 Washington, DC 20005 202-435-7700

Jack Lewis Tom Moyle

[No page 152] [Page 153]

APPENDIX E: STATUTORY POPULAR NAME TABLE

Access Device Fraud Statute .... 18 U.S.C. 1029
Computer Fraud and Abuse Act ..... 18 U.S.C. 1030
No-Knock Statute .... 18 U.S.C. 3109
Privacy Protection Act ..... 42 U.S.C. 2000aa
Stored Communications Access ..... 18 U.S.C. 2701, et seq.
Wiretap Statute ("Title III") ..... 18 U.S.C. 2510, et seq.

[No page 154] [Page 155]

APPENDIX F: TABLE OF AUTHORITIES

Cases [number following case is page number on which case is cited]

Abel v. United States, 362 U.S. 217 (1960) 36

Aguilar v. Texas, 378 U.S. 108 (1964) 27

Andresen v. Maryland, 427 U.S. 463 (1976) 30, 37, 38

Application of Commercial Inv. Co., 305 F. Supp. 967 (S.D.N.Y. 1969) 37

Blair v. United States, 665 F.2d 500 (4th Cir. 1981) 11

Blinder. Robinson & Co. v. United States, 897 F.2d 1549, 46 CrL 1537 (10th Cir. 1990) 107

DeMassa v. Nunez, 747 F.2d 1283 (9th Cir. 1984) 43

Donovan v. A.A. Beiro Construction Co., Inc., 746 F.2d 894 (D.C. Cir. 1984) 21

Floyd v. United States, 860 F.2d 999 (1Oth Cir. 1988) 106

Frazier v. Cupp, 394 U.S. 731 (1969) 15

Horton v. California, 496 U.S. 128, 47 CrL 2135 (1990) 9

Illinois v. Rodriguez, 497 U.S. 177, 47 CrL 2177 (1990) 16, 17

In Re Grand Jury Subpoena Duces Tecum Dated November 15, 1993, 846 F. Supp. 11, 54 CrL 1506 (S.D.N.Y. 1994) 98

In Re Grand Jury Subpoenas, 926 F.2d 847 (9th Cir. 1991) 53

In Re Southeastern Equipment Co. Search Warrant, 746 F. Supp.1563 (S.D. Ga. 1990) 105

Klitzman v. Krut, 744 F.2d 955 (3d Cir. 1984) 40

Lafayette Academy, Inc., Application of, 610 F.2d 1 (1st Cir. 1979) 53, 98

Lambert v. Polk County, Iowa, 723 F. Supp. 128 (S.D. Iowa 1989) 80

Marron v. United States, 275 U.S. 192 (1927) 37

Marvin v. United States, 732 F.2d 669 (8th Cir. 1984) 58

Matter of Search of Kitty's East, 905 F.2d 1367 (10th Cir. 1990) 106. 107

Mincey v. Arizona, 437 U.S. 385 (1978) 10

Minneapolis Star & Tribune Co. v. United States, 713 F. Supp. 1308 (D. Minn. 1989) 80

National City Trading Corp. v. United States, 635 F.2d 1020 (2d Cir. 1980) 83

National Federation of Federal Employees v. Weinberger, 818 F.2d 935 (D.C. Cir. 1987) 19

Naugle v. Witney, 755 F. Supp. 1504 (D. Utah 1990) 58

O'Connor v. Ortega, 480 U.S. 709 (1987) 18, 19, 21

Pell v. Procunier, 417 U.S. 817 (1974) 71

Pleasant v. Lovell, 876 F.2d 787 (10th Cir. 1989) 24

Schneckloth v. Bustamonte, 412 U.S. 218 (1973) 12, 13

Securities and Exchange Commission v. McGoff, 647 F.2d 185 (D.C. Cir.), cert. denied, 452 U.S. 963 (1981) 71

Steele v. United States, 267 U.S. 498 (1925) 96

Steve Jackson Games. Inc. v. U.S. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), appeal filed on other grounds, (Sept. 17, 1993) 82, 83, 88

Texas v. Brown, 460 U.S. 730 (1983) 11

United States Postal Service v. C.E.C. Services, 869 F.2d 184 (2d Cir. 1989) 56

United States v. Agrusa, 541 F.2d 690 (8th Cir. 1976) cert. denied, 429 U.S. 1045 (1977) 101

United States v. Aguilar, 883 F.2d 662 (9th Cir. 1989), cert. denied, 498 U.S. 1046 (1991) 24

United States v. Arias, 923 F.2d 1387 (9th Cir.), cert. denied, 112 S. Ct. 130 (1991) 10

United States v. Barrett, 725 F. Supp. 9 (D.D.C. 1989) 100

United States v. Bentley, 825 F.2d 1104 (7th Cir.), cert. denied, 484 U.S. 901 (1987) 56, 58, 98

United States v. Beusch, 596 F.2d 871 (9th Cir. 1979) 58

United States v. Bilanzich, 771 F.2d 292 (7th Cir. 1985) 20

United States v. Block, 590 F.2d 535 (4th Cir. 1978) 15, 18

United States v. Blok, 188 F.2d 1019 (D.C. Cir. 1951) 21

United States v. Boyette, 299 F.2d 92 (4th Cir.), cert. denied, 369 U.S. 844 (1962) 28

United States v. Brown, 556 F.2d 304 (5th Cir. 1977) 100

United States v. Bustamante-Gamez, 488 F.2d 4 (9th Cir. 1973), cert. denied, 416 U.S. 970 (1974) 100

United States v. Caballos, 812 F.2d 42 (2d Cir. 1987) 13

United States v. Carter, 566 F.2d 1265 (5th Cir. 1978), cert. denied, 436 U.S. 956 (1978) 102

United States v. Darensbourg, 520 F.2d 985 (5th Cir. 1975) 96

United States v. David, 756 F. Supp. 1385 (D. Nev. 1991) 9, 11, 14, 54

United States v. Duran, 957 F.2d 499, 51 CrL 1009 (7th Cir. 1992) 17

United States v. Fawole, 785 F.2d 1141 (4th Cir. 1986) 59

United States v. Francis, 646 F.2d 251 (6th Cir.), cert. denied, 454 U.S. 1082 (1981) 101

United States v. Gargiso, 456 F.2d 584 (2d Cir. 1972) 20

United States v. Griffin, 530 F.2d 739 (7th Cir. 1976) 13

United States v. Henson, 848 F.2d 1374 (6th Cir. 1988), cert. denied, 488 U.S. 1005 (1989) 57

United States v. Hillyard, 677 F.2d 1336 (9th Cir. 1982) 84

United States v. Houle, 603 F.2d 1297 (8th Cir. 1979) 11

United States v. Johns, 948 F.2d 599, 50 CrL 1224 (9th Cir. 1991), cert. denied, 112 S. Ct. 3046 (1992) 35

United States v. Judd, 687 F. Supp. 1052 (N.D. Miss. 1988), aff'd 889 F.2d 1410 (5th Cir. 1989), cert. denied, 494 U.S. 1036 (1989) 93

United States v. Korman, 614 F.2d 541 (6th Cir.), cert denied, 446 U.S. 952 (1980) 39

United States v. Lefkowitz, 285 U.S. 452 (1932) 37

United States v. Leon, 468 U.S. 897 (1984) 9

United States v. Lindenfield, 142 F.2d 829 (2d Cir.), cert. denied, 323 U.S. 761 (1944) 38

United States v. Long, 524 F.2d 660 (9th Cir. 1975) 15

United States v. Lucas, 932 F.2d 1210, 49 CrL 1138 (8th Cir.), cert. denied, 112 S. Ct. 399 (1991) 53

United States v. Markis, 352 F.2d 860 (2d Cir. 1965), vacated without opinion, 387 U.S. 425 (1967) 28

United States v. Matlock, 415 U.S. 164 (1974) 14, 16, 17

United States v. Mendenhall, 446 U.S. 544 (1980) 13

United States v. Milan-Rodriguez, 759 F.2d 1558 (11th Cir.), cert. denied, 474 U.S. 845 (1985), and cert. denied, 486 U.S. 1054 (1988) 12

United States v. Murrie, 534 F.2d 695 (6th Cir. 1976) 100

United States v. Musson, 650 F. Supp. 525 (D. Colo. 1986) 53

United States v. Patino, 830 F.2d 1413 (7th Cir. 1987), cert. denied, 490 U.S. 1069 (1989) 11

United States v. Price, 599 F.2d 494 (2nd Cir. 1979) 13

United States v. Prout, 526 F.2d 380 (5th Cir.), cert. denied, 429 U.S. 840 (1976) 94

United States v. Ramsey, 431 U.S. 606 (1977), cert. denied, 434 U.S. 1062 (1978) 12

United States v. Reed, 935 F.2d 641 (4th Cir.), cert. denied, 112 S. Ct. 423 (1991) 10

United States v. Remigio, 767 F.2d 730 (1Oth Cir.), cert. denied, 474 U.S. 1009 (1985) 100

United States v. Reyes, 798 F.2d 380 (1Oth Cir. 1986) 53

United States v. Robinson, 287 F. Supp. 245 (N.D. Ind. 1968) 29

United States v. Rodriguez, 968 F.2d 130, 51 CrL 1097 (2d Cir.), cert. denied, 113 S. Ct. 140 (1992) 94

United States v. Ruminer, 786 F.2d 381 (10th Cir. 1986) 101

United States v. Santarelli, 778 F.2d 609 (11th Cir. 1985) 60

United States v. Santarsiero, 566 F. Supp. 536 (S.D.N.Y. 1983) 27, 39

United States v. Sawyer, 799 F.2d 1494 (11th Cir. 1986), cert. denied sub nom. Leavitt v. United States, 479 U.S. 1069 (1987) 56

United States v. Scheer, 600 F.2d 5 (3d Cir. 1979) 12

United States v. Scott, 578 F.2d 1186 (6th Cir.), cert. denied, 439 U.S. 870 (1978) 13

United States v. Sealey, 830 F.2d 1028 (9th Cir. 1987) 16

United States v. Sinclair, 742 F. Supp. 688 (D.D.C. 1990) 101

United States v. Sklaroff, 323 F. Supp. 296 (S.D. Fla. 1971) 96

United States v. Snow, 919 F.2d 1458 (1Oth Cir. 1990) 57

United States v. Stern, 225 F. Supp. 187 (S.D.N.Y. 1964) 28, 29, 38

United States v. Stewart, 867 F.2d 581 (1Oth Cir. 1989) 102

United States v. Taft, 769 F. Supp. 1295 (D. Vt. 1991) 108

United States v. Talkington, 875 F.2d 591 (7th Cir. 1989) 9

United States v. Tamura, 694 F.2d 591 (9th Cir. 1982) 58, 60, 100

United States v. Tropp, 725 F. Supp. 482 (D. Wyo. 1989) 84

United States v. Truitt, 521 F.2d 1174 (6th Cir. 1975) 27, 30

United States v. Turk, 526 F.2d 654 (5th Cir.), cert. denied, 429 U.S. 823 (1976) 11

United States v. Valenzuela, 596 F.2d 824 (9th Cir.), cert. denied, 441 U.S. 965 (1979) 100

United States v. Viera, 569 F. Supp. 1419 (S.D.N.Y. 1983) 28

United States v. Villegas, 899 F.2d 1324, 47 CrL 1041 (2d Cir.), cert. denied, 498 U.S. 991 (1990) 35, 36

United States v. Whitten, 706 F.2d 1000 (9th Cir. 1983), cert. denied,

465 U.S. 1100 (1984) 39

United States v. Wuagneux, 683 F.2d 1343 (11th Cir. 1982), cert. denied,
464 U.S. 814 (1983) 58

United States v. Wysong, 528 F.2d 345 (9th Cir. 1976) 102

Vaughn v. Baldwin, 950 F.2d 331 (6th Cir. 1991) 13

Voss v. Bergsgaard, 774 F.2d 402 (1Oth Cir. 1985) 53

Warden v. Hayden, 387 U.S. 294 (1967) 26, 28, 29, 37

Yancey v. Jenkins, 638 F. Supp. 340 (N.D. Ill. 1986)27

Zurcher v. Stanford Daily, 436 U.S. 547 (1978) 72, 76

Statutes

18 U.S.C. 1029 36, 77

18 U.S.C. 1030 36, 77

18 U.S.C. 2510 86, 131

18 U.S.C. 2701, et seq. 56, 71

18 U.S.C. 2702 23, 50, 85

18 U.S.C. 2703 85-88, 131

18 U.S.C. 2711 85

18 U.S.C. 3109 100

26 U.S.C. 6103 66

42 U.S.C. 2000aa 41, 42, 56, 72-75, 77-80, 82-84

Federal Rules

124 F.R.D. 428 107

Fed. R. Crim. P. 41 1, 26-28, 30, 35-37, 86-89, 92-96, 105-110, 125, 126

Fed. R. Evid. 16 69

Fed. R. Evid. 501 41

Fed. R. Evid. 803(6) 113, 122, 123

Fed. R. Evid. 803(10) 121

Fed. R. Evid. 901 115, 116, 119

Fed. R. Evid. 1001 108, 114, 115, 120

Fed. R. Evid. 1002 114

Fed. R. Evid . 1003 115

Fed. R. Evid. 1006 122

Federal Regulations

28 C.F.R. 50.10 73

28 C.F.R. 59.1-.6 30, 41

Legislative History

H.R. Rep. No. 647, 99th Cong., 2d Sess. 87

H.R. Rep. No. 1064, 96th Cong., 2d Sess. 76, 79

S. Rep. No. 874, 96th Cong., 2d Sess. 73, 75, 76, 78

Testimony of Richard J. Williams, Vice President, National District Attorney's Association, in Hearing before the Committee on the Judiciary, United States Senate, 96th Cong., 2d Sess. on S. 115, S. 1790, and S. 1816 (Mar. 28, 1980) Serial No. 96-59, at 152-3 76

Reference Materials

Rose, Steve Jackson Games Decision Stops the Insanity, Boardwatch, May 1993 83

The American Heritage Dictionary, (2d ed. 1983) 92

W. LaFave, Search and Seizure: A Treatise on the Fourth Amendment (2d ed. 1987) 15, 17

Webster's Dictionary of Computer Terms (3d ed. 1988) 2, 139

Wright & Miller, Federal Practice and Procedure: Criminal 2d (1982) 29
.