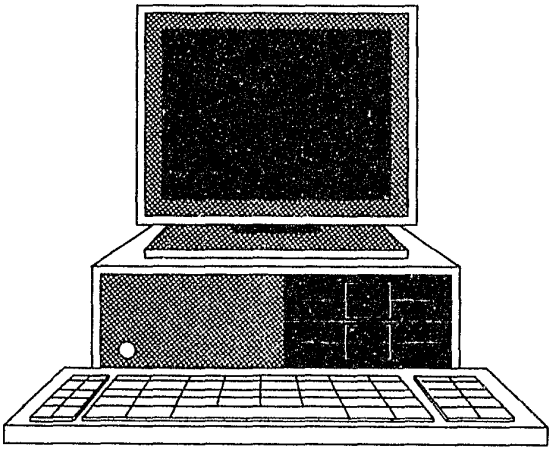
U.S. Department of Justice
Justice Management Division

Basic Considerations in Investigating and Proving Computer-Related Federal Crimes



November 1988

PROLOGUE

After hearing the evidence in this case the first finding the court is constrained to make is that, in the computer age, lawyers and courts need no longer feel ashamed or even sensitive about the charge, often made, that they confuse the issue by resort to legal "jargon," law Latin or Norman French. By comparison, the misnomers and industrial shorthand of the computer world make the most esoteric legal writing seem as clear and lucid as the Gettysburg Address; and add to this Babel, the experts in the computer field, while using exactly the same words, uniformly disagree as to precisely what they mean. ... Honeywell, Inc. v. Lithonia Lighting, Inc., 317 F.Supp 406 (N.D.Ga. 1970)

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

PREFACE

Nationwide, there are millions of employees in computer-related jobs, and our financial systems and processes have become inextricably dependent on computers for managing and disbursing billions of dollars. All this, coupled with the millions of personal computers (PC's) used in private business and in the home, set the stage for concern over the potential for an explosive increase in computer-related crime.

According to an American Bar Association survey, */ the most significant types of computer crimes **/ are use of a computer to:

1) steal tangible or intangible assets;

2) destroy or alter data;

3) embezzle funds;

4) destroy or alter software;

5) defraud consumers, investors or users; and

6) steal computer software (not necessarily through use of a computer).

This same survey indicated that 25% of the respondents had a "known and verifiable" loss per respondent due to computer crime experienced during the preceding twelve month period ranging from approximately $2 million to over $10 million. ***/ This led the survey task force to conclude that:

---

*/ Task Force on Computer Crime, Section of Criminal Justice, American Bar Association, Report on Computer Crime, at p. 10 (1984).

**/ The terms "computer crime" and "computer-related crime" are used interchangeably to mean a crime in which a computer is somehow involved.

***/ The survey questionnaire was distributed to 1,000 organizations of which 275 responded, including Fortune 500 companies, banks, insurance companies, financial services/brokerage firms, accounting firms, computer/electronics firms, major Federal agencies, state Attorneys General, a sample of district attorneys and several trade associations.

> [a]t the very least, the results of the survey support the proposition that the annual losses sustained by American business and government organizations as the result of computer crime are, by any measure, huge. If the annual losses attributable to computer crime sustained by the relatively small survey group are, conservatively estimated, in the range of half a billion dollars, then it takes little imagination to realize the magnitude of the annual losses sustained on a nationwide basis. */

The would-be perpetrator will find greater opportunity to enlarge these estimates with the ever-increasing dependence of corporations and government agencies on computers for conducting their business.

Considering the ease of altering codes or patterns represented by electronic impulses or magnetic fields, investigating and proving a crime involving computer-related evidence may require taking unfamiliar extraordinary precautions in gathering, preserving and preparing such evidence and its source for trial. To assist Federal prosecutors and investigators in this relatively new area of criminal activity, this monograph was developed by the Justice Management Division's Systems Policy Staff at the request of the United States Attorney for the District of Columbia. It essentially expands on an earlier monograph **/ - providing a comprehensive text that covers the basic technical and legal considerations involved in dealing with a computer-related criminal case.

Both monographs were written by George S. Kondos and reviewed by David F. Geneson of the Office of the U.S. Attorney for the District of Columbia, Special Prosecutions Section. The present monograph was also reviewed by Kenneth M. Frankel, Trial Attorney with the Antitrust Division, Litigation II Section. Some of the topics covered in the present monograph were suggested by Mr. Geneson, and material under two of these topics was taken from notes provided by him based on his ongoing lectures to law enforcement personnel dealing with prosecution of computer-related crimes. (Mr. Geneson's contributions are indicated by footnote citations.)

---

*/ Id., at p.15.

**/ Computer-Related Evidence in Federal Criminal Cases, developed at the request of the Criminal Division's Fraud Section. Available on JURIS as a Criminal Division monograph and incorporated herein virtually in its entirety.

The chapter entitled Making the Case (including Appendix C: How to Process Computer Evidence) consists primarily of material contributed by Paul A. Boedges, Chief of the Computer Crime Division, Air Force Office of Special Investigations, and his Assistant Chief, Jim Christy. This chapter is in essence a manual on how to investigate computer-related crimes and was extensively edited and added to by the Federal Computer Investigations Committee and Gail Thackeray, Assistant Attorney General, Office of the Attorney General for the State of Arizona.

The monograph consists of five chapters: Chapter I, Uniqueness of Computer Crimes, is intended to provide prosecutors and investigators with an understanding of the nature and unique aspects of computer-related crimes, while Chapter II, Perpetrator Techniques, describes common techniques employed in such crimes. Chapter III, Problems of Proof, (along with parts of Chapter IV) addresses problems that prosecutors are apt to encounter because of the particular nature of computer crime cases. Chapter IV, Computer-Related Evidence Law, represents a legal brief on how the Federal courts have ruled on computer-related evidence matters. Chapter V, Making the Case, provides detailed guidance for investigators in gathering, handling and processing computer-related evidence.

Comprehensive legal analysis of a given topic is applied only in Chapter IV, and is limited to the extent necessary to discuss the law in that area in relation to computer-related evidence. Because of the paucity of Federal cases involving computer-related crime that have gone to trial and appeal, there is heavy dependence in discussing evidence issues on analogous fact situations in citing authority. Over 130 cases are cited.

Only computer crimes that pose difficulty in proof because of peculiarities of the technology are addressed, such as theft or destruction of information contained in computer equipment, unauthorized access to such information in storage or transmission, or use of a computer as the instrumentality of a crime. Hence, excluded from the purview of the manual are crimes where theft or destruction of computer equipment is the sole computer-related criminal charge, since such crimes pose problems of proof essentially no different than cases of theft or destruction of property in general.

CONTENTS

CHAPTER I: UNIQUENESS OF COMPUTER CRIMES

1. HIDDEN CRIMINALITY

> When a violent or other common crime is committed, the offender will normally give very careful consideration to shielding his identity. He will act in the dark, wear a mask, perhaps even kill to prevent the survival of a witness who can point him out in a lineup. Concealing the crime itself is often a secondary consideration.
>
> For the computer crime perpetrator, concealment of the crime from the victim as well as from law enforcement agencies is always a priority objective. Concealment is especially important because the perpetrator operates in the open. He cannot obtain victim cooperation by wearing a mask. The ideal crime from the point of view of the perpetrator is one that will never be recognized as a crime or wrongful act. */

Various techniques have been employed that underscore the surreptitious nature of most computer crimes. These techniques have come to be identified by imaginative descriptive labels such as "trojan horse," "salami" and "superzapping." (Descriptions of these and other commonly used techniques are presented in a later chapter.) They employ schemes that may seem ingenious to the layman, but they are for the most part nothing more than variations on programming macros or utilities familiar to the accomplished computer programmer (particularly one that codes in assembly or machine language). In some cases, they are simply obvious ways to effect an unauthorized or fraudulent act where knowledge of computer programming is not needed, or where involvement of a computer is passive.

For example, in the notorious Rifkin case, **/ $10.2 million was stolen from a bank by an outside technician brought in to create a back-up system for the wire room that controlled the bank's electronic fund transfers. Through knowledge gained by working on the back-up system, and by copying an authorization

---

*/ Somers, Economic Crimes, Investigative Principles and Techniques, at p. 127 (1984).

**/ United States v. Rifkin, CR No.78-1050(A)-WMB (C.D.Calif. 1978).

code symbol from a slip of paper on the wall of the wire room, Rifkin was able to: 1) go to a pay phone; 2) call the wire transfer room; 3) identify himself as an officer of the bank; 4) request that $10.2 million be transferred to an account in another bank; and 5) subsequently have the funds transferred to a Swiss bank for purchase of diamonds. Computers were only nominal instruments of the crime, since the illegal electronic fund transfer was accomplished by initiating a wire transfer action through a phone call. There were no "trojan horse" or "salami" computer instructions involved - just knowledge of the bank's authorized electronic fund transfer procedures. */

Rifkin's bold enterprise was discovered only after persons in whom he had confided notified the FBI. Presumably, the bank would have eventually been alerted to the missing funds, but tracing the loss to Rifkin might have been another matter without the tip-off, considering that the funds ended up in a Swiss bank account.

The undiscovered crime naturally goes unreported. However, even those known to the victim or a witness are unreported for a variety of reasons (e.g., embarassment, fear of retaliation, unwillingness to become involved). Victims of corporate fraud have their own reasons:

> Statistics summarizing reported and prosecuted crimes are an innacurate measure of the scale and scope of corporate fraud. Estimates suggest that less than 15 per cent of discovered cases are reported to the police. The reasons for non-reporting vary from the reluctance of victims, and particularly banks, to admit that they have been defrauded to failure to recognize that losses were dishonest.
>
> Other victims are dissuaded against taking action out of misguided sympathy for the perpetrator, lost management time in courts, or in the belief that funds cannot be recovered. ... **/

Although fraud generally involves misrepresentation of a material fact with intent to defraud, the above observation applies equally to any crime resulting in loss or destruction of valu-

---

*/ See Vol. II, No. 3 Computer/Law Journal 471 (Summer 1980), Rifkin, a Documentary History, by Jay Becker.

**/ Comer, Corporate Fraud, at pp. 2-3 (2d Ed. 1985).

able corporate assets (e.g., physical asportation of a tape reel containing valuable data; destruction of equipment by a disgruntled employee).

Reluctance of business victims to cooperate is compounded by the intrinsic hidden criminality of computer crime. This, coupled with difficulty in identifying perpetrators, adds to the complications of dealing with a technology whose intricacies can be elusive even to the trained expert. It is no wonder that computer crimes reported to date represent the tip of a largely immeasurable iceberg.

Presenting alarming threats to the security and integrity of computer programs in virtually every computer environment is the tampering with computer systems by the introduction of a so-called "computer virus." This is a set of computer instructions surreptitiously introduced that reproduce themselves throughout a system, or from one system to another, which, when executed, cause results ranging from mischievous to disastrous. Of particular concern is the threat to computer systems in financial institutions and sensitive government operations accessible through external telecommunications networks.

Donald Burleson has the dubious distinction of being the first to be prosecuted on charges of computer sabotage and burglary where the charges are based in part on infecting a computer system with a virus. After being fired from his job as a computer programmer with a Fort Worth-based insurance and securities concern, Burleson erased thousands of important company computer records and introduced a set of computer instructions programmed to move through the system and erase additional records in the future.

The most notorious computer virus case, under investigation at this writing, is the case of Robert Morris, a Cornell University graduate student, who created a virus that disabled thousands of computer systems throughout the country. Since many of the systems invaded were on "Federal interest" computers, the FBI is investigating to determine whether, inter alia, the Computer Fraud and Abuse Act of 1986 was violated.

According to one news account, */ Morris exploited flaws in the operating system used by a nationwide telecommunications network to break into private files, whereby he attempted to introduce a program "that would silently invade other computers but would not harm them." A programming error supposedly permitted the program to multiply within each computer, choking systems on the network throughout the country.

---

*/ Washington Post, November 8, 1988.

2. DESTRUCTIBILITY OF EVIDENCE

Computer-related evidence includes, but is not limited to, the following:

- Mainframe central processing units (CPU's) and associated hard-wired peripheral equipment (e.g., readers, printers, display units, tape units, disk units, magnetic drums, hard disks, and mass memory units)

- Removable electronic or magnetic storage devices (e.g., tape reels, disk drives, diskettes and video disks)

- Personal or professional computers (PC's) and associated peripheral equipment

- Remote input/output devices (e.g., reader, printer and screen display terminals)

- Remote processing devices (e.g., programmable terminals and PC's)

- Telecommunications equipment used to communicate with a computer

- Electronic communications transmitted to or from a computer

Although all of the above items or their contents can be the object of a subpoena, a discovery request, or a search and seizure, crimes involving unauthorized access to a computer or electronic communications, or use of a computer in furtherance of an illegal act, usually involve as evidence only items containing information or data (e.g., tapes, disks, print-outs) and related documentation.

The intangible nature of information stored or transmitted in electronic or magnetic form raises special problems because the information is not visible to the naked eye and because of the ease with which such information can be altered or destroyed. Destruction of evidence of a crime before it is discovered or seized is foremost in the mind of the seasoned or professional criminal. (Visualize: use of flash paper or dissoluble rice paper by bookmakers to record bets, or the flushing or swallowing of heroin packets at the sound of a knock on the door.) There is no reason to believe that the computer criminal is any different. In fact, given the facility with which computer-stored information can be altered, erased or overwritten, the well-planned computer crime offers unique methods for causing evidence

to disappear without a trace. */

Most computer centers use an electrical device called a "degausser" to routinely erase magnetic tapes or removable disks for reuse as "blank" tapes or disks or to remove sensitive data from recently used tapes or disks before returning them to a common pool. Although this is one method for a disgruntled employee to sabotage valuable computer files, this is not the way to erase evidence of an illegal program or data base alteration without arousing suspicion. The sophisticated perpetrator would more likely include as part of his "trojan horse" or "trap door," instructions that restore the violated program or data base back to its original form after the deed is done - literally covering up his tracks.

---

*/ Alterations or erasures are accomplished in an incomprehensible period of time once appropriate computer instructions have been initiated. Erasure of information in a computer's main memory is measured in milli-, micro or nanoseconds (thousandth, millionth, billionth of a second, respectively).

3. IDENTIFICATION OF PERPETRATORS

Because of the ease with which an unidentified person who knows the process can make a transparent entry into a computer system, and the ability of many to wipe out any trace of the entry, identification of the perpetrator of a computer crime can be difficult or even impossible to determine. Consequently, targeting of suspects often requires orchestration of unusual investigative procedures. This is well illustrated in the case of United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978).

Seidlitz had assumed the position of Deputy Project Director for a computer service company which was under contract to install, maintain, and operate a computer facility for use by the Federal Energy Administration (FEA). He had helped to prepare the software installed at the facility, which provided for online access to the facility's systems through remote terminals, and was responsible for security of the central computer system. Seidlitz had full access to facility computers and to a software system known as "WYLBUR" residing within them.

Seidlitz resigned his job and was working at his own computer firm when an FEA computer specialist temporarily assigned to the facility attempted to locate a friend who might be a system user by requesting a terminal display of initials of everyone currently accessing the WYLBUR software. Among the displayed initials were those of his supervisor who was standing nearby and obviously not using the system.

Suspicious that an unauthorized intruder was accessing the system under the guise of the supervisor, he brought the matter to the attention of contractor employees who initiated a terminal request to display system information about to be transmitted to the possible intruder. The information proved to be a portion of the WYLBUR "source code," which was proprietary system software. Through a capability provided by the system, it was determined that the intruding connection was by a telephone outside the facility. The telephone company was requested to manually trace the call which turned out to emanate from Seidlitz' office, but the identity of the caller could not be divulged without a subpoena.

The following day, the contractor activated a feature of the WYLBUR system which automatically recorded any further requests initiated by the intruder as well as any responses sent to him. The telephone company was requested to perform another manual trace when an intrusion was suspected and again this led to Seidlitz, and again the contractor was not given his identity.

The contractor informed the FBI of the events, whereupon a search warrant was obtained to search Seidlitz' office. Before

executing the warrant, the FBI requested that the telephone company perform two more traces when alerted by the contractor of incoming calls, but in each instance the calls were terminated before the traces had progressed beyond the telephone company's office (which served 10,000 subscribers). The telephone company then installed "originating accounting identification equipment" which enabled automatic and quick determination of the number of any of the area phones from which calls to the computer facility originated without intercepting the contents of any communication. The equipment ascertained that two subsequent calls to the computer facility originated from Seidlitz' residence.

The FBI promptly executed the warrant to search Seidlitz' office, seizing a copy of the user's guide for accessing the contractor's system and some forty rolls of computer paper containing a printout of the WYLBUR software source or program code. Pursuant to a warrant to search Seidlitz' residence, a portable communications terminal with a teleprinter was found, as well as a notebook containing information relating to access codes that had been assigned to authorized users of the contactor's systems.

Seidlitz' conviction on two counts of fraud by wire was upheld. However, if the alert FEA computer specialist had not chanced to be on the system at a time when the person whose initials were displayed was near by and not using the system, and if Seidlitz was near completion of appropriating what he was after, the crime would have probably gone undetected.

Profiles of criminals are of dubious assistance in an investigation, but as with other types of crimes, studies have been conducted to establish one for perpetrators of computer-related crime. Some characteristics propounded for the "computer criminal" are that: */

> Most perpetrators are between 18 and 35 years old.
>
> ....
>
> Few perpetrators are females. Computer technical positions have been predominantly held by males. As more females enter these positions, this characteristic can be expected to change.
>
> ....
>
> Perpetrators are bright, highly motivated, adventuresome, creative, and willing to accept a

---

*/ Somers, Economic Crimes, Investigative Principles and Techniques, supra, at pp. 127-128.

> challenge. They tend to be amateur criminals. They are hard workers, first to arrive at and the last to leave work. More often than not, they are among the most trusted employees. Perpetrators have a fear of exposure. Often they will spend a great deal more time covering up a computer-related crime than they did perpetrating the crime. When caught, they minimize the "criminal" intent. Seldom do they see themselves as true criminals.
>
> ....
>
> As a group, perpetrators may occupy a wide range of computer-related skill levels. These individuals are not only the highly experienced technical professionals but also may be found in the lower-level non-technical positions.

One writer suggests that "[c]omputer criminals may be broadly separated into two categories: hackers and white collar criminals," where one is some sort of free-spirited adventurer and the other is a common thief or data base hit man:

> The ordinary hacker is characterized as a male under the age of 21, intelligent, but not necessarily an over-achiever. He is generally motivated by the thrill of the chase, and is merely concerned with gaining access, not with doing any damage after the access has been achieved.
>
> ....
>
> The white collar criminal is generally an individual who is a part of the work force and is in a position to gain inside information concerning computer access. The criminal is often a male with at least some college education and a desire for financial security. This type of criminal has two routes to monetary success. He may gain access to computer data banks either to transfer money to his own account or to steal or destroy valuable information for third parties who will pay him well for his efforts. */

There are those that take a dim view of characterizing hackers as some sort of juvenile interlopers in an electronic playground, dismissing their intrusions with a "boys will be boys" attitude. The following illustrates what the so-called "free-spirited

---

*/ Smith, Who is Calling Your Computer Next? Hacker!, Vol. 8, No. 1 Criminal Justice Journal 93, at 93-94 (1985).

adventurer" is capable of:

> In August 1986, Dr. Clfford Stoll, a computer systems administrator at Lawrence Berkeley Laboratories (LBL), a research lab for the Department of Energy, discovered an unauthorized user accessing his computer system. Dr. Stoll identified the security holes used by the intruder and immediately patched them to prevent future unauthorized access. Dr. Stoll approached this intruder as an academic challenge and proceeded to attempt to identify this "13 year old, spectacled, antisocial computer enthusiast." He decided to allow the intruder access to his system so he could monitor his activity and trace the phone calls in an attempt to identify the subject.
>
> Dr. Stoll discovered, by observing the activity of this intruder, that the individual was extremely patient and persistent. He seemed to be interested only in military computers and computers of defense contractors. The intruder, after accessing the computer, would (through faulty security) gain administrator privileges and scan files in the system for "nuclear," "norad," "cia," "icbm," "sdi," "stealth," etc.
>
> ....
>
> Over 45 systems were successfully penetrated, and in 10-15 of these sites, the intruder was able to give himself system administrator privileges, which means he "owned the systems." The systems identified are only the ones we know about. It is quite probable the intruder had successfully penetrated many more.
>
> ....
>
> Overall, 450 DoD contractor computer systems were attacked.
>
> ....
>
> The crime scenes were located in approximately 500 locations in 40 different states, and 15 countries. The only thing the different crime scenes had in common were the hacker and the fact that the path used by the hacker usually went through LBL's computer.
>
> ....
>
> ... To date, we do not know the motivation of this

> intruder who spent thousands of hours penetrating military computers only to make copies of the files he could gain access to. Rarely did he ever modify or delete the data once he had gained access. When he did, it was only to cover his trail or to plant the seed that would allow easy access at a later time. */

The hacker, Marcus Hess, was eventually identified through the combined efforts of the FBI, the Air Force Office of Special Inestigations, West German authorities and Tymnet. Hess used an Apple and Atari computer located in his house in West Germany to accomplish the intrusions. Despite the seizure of 80 incriminating floppy disks, on April 26, 1988, a German court ruled that the (German) prosecution did not have sufficient evidence to prosecute. So much for "free-spirited adventurers!"

Regardless of categorization or profile, as with most other crimes, computer crimes are committed by individuals whose mens rea or criminal intent is formed by two basic factors: opportunity to commit the crime and vulnerability of the victim or target. The former can be expected to increase with the growing dependence on computers to store sensitive information and conduct monetary transactions. Vulnerability increases with the complexity of security problems caused by increased use of remote input/output devices (terminals), online microcomputers (PC's), and communications networks to access information or transact business. Both factors are compounded by the growing pool of potential perpetrators created by "the exponential growth of computer literate users who are capable of exploiting this new vulnerability and ... the trend towards allowing clients and customers to submit instructions directly into a vendor's or bank's mainframe." **/

A study of computer-related fraud in the banking and insurance industries indicates a wide-ranging perpetrator profile and objective of the fraud within these industries:

> The cases show the range of perpetrators covered almost every aspect of corporate operations, with the preponderance outside the EDP area. Most perpetrators in the banking industry were either data entry clerks or

---

*/ Excerpt from Christy, The Autopsy of an International Computer Hacker Investigation, A report of the Computer Crime Division, Air Force Office of Special Investigations (June 1988).

**/ Balding, Computer Breaking and Entering: The Anatomy of Liability, Vol. 5, No. 1 The Computer Lawyer 5 (January 1988).

loan officers. In the insurance industry, most were claim processors or policy service clerks. Where perpetrators were supervisors or management personnel, their schemes generally lasted longer and involved larger dollar amounts.

In several cases, accomplices were used to receive or negotiate funds; but, in virtually all of these cases, they were not necessary to perpetrate the fraud.

The primary objective of most perpetrators was to take money from the bank or insurance company; however, some perpetrators manipulated data to show a better record of performance (for example, one bank loan officer extended due dates on loans to show a good record of loan collections). */

In virtually all cases, perpetrators were employees and were later dismissed from employment. In the majority of cases, legal action was taken or was pending. In many cases, restitution was made or was in process.

One-third of the cases reported were detected by systems of internal accounting control or routine internal or external audits. Another third were detected through accident, unusual activity of the perpetrator, tip-off or other non-routine event. Most cases were uncovered by persons within the company while many were discovered as the result of customer complaints. In the insurance cases, policyholders usually were not aware that fraudulent transactions had been processed against their policies. **/

---

*/ Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries, EDP Fraud Review Task Force,American Institute of Certified Accountants, at pp. 7-8 (1984). (The study was based on a survey response from 5,127 banks and 854 insurance companies in which a total of 145 computer-related frauds were reported. Id., at p.5.)

**/ Id., at p. 8.

CHAPTER II: PERPETRATOR TECHNIQUES

There are a wide range of techniques employed in perpetrating computer-related crimes. However, the choice of technique is largely determined by the knowledge possessed by the perpetrator of the particular system chosen to be victimized or used as an instrumentality, coupled with the opportunity to apply this knowledge to effectuating the crime. The technique itself can be highly sophisticated, requiring considerable technical expertise, or quite mundane, requiring little or no technical knowledge or ability.

Following are descriptions of some of the more commonly employed techniques: */

1. Data Diddling

   This is the simplest, safest, and most common method used in computer-related crime. It involves changing data before or during their input to computers. The changing can be done by anybody asociated with or having access to the processes of creating, recording, transporting, encoding, examining, checking, converting, and transforming data that ultimately enter a computer. Examples are forging or counterfeiting documents; exchanging valid computer tapes, cards, or disks with prepared replacements; source entry violations; punching extra holes or plugging holes in cards; and neutralizing or avoiding manual controls.

2. Trojan Horse

   The Trojan horse method is the covert placement of computer instructions in a program so that the computer will perform unauthorized functions but usually still will allow the program to perform its intended purposes. This is the most common method in computer program-based frauds and sabotage. Instructions may be placed in production computer programs so that they will be executed in

---

*/ Excerpted from National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration (LEAA), U.S. Department of Justice, Computer Crime, prepared under an LEAA grant by SRI International (1979). Most, but not all, techniques appearing in the LEAA report are described.

the protected or restricted domain of the program and have access to all the data files that are assigned for exclusive use of the program. Programs are usually constructed loosely enough to allow space to be found or created for inserting the instructions.

3. Salami Techniques

An automated form of crime involving the theft of small amounts of assets from a large number of sources is identified as a salami technique (taking small slices without noticeably reducing the whole). For example, in a banking system the demand deposit accounting system for checking accounts could be changed (using the Trojan horse method) to randomly reduce a few hundred accounts by 10 cents or 15 cents by transferring the money to a favored account where it can be legitimately withdrawn through normal procedures. No controls are violated because the money is not removed from the system of accounts. Instead, a small fraction of it is merely rearranged. The success of the fraud is based on the idea that each checking account customer loses so little that it is of little consequence. Many variations are possible. The assets may be an inventory of products or services as well as money.

4. Superzapping

Superzapping derives its name from superzap, a macro/utility program used in most IBM computer centers as a systems tool. Any computer center that has a secure computer operating mode needs a "break glass in case of emergency" computer program that will bypass all controls to modify or disclose any of the contents of the computer. Computers sometimes stop, malfunction or enter a state that cannot be overcome by normal recovery or restart procedures. Computers also perform unexpectedly and need attention that normal access methods do not allow. In such cases, a universal access program is needed. This is similar in one way to a master key to be used if all other keys are lost or locked in the enclosure that they were meant to open.

....

Utility programs such as superzap are powerful and dangerous tools in the wrong hands. They are

normally used only by systems programmers and computer operators who maintain computer operating systems. ...

....

Unauthorized use of superzap programs can result in changes to data files that are normally updated only by production programs. There are usually few if any controls that would detect changes in the data files from previous runs. ...

5. Trap Doors

In the development of large application and computer operating systems, it is the practice of programmers to insert debugging aids that provide breaks in the code for insertion of additional code and intermediate output capabilities. The design of computer operation systems attempts to prevent both access to them and insertion of code. Consequently, system programmers will sometimes insert a code that allows compromise of these requirements during the debugging phases of program development and later when the system is being maintained and improved. These facilities are referred to as trap doors. Normally, trap doors are eliminated in the final editing but sometimes they are overlooked or purposely left in to facilitate ... future access and modification. In addition, some unscrupulous programmers may purposely introduce trap doors for later compromising programs. ...

Trap doors may also be introduced in the electronic circuitry of computers.

6. Logic Bombs

A logic bomb is a computer program executed at appropriate or periodic times in a computer system that determines conditions or states of the computer that facilitate the perpetration of an unauthized, malicious act. ...

A logic bomb can be programmed to trigger an act based on any specified condition or data that may occur or be introduced. Logic bombs are usually placed in the computer system using the Trojan horse technique.

7. Scavenging

Scavenging is a method of obtaining information that may be left in or around a computer system after the execution of a job. Simple physical scavenging could be the searching of trash barrels for copies of discarded computer listings or carbon paper from mutiple-part forms. More technical and sophisticated methods of scavenging can be done by searching for residual data left in a computer after job execution.

For example, a computer operating system may not properly erase buffer storage areas used for the temporary storage of input or output data. Some operating systems do not erase magnetic disk or magnetic tape storage media because of the excessive computer time required to do this. Therefore, new data are written over the old data. It may be possible for the next job to be executed to read the old data before they are replaced by new data ... thus capturing - scavenging - data that were stored by the previous job.

8. Data Leakage

A wide range of computer-related crimes involves the removal of data or copies of data from a computer system or computer facility. ...

....

Several techniques can be used to leak data from a computer system. The perpetrator may be able to hide the sensitive data in otherwise innocuous looking output reports. ... An even more sophisticated method might be to encode data to look like something different than they are. ... Another method is controlling and observing the movement of equipment parts, such as the reading and writing of a magnetic tape causing the tape reels to move clockwise and counterclockwise in a pattern representing binary digits 0 and 1. ...

9. Piggybacking and Impersonation

Piggybacking and impersonation can be done physically and electronically. Physical piggybacking is a method of gaining access to controlled access areas when control is accomplished by electronically or mechanically locked doors. Typically an individual usually with hands full of computer-

related objects such as tape reels stands by the locked door. When an authorized individual arrives and opens the door, the piggybacker goes in after or along with him. ...

....

Electronic piggybacking can take place in an on-line computer system where individuals are using terminals, and identification is verified automatically by the computer system. ... Compromise of the computer can take place when a hidden computer terminal is connected to the same line through the telephone switching equipment and when the legitimate user is not using his terminal. Piggybacking can also be accomplished when the user signs off improperly, leaving the terminal in an active state where it assumes the user is still active.

Impersonation is the process of one person assuming the identity of another. Physical access to computers or computer terminals and electronic access through terminals to a computer require positive identification of an authorized user. The verification of identification is based on some combination of something the user knows, such as a secret password; something the user is ... ; and something the user possesses, such as a magnetic stripe card or metal key. Anybody with the right combination of identification characteristics can impersonate another person.

10. Wiretapping

....

Wiretapping requires (costly) equipment ... and a method of recording and printing the the information. The perpetrator usually will not know when the particular data he is interested in will be sent. Therefore, he must collect relatively large amounts of data and search for the specific items of interest. Identification and isolation of the communications circuit can pose a problem for the perpetrator.

CHAPTER III: PROBLEMS OF PROOF

1. CHARGING A CASE

Upon reviewing evidence indicating that a crime has been committed, the Federal prosecutor must determine what, if any, Federal statutes have been violated and which district or districts have prosecutorial jurisdiction (i.e., where to venue the case). */ Further, he or she should ascertain whether the matter would best be prosecuted by state authorities under a more effective state law.

As with any crime involving highly complex issues, factors to consider where there is a choice of venue include:

a. Availability of investigative and prosecutorial resources with a track record in dealing with computer-related criminal cases.

b. Small versus large district, where odds might be better in a large district for going before a jurist and a jury more comfortable with technical terms.

c. Availability of government witnesses qualifiable as experts in the computer processes at issue.

d. Existence of state statutes that can be used alternatively or as leverage for plea bargaining. **/

These factors are particularly important in an evolving area of criminality such as computer-related crime where special statutes are couched in technical terms and where other applicable statutory proscriptions did not contemplate crimes involving computers. Most states as well as the Federal

---

*/ Federal Rules of Criminal Procedure, Rule 18, states:

> Except as otherwise permitted by statute or by these rules, the prosecution shall be had in a district in which the offense was committed. The court shall fix the place of the trial within the district with due regard to the convenience of the defendant and the witnesses and the prompt administration of justice.

**/ From notes provided by Assistant U.S. Attorney David F. Geneson, based on lectures given to criminal investigators at the Federal Law Enforcement Training Center.

government have enacted laws in an attempt to overcome both perceived and real definitional problems encountered in trying to apply traditional criminal sanctions to computer-related crimes.

a. The Need for Special Statutes */

Absent a statute specifically addressing computer crimes, Federal, state and local prosecutors must rely on traditional criminal prohibitions in making a case (e.g., larceny, embezzlement, false pretenses, and forgery), each having specific elements that must be satisfied. There are numerous Federal statutes that can be used in prosecuting computer-related crimes, for example, mail fraud, wire fraud, and banking statutes. **/ Not to be overlooked is the Racketeer Influenced and Corrupt Organizations (RICO) Act, 18 U.S.C. §§ 1961-1968, in cases such as software piracy involving a pattern of racketeering activities and specified predicate crimes. ***/ Also, the Electronic Fund Transfer Act, 15 U.S.C. §§ 1693 et seq., provides criminal liability regarding specified uses of a "fraudulently obtained debt instrument" which is defined as a "card, code, or other

---

*/ This subsection includes excerpts from an article entitled Problems in Prosecuting Computer Fraud written by the author of this monograph that appeared in the October 1982 issue of the National Association of Attorneys General Criminal Justice Report. Material is reprinted with the permission of the Association.

**/ A particularly effective statute is 18 U.S.C. § 641 (Public money, property or records), which states in pertinent part:

> Whoever embezzles, steals purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, ... or
>
> Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted -- ...
>
> Shall be fined ... or imprisoned ... or both. [Emphasis added.]

***/ See Coolley, RICO: Modern Weaponry Against Software Pirates, Vol. V, No. 2 Computer/Law Journal 143 (Fall 1984). (The focus of this article is on civil RICO actions, but discusses criminal cases supporting predicate offenses.)

device ... by the use of which a person may initiate an electronic fund transfer." 15 U.S.C. § 1693n. */

Generally speaking, a hacker is one who intentionally uses a computer terminal or microcomputer to gain unauthorized or illegal telecomunications access to a computer. This often requires "phreaking," or using illegally obtained authorized customer account numbers or access codes that have been acquired by other hackers and published in underground electronic bulletin boards, or by doing one's own account number or access code hacking.

Computers are invariably involved in phreaker hacking, either by the hacker as a method of generating and automatically trying hundreds or thousands of fabricated numbers or codes and recording "hits," or by the organization being hacked to validate authorized access. This type of "computer-related" criminal activity is often charged under 18 U.S.C. 1029 (credit card/access device fraud) if it affects interstate or foreign commerce. (A notable case is U.S. v. Brewer, 835 F.2d 550 (5th Cir. 1987), which is the first case to "read long distance access codes into the section 1029 definition of 'access device.'")

Conforming computer concepts to a specific statutory or common law prohibition can be a difficult task, but it is questionable whether some illegal acts should be considered a computer crime just because a computer-related item is the object of the act. For example, if a perpetrator physically takes a reel of magnetic tape with intent to steal a copy of a valuable computer program or collection of sensitive data recorded on the tape, no special computer crime statute is required to prosecute for larceny. **/ If, however, this same information is obtained by line transmission to a tape unit, disk drive, or printer attached

---

*/ United States Code Title 15, § 1693a(6) states in pertinent part:

> [T]he term "electronic fund transfer" means any transfer of funds ... which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape, so as to order, instruct, or authorize a financial institution to debit or credit an account. ... [Emphasis added.]

**/ Query whether the owner is "deprived" of the program or data (required by some definitions of larceny). See Taber, On Computer Crime (Senate Bill 240), Vol. 1, No. 3 Computer/Law Journal 517, note 55 at p. 525 (Winter 1979).

to a remote terminal or microprocessor located in the perpetrator's home, the case for theft can meet frustrating problems of proof absent a special statute. The classic case of Ward v. Superior Court, 3 CLSR 206 (Cal. Super. Ct. 1972), is a case in point.

In the Ward case, an unauthorized duplication of a program was made through a remote terminal. The prosecutor charged grand theft and theft of a trade secret. To meet the definition of theft, it was necessary to show the element of asportation. The court stated:

> Implicit in the definition of "article" ... is that it must be something tangible, even though the trade secret which the article represents is intangible. Based upon the record here, the defendant Ward did not carry any tangible thing ... from the ISD computer to the UCC computer unless the impulses which defendant allegedly caused to be transmitted over the telephone wire could be said to be tangible. It is the opinion of the Court that such impulses are not tangible and hence do not constitute an "article" within the definition contained in (the statute) ... [3 CLSR 206, 208]. */

Although Federal and state statutes have since been enacted to address problems such as the "intangible" nature of electronic impulses or magnetic records, the Ward case is an example of how prosecution of a seemingly strong case can deteriorate by a court's analysis of technical facts as they relate to applicable laws. (This is compounded when the defense is offering misleading explanations of technical processes.)

Federal and state computer crime legislation is intended to remove some of the burdens imposed on prosecutors who must otherwise rely on traditional legal proscriptions developed before the computer age. As with any new laws dealing with an emerging socio-economic problem, there is considerable diversity of approach among the various legislative bodies in addressing the issues. Uniformity will have to await judicial experience with concepts and terminology involved in computer-related legal con-

---

*/ Ingraham, On Charging Computer Crime, Vol. II., No. 2 Computer/Law Journal 429 (Spring 1980). (Although the element of asportation was not met regarding the electronic transmission of information, the court found that a printout of the program was deemed to be an "article" that was "carried away" by Ward.) See also Seidlitz, supra.

troversy. In any event, Federal prosecutors and investigators should be aware of state sanctions to determine whether to pass a case that cannot be federally charged to a state having jurisdiction. (The chapter on Computer-Related Evidence Law presents an indication of current attitudes in dealing with the technology as expressed in recent Federal opinions.)

b. Federal Computer Crime Statutes

The Federal prosecutor has a sizable arsenal of so-called "traditional" statutes to draw on in dealing with crimes involving a computer. It is estimated that as many as forty Federal statutes may possibly be used, depending on the circumstances and issues. */ Equally important are changes to the Federal Rules of Evidence that recognize information in electronic or magnetic form as "writings and recordings" and printouts thereof as "originals." **/

Difficulties in depending on traditional criminal statutes to charge crimes involving use of a computer or access to electronically stored information as part of the proscribed act prompted enactment of the Computer Fraud and Abuse Act of 1984, the subsequent enactment of the Computer Fraud and Abuse Act of 1986, and inclusion of computer-related provisions in the Electronic Communications Privacy Act of 1986. Following is a summary of these Acts:

(1) Computer Fraud and Abuse Act of 1986

The first Federal computer crime statute was enacted in 1984 as part of P.L. 98-473, which added § 1030 (Computer Fraud and Abuse Act of 1984) to United States Code Title 18, Chap. 47 (Fraud and False Statements). This Act made it a felony to access without authorization classified information in a computer, and a misdemeanor to trespass into a government computer or access financial records or credit histories in financial institutions.

After two years of further debate and public comment on the 1984 statute, P.L. 99-474 (Computer Fraud and Abuse Act of 1986) was enacted to modify the wording and expand prohibitions and penalties of § 1030. Salient aspects of the 1986 Act are provi-

---

*/ Volgyes, The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the-Art Review, supra, at p. 396.

**/ Fed. Rules of Evid., Rules 1001(1) and 1001(3), respectively.

sions that make it a first-offense felony to in essence: */

1) knowingly access a "Federal interest computer" without authorization with the intent to defraud and thereby obtain anything of value; or

2) intentionally access a "Federal interest computer" without authorization, causing damage to information in the computer or preventing use of the computer or information resulting in a loss valued at $1,000 in one year or in modification or impairment of an individual's medical records; and

3) make it a first-offense misdemeanor to knowingly, without authorization, and with intent to defraud, traffic in computer password information affecting interstate or foreign commerce or involving a computer used by or for the Federal government.

(It should be noted that the inclusion of unusual required elements of proof in various provisions of the statute, coupled with the awkward wording of certain definitional sections, has reduced its prosecutorial utility.)

(2) Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 amends the Federal wiretap law enacted in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to, inter alia, account for advances in computer and communications technology. Title I of the Act addresses interception of wire, oral and electronic communications, while Title II addresses access to stored wire and electronic communications and transactional records. Electronic communications covered include computer message and data transmissions, which the Act makes unlawful to intercept or access unless the communication is readily accessible to the general public.

Regarding stored electronic communications, the Act proscribes intentional access without authorization of a facility through which an electronic service is provided, whereby an

---

*/ The 1986 Act was enacted after consideration and passage of House bill H.R. 4718 and Senate bill S. 2281. The House bill was passed as P.L. 99-474 after amendments incorporating much of the text of the Senate bill. The legislative history of H.R. 4718 and S. 2281 is contained in: 1) House Report No. 99-612 (Judiciary Committee); 2) Senate Report No. 99-432 accompanying S. 2281 (Judiciary Committee); and 3) Congressional Record, Vol. 132 (1986).

electronic communication is obtained, altered, or authorized access to the communication is prevented. In addition, provisions prohibit specified disclosures of the contents of an electronic communication, spell out requirements for governmental access, and permit including in a subpoena or court order a requirement that the electronic service provider create a backup copy of the electronic communications for preservation. */

The Act amends United States Code Title 18, Chap. 119 (amended title: Wire and Electronic Communications Interception and Interception of Oral Communications), § 2510, et seq., and § 2232 (Destruction or removal of property to prevent seizure), and adds § 2521 (Injunction against illegal interception). In addition, it inserts a new chapter after Chap. 119, namely Chap. 121 (Stored Wire and Electronic Communications Transactional Records Access) as §§ 2701-2710.

Although the new legislation does indeed offer additional proscriptions on which to base computer-related crime charges, some would argue that it does not go far enough. For example, absent the required elements (such as intent to defraud, damage to information, etc.), the act of "hacking" (defined earlier) through a remote terminal or microprocessor just to see if it can be done, is not per se a Federal crime even if it is done to a "Federal interest" computer.

One writer suggests that "there is no such thing as a `computer crime,' and therefore there is no need for special legislation." **/ Another contends that although "[t]echnologically, the 1986 Act enabled Title III to come of age; unfortunately, the Act caused corresponding privacy rights to regress." ***/ Whatever real or perceived flaws there may be in current legislation, the fact remains that lawmakers throughout the

---

*/ The Act was enacted after consideration and passage of House bill H.R. 4952 and Senate bill S. 2575. The House bill was passed as P.L. 99-508 after amendments incorporating much of the text of the Senate bill. The legislative history of H.R. 4952 and S. 2575 is contained in : 1) House Report No. 99-647 (Judiciary Committee); 2) Senate Report No. 99-541 (Judiciary Committee); and 3) Congressional Record, Vol. 132 (1986).

**/ See Taber, On Computer Crime (Senate Bill S. 204), supra, at p. 518.

***/ Burnside, The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunication Technologies, 13, No.2 Rutgers Computer & Technology Law Journal 451, at p. 517 (1987). (A comprehensive analysis of the 1986 Act.)

nation are responding to real problems in prosecuting crimes involving computers. Experience with current computer-related legislation as the frequency and seriousness of unauthorized computer intrusions grows will undoubtedly lead to periodic legislative revisitation in this area.

2. USE OF EXPERTS

An expert is generally regarded as one who has authoritative knowledge in a particular field, or is highly proficient in some specialty, skill or process. Experts in various aspects of computer processes (e.g., programming, systems analysis, operations, input preparation, etc.) can be essential in investigating and proving a computer crime.

Assistance of experts is frequently necessary to gather and safeguard evidence and to identify and apprehend the perpetrator. Further, experts may be necessary to provide an adequate legal foundation for the entry of computer records into evidence at trial. In many cases, auditing and accounting expertise is needed in addition to computer professionals or technicians.

An investigative team may require a combination of expertise to assure complete understanding of areas such as:

1) documented types of computer-related crimes;

2) electronic data processing concepts and equipment;

3) nature of computer vulnerabilities;

4) investigative auditing; and

5) applicable Federal, state and local laws. */

Auditors may be needed to trace the flow of information in a system while accountants may be necessary to interpret financial transactions and record keeping practices.

Experts familiar with the computer environment and programs involved in the crime are best prepared to retrace the perpetrator's actions in committing the crime and to identify and describe suspect computer files and other evidence sufficiently to meet particularity requirements of a search warrant. These individuals can also facilitate determining what computer programs must be acquired or written to display or analyze infor-

---

*/ Volygyes, The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the-Art Review, Vol. II, No. 2 Computer/Law Journal 385 (Spring 1980).

mation contained in these files.

Investigation of a computer crime frequently requires search of a computer center or location of a remote terminal or microcomputer. In addition to the above, various experts might be called upon to:

1) determine the optimum time for executing a warrant to assure seizure of data files and software when evidence of the perpetrator's illegal activity is present;

2) identify specific units or devices in the permissible search area apt to contain targeted information (e.g., disk packs, tape reels, online input/output units, program libraries, backup files, hard disks attached to or a part of a microprocessor);

3) determine the best way to duplicate seized files with a minimum disruption of a computer center that is a victim and not a party to the crime (e.g., using the center's duplicating procedures);

4) establish procedures for safeguarding seized computer files from inadvertant damage (e.g., tape reel warpage; degaussing);

5) determine what hardware, if any, should be seized; and

6) assist in preparing trial exhibits, selecting expert witnesses and drafting technical questions for examination of witnesses.

Usually the best source of appropriate experts to assist in a computer crime investigation is the cooperative victim's computer services staff; however, care must be taken not to tip off a yet to be identified perpetrator who might be a member of this staff. This precaution applies equally to the victimized government agency (which presumably will be cooperative).

Other sources usually available to government investigators are computer services, audit and finance organizations in the various government agencies. This may be the least costly, but care must be taken not to accept the services of someone who happens to be available but does not have the particular knowledge or experience required. For example, evidence of the crime might be imbedded in a computer program written in assembly or machine language, requiring someone who understands this kind of computer code (as opposed to COBOL or FORTRAN). Short of hiring a consultant to assist in selecting qualified experts, investi-

gators and prosecutors can prevent serious negative consequences by gaining sufficient familiarity with computer technology to be able to detect obvious shortcomings in a proposed "expert."

An expert who assists in investigating a crime can be called as a witness, and as with witness testimony in general, he "may not testify to a matter unless evidence is introduced sufficient to support a finding that he has personal knowledge of the matter." Fed. Rules of Evid., Rule 602. An exception to this is "expert witness" testimony. */ This is not to say that an expert who gains first-hand knowledge of a matter in evidence during an investigation cannot also qualify as an expert witness as to that or some other matter.

The following suggests criteria for selection of experts needed to testify for various kinds of evidence frequently proffered in a computer crime trial:

(1) If it is necessary to show how a system works, how it can be violated, or how the information you need to get in to evidence was generated, you need the systems analyst who designed the system and most likely a substantial portion of the documentation and design work in graphic form (to simplify the testimony) is most appropriate.

(2) If it is necessary to describe or detail that portion of a system or program that has been manipulated and how it was manipulated, the programmer who wrote and tested the program is most appropriate.

(3) If it is necessary to show an operations-based manipulation of data, physical destruction, or an unauthorized entry (physically or logically, as reflected on the console log of the system), the computer operations supervisor or lead operator is appropriate. The same witness is needed to authenticate tape reels, disk packs, or listings generated by the particular system containing evidence

---

*/ Fed. Rules of Evid., Rule 702 states:

> If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise. [Emphasis added.]

of the crime, and to explain controls in place that supposedly prevent unauthorized access to records contained in the computer's storage media.

(4) If it is necessary to show the accuracy of information contained in computer storage media as compared to the source documents (e.g., hard or paper copy), the data preparation supervisor or persons who entered the data into the storage media are appropriate.

(5) To show the accuracy of data maintenance procedures and particularly to authenticate the nth generation of a master file as being an unviolated update, it may be necessary to have the tape/disk librarian testify as to the integrity of the file maintenance system or procedures. (Note: backup master files and input may also have to be authenticated.)

(6) If the issue turns on destruction of the system through physical damage, the accuracy of data transmission, reproduction or duplication storage media contents as a function of hardware integrity, or absence of accident or mistake that would affect hardware integrity, it will be necessary to produce the systems engineer who performs the physical maintenance of the hardware, including diagnostic results, manuals and other materials to show continued accuracy and/or lack of accidental malfunction.

(7) If data manipulation or accuracy at the input or output points is at issue, the input and output clerks responsible for the manual handling of card decks, tape reels, disk packs, printouts, etc., during these stages of processing are appropriate.

(8) Where the case involves manipulation of the computer's operating system software (programs that control the execution of all other programs introduced into a given computer system), such as unauthorized access to programs or files, execution of secretly introduced program modules during operation of other programs, running unauthorized programs or running authorized programs in an unauthorized manner, the systems programmer responsible for the accuracy and integrity of the operating systems software is most appropriate. */

---

*/ Geneson notes, supra.

The principal question in selection of a particular witness is whether his testimony will support the relevancy, authenticity and probity of the prosecution's evidence, while serving to rebut expected contrary contentions of the defendant and his witnesses. These and other evidence issues are comprehensively discussed in the chapter devoted to computer-related evidence, citing court opinions regarding the best evidence rule, authentication, hearsay, business records or records of a regularly conducted activity, and laying a proper foundation.

In addition to questioning the veracity and competence of prosecution witnesses, a defendant's counsel can be expected to assault the evidence against his client not only on relevancy and authenticity grounds, but on the reliability and integrity of equipment and personnel resources involved in various stages of computer processing. Common items or areas of such assaults are:

(1) Data Preparation or Input Stage

- Handling of data and input devices
- Audit and quality control procedures
- Numerous sources of input to the same data base
- Accessibility of physical data prior to input
- Personnel technical qualifications
- Equipment standardization
- Error detection/audit verification systems and procedures

(2) Storage Processes

- Reliability of storage media
- Safeguards against loss or damage
- Precautions against tampering or falsification
- Logging/control of access
- Spectrum of persons who have actual access

(3) Development and Operations

- Programming problems

- Quality and security of operating system

- Documentation of systems and programs

- Levels of compliance by personnel

- Processing and preparation procedures

(4) Output Stage

- Actual and perceived reliability of products by end users

- Audit or accuracy measures actually used to determine reliabilty

- Timing of output preparation relative to input of information regarding events described. */

---

*/ Id.

3. USE OF DEMONSTRATIVE EVIDENCE

Demonstrative evidence or visual aids can be real things (such as a gun of the same type used in a homicide), representations of real things (such as a photograph or map), simulations of operations or activities (such as a railroad switch yard), or charts or diagrams of the flow of events or processes (such as a chart tracing monetary transactions). Usually, but not necessarily, this kind of evidence is in the form of visual aids in the sense that the trier of fact is provided a means of "visualizing" the thing or process at issue. The key to meeting opposing counsel's objections to this kind of evidence is to show that the demonstrative evidence represents the level of accuracy being suggested of the thing or process it purports to be. Depending on the nature of the evidence, an expert may be required to lay a proper foundation for its admission.

Following are typical visual aids that should be considered in a computer crime trial (excerpted from Geneson notes, supra):

(1) Flow charts - to show the system design logic, flow of data and other processes, and/or how the system was violated.

(2) Program listings - to show where computer program code was altered and the effect of the alteration.

(3) Data listings - to show the real data and how it was manipulated, what occurred on a specific date (i.e., reconstruct history), and/or how information was changed by the manipulation.

(4) Remote terminals or microprocessors - to show how the system is used from a separate location, the way in which security controls were violated through such a device, and/or how programs or data were accessed or altered.

(5) System model - to demonstrate an analogous fraud by setting up a "mini-system" and having an expert perform the purported fraud in court.

(6) Photos - showing the computer site that was violated, and/or hardware involved that cannot be brought to the court room (e.g., victim's mainframe and peripheral equipment).

(7) Diagrams - showing the various devices involved (e.g., terminals, phone lines, mainframes, disk drives), how they are linked together, and what the perpetrator physically operated.

4. DISCOVERY AND INSPECTION

The chapter on Computer-Related Evidence Law includes a section on discovery under Federal Rules of Criminal Procedure, Rule 16. Cases discussed make it clear that computer programs and related materials (e.g., printouts, contents of magnetic storage media, etc.) are subject to a Rule 16 discovery request, and that the courts recognize the particular need for providing an adequate pretrial opportunity to examine such items. Otherwise, cross-examination of witnesses attesting to the veracity of computer-produced evidence can be unjustly hampered.

The cases discussed in the "evidence" chapter are quite pertinent to the subject of problems of proof. However, to avoid redundancy, this section is limited to such problems stemming from discovery and inspection costs, and requests for proprietary information.

a. Costs

U.S. Code Title 28, Section 1918(b) provides that:

> [w]henever any conviction for any offense not capital is obtained in a district court, the court may order that the defendant pay the costs of the prosecution. [Emphasis added.]

This includes the cost of discovery "as long as the items of cost are authorized by the statutes and are imposed only on non-indigent defendants in a non-discriminatory manner." United States v. Pommerening, 500 F.2d at 102, citing United States v. Gering, 716 F.2d 615 (9th Cir. 1983). Although the statutory language is permissive, as a practical matter, the government rarely bears the burden of the costs of discovery.

Discovery of computer programs and related materials can result in considerable expenditures. The defendant (as well as the prosecution) is afforded protection against an excessive discovery burden by Rule 16(d)(1), which states in pertinent part that:

> [u]pon sufficient showing the court may at any time order that the discovery or inspection be denied, restricted, or deferred, or make such other order as is appropriate. ...

In United States v. Davey, 543 F.2d 996, 1000 (2d Cir. 1976), the court recognized that a district court may "impose conditions as to cost ... which are designed to minimize the burden" of a dis-

covery summons. */

U.S. Code Title 28, Section 1920 enumerates expenditures that the court may tax in a case (e.g., various court fees; compensation for court appointed experts). However, "[t]here is clearly a lack of consistency among the courts when it comes to determining which items are recoverable as costs or expenses" under this section (and under Section 2412(d)(2)(A) of the Equal Access to Justice Act). Louis v. Nelson, 646 F.Supp. 1300, 1319 (S.D.Fla. 1986).

Given the high cost of computer resources in a large mainframe data processing environment, prosecutors should take care in framing discovery requests to avoid Rule 16 challenges. This applies equally to responding to a defendant's request lest the government is encumbered with unnecessary expenditures.

b. Proprietary Information

Computer-related evidence that is the target of a Rule 16 discovery request often includes proprietary information (i.e., information that is owned or controlled by a third party and licensed or leased to the defendant or to the government for a particular use), or information containing trade secrets that the disclosing party or a third party proprietor does not want to fall into the hands of a competitor.

More often than not, the information is a computer program or data base in machine-readable form required by the requesting party to determine and evaluate the process used to produce computer output proferred for admission by the opposing party. This usually involves running the program with test or actual data, either on the disclosing or the requesting party's computer, or on a disinterested third party's computer.

There are generally three methods of providing legal protection to proprietary or economically sensitive computer programs: patent, copyright and trade secret law. Computer programs (or software) have been patentable for some time. "As viewed by the patent law, software can be considered a method for operating a digital computer. The 'thing' controlled need be nothing more than the hardware every computer includes, e.g., its memory, registers or CRT display." */ However, trade secret and copyright protection are the two methods most commonly used, where the choice depends in large part on the extent of market

---

*/ Lundberg, Sumner and Boyer, Twelve Myths About Patent Protection, 5 The Computer Lawyer 9 (No. 5 1988).

distribution. */

The "fair use" doctrine should dispel any fear of copyright infringement in discovery of copyrighted computer programs or data bases, while no patent infringement can be alleged by merely executing or inspecting a computer program to determine the accuracy or consistency of its results. In either case, a Rule 16(d)(1) protective order can effectively restrict use of the program to stated trial preparation needs.

A protective order is particularly important where a trade secret is involved (which is often the case even with a patented computer program). While recognizing "that proper safeguards should attend the disclosure of trade secrets," Safe Flight Instrument v. Sunstrand Data Control, 682 F.Supp. 20, 21-2 (D.Del 1988), the courts generally limit disclosure of technical information under a protrective order "only to the receiving party's trial attorneys, and, with prior approval of the disclosing party and written assurances, to independent experts assisting the trial attorneys ... and often afford fuller protection to technological information than that extended to ordinary business information." (Emphasis added. Citations omitted.) **/ Hence, it is particularly important for experts that will be inspecting a requested computer program to have no existing or prospective interest in the program that poses a "threat of serious economic injury to the discloser" (or to a third party proprietor of the program). ***/

---

*/ From the onset of the computer age, trade secret protection (often memorialized by contract) has been the legal protection method upon which the software industry has relied most heavily. In the past several years the popularity of copyright has surged, although trade secret protection has continued to be popular. Marketers of mass-distributed program packages largely for use on PCs, today generally place primary reliance on copyright. On the other hand, those who market or use software on mainframe computers, especially where proliferation is rather low, generally rely on trade secret protection.

Bender, The Viability of Copyright Where Trade Secret is Sought, 3 The Computer Lawyer 11 (No. 6 June 1986).

**/ Id., at 22.

***/ Id., at 22.

5. SUBPOENAS

Federal Rules of Criminal Procedure, Rule 17(a), provides for issuance of a subpoena that "shall command each person to whom it is directed to attend and give testimony at the time and place specified therein," while Rule 17(c) provides for issuance of a subpoena commanding production of "books, papers, documents or other objects designated therein." [Emphasis added.]

Although computer printouts of computer programs or data qualify as "documents," and magnetic storage media containing computer programs or data qualify as "other objects," these are of little use to the prosecutor without information describing the operating system, record layouts and other attributes that will enable either:

1) eliciting testimony linking the stored information as the source of the printouts;

2) obtaining printouts of subpoened magnetic storage media; or

3) execution of subpoened computer programs.

Therefore, it is important to include in the schedule of items to be produced clear definitions of technical terms used in the schedule, and documentation that describes computer programs or data produced on magnetic storage media in sufficient detail to enable the prosecutor's computer expert to understand precisely how the above can be achieved. (See Appendix A for an example of such a schedule.)

Unlike a trial, the prosecutor is not allowed to have the computer expert assisting him present during a grand jury investigation while the grand jury is in session. However, this does not preclude consulting with "government personnel" during recesses, including computer experts. Fed. Rules Crim. Proc., Rule 6(e)(3)(A)(ii). Of course, the prosecutor must "promptly provide the district court, before which was impaneled the grand jury whose material has been so disclosed, with the names of the persons to whom such disclosure has been made." Fed. Rules. Crim. Proc., Rule 6(e)(3)(B).

Consultation with the computer expert can be vitally important under circumstances where computer technicians of an uncooperative target organization have been subpoened to testify as to the workings of a computer program and the contents of magnetic storage media. This is especially so in verifying technical descriptions produced in subpoened documents and in filling in purposeful omissions of technical details.

6. MAINTENANCE OF EVIDENCE

The chapter on Making the Case includes a section that presents procedures for investigators to consider in collecting and preserving computer evidence, while the chapter on Computer-Related Evidence Law includes sections that discuss court opinions regarding admissibility and chain of custody issues. These sections address in detail various aspects of properly maintaining computer-related evidence. Following is a brief summary of special procedures that are particularly important in avoiding problems of proof caused by improper care and handling of such evidence:

a. Maintaining evidence in the form of computer storage media presents problems that differ from handling other types of evidence. Because they are subject to erasure and easily damaged, magnetic or electronic storage devices must be carefully guarded and kept under controlled temperature and humidity to avoid deterioration.

b. In investigating and prosecuting a case involving such evidence, one of the early steps a prosecutor should take is to retain an appropriate computer expert for technical assistance. This can be critical in avoiding problems resulting from inept maintenance procedures or inadvertant loss of key information.

c. Sometimes the contents of dozens or even hundreds of computer tapes or disks must be copied to allow the business to continue operating while the case is being prosecuted. This must be done under the close supervision of an expert who can not only assure that it's done right, but can determine the least costly procedure.

d. Initials of the seizing agent and the date should be scratched on each storage media container and a chain of custody sheet or log should be made for every container. The log should show, at a minimum, the date, place and specific location of the seizure, and the name of the agent making the seizure. */

---

*/ Distilled and paraphrased from Prosecutor's Manual on Computer Crimes, pp. 29-30, by Gordon H. Miller, Assistant District Attorney, Atlanta Judicial Circuit, Prosecuting Attorneys' Council of Georgia (1978).

As pointed out in other sections, the agents investigating the case are likely to have considerable expertise in maintaining computer evidence, gained from training and experience. Their advice and assistance can be invaluable to the prosecutor in minimizing problems of proof inherent in computer-related crimes.

7. PROSECUTOR-INVESTIGATOR RELATIONSHIP */

Problems of proof can develop or become exacerbated by failure to establish a proper relationship between the prosecutor and investigator, particularly in a complex case. It would be easy to suggest that somehow the introduction of complex technology into the investigative and prosecutive mix changes the need or eases the development of trust and mutual respect between the investigator and prosecutor. Of course this is not the case. However, there are certain advantages in this type of prosecution that allows the investigator to develop in the prosecutor a dependence and trust often not present in other types of litigation. If the prosecutor is relatively ignorant of the particular technology, and alternatively the investigator is not, the normal mix changes.

It is not uncommon for the investigator to have superior understanding of the technology involved in a case and also know how to seek out and make use of evidence peculiar to this technology. As a consequence, he or she will usually assume the greater responsibility and say-so in structuring the investigatigative and case preparation process.

What this means in terms of the prosecutor-investigator relationship in the investigation and prosecution of a computer-related crime is an increase in the responsibilities of the investigator. The following suggests additional responsibilities of the "computer literate" investigator under these circumstances:

(1) The investigator may need to educate the prosecutor as to what the technological aspects of the case consist. As in a complex bank embezzlement or government fraud case requiring understanding of special terms and processes, the education of the prosecutor becomes critical from the start.

(2) Concomitantly, the investigator's professed understanding of the technology must be right. If the investigator tells the prosecutor that it is essential to get a search warrant because the data will be erased by the operations supervisor (who may be criminally inculpated), then that possibility had better exist and not turn out to be procedurally impossible - e.g., the operations supervisor has no way of accessing the desired data.

(3) The investigator must understand evidentiary procedures as they apply to the peculiarities of computer processing to assure that the evidence control techniques, both during the investigating process and into trial, take into account the actual ability to move things into evidence. Given the inherent

---

*/ Geneson notes, supra.

precision of computer processing activities, it becomes even more critical to appear to put on a flawless case. Since the issues deal with exactitude, the sloppy prosecution becomes magnified.

(4) The investigator must be particularly familiar with the essence of computer-related evidence; that is, not just its content, but whether the evidence can actually be introduced in court. Authenticity of computer-related evidence is particularly subject to creative undermining. This makes choosing witnesses more critical. Because the investigator probably knows more about the system and the processes, the choice of witnesses may fall to him or her. This leads to the responsibility of convincing the prosecutor of the necessity and worth of proposed witnesses, e.g., using "experts" as records custodians, something more easily done by the "expert" investigator.

(5) The process of networking, while common to all complex cases, is particularly important in computer crime cases. With the technologically ignorant (or relatively so) prosecutor, it becomes doubly important for the investigator to know what is going on in the field, i.e., whether other cases similar to the one he or she is investigating have occurred, what prosecutors and investigators are experienced with such cases and how to contact them. The most wasteful loss of a case is one that could have been prevented by tapping the experience of others.

(6) The investigator may be a witness during the litigation. In a computer crime case where the investigator has computer expertise he or she can be a particularly useful witness. In litigation over execution of a search warrant or other means of obtaining evidence, the investigator responsible for development of the search affidavit (and often the warrant execution) will have to be a witness. His or her expertise in the system architecture, how the search was performed, and the rational and legal basis for the search are essential for survival against skillful requests to the court for return of seized materials or motions to suppress.

(7) The skilled case agent can serve as the summary expert (analogous to the IRS accountant that sits at the back of the court room during trial and then summarizes what has gone into evidence -- from a financial standpoint). If evidence is in the form of voluminous data, particularly data from complex system activity, a summary expert is essential. In most districts the case agent can sit at the counsel's table during trial, and "the Rule" notwithstanding (sequestration of all witnesses so they do hear or discuss each other's testimony), he or she is allowed to testify. This, of course, is remarkably useful, enabling the prosecution not only to clean up loose ends but to clear up technical aspects of the evidence of criminal conduct.

8. EDUCATING THE COURT

As with any case involving technical concepts and terms, the prosecutor can not expect the judge or jury to be schooled in the complexities of computer technology. This, coupled with the various meanings attached to words such as "system," "record," "file," and "software," requires careful explanation of the criminal act and evidence, and close control of expert testimony.

Issues must be defined in such a way that they are not easily distorted by defense counsel's tactics designed to confuse the trier of fact with computer jargon or unfounded technical assumptions. In this regard, the prosecutor must be alert to object when questions are posed to witnesses that are couched in technical terms that have varying interpretations in the industry and can be misleading if answered with a simple "yes" or "no." At the very least, he or she should be prepared on cross or redirect examination to elicit a clarification.

An expert witness should be called upon to show what knowledge or experience is required to effect the crime, followed by evidence showing that the defendant possessed this knowledge or experience (e.g., he was a computer programmer or accessed computers at work; he owned a PC; pertinent computer user manuals were seized in his home).

The use of visual aids is particularly important in educating the court regarding the nature of the (computer) beast, the steps involved in a complex computer process, or the flow of electronically transmitted and manipulated information. In-court demonstations with a PC or through remote access to a mainframe can be especially effective in showing how the crime was perpetrated. (See the section on Use of Demonstrative Evidence for a list of typical visual aids that should be considered.)

Of course, before one can hope to educate the court, one must first be educated. Since prosecutors are just as likely as judges and jurors to be unschooled in the technology, appropriate technical experts must be enlisted early on to not only assist in case preparation, but to serve as tutors on every issue involving technical concepts and terminology.

CHAPTER IV: COMPUTER-RELATED EVIDENCE LAW

This chapter is in the form of a legal brief, citing 133 cases on the law of computer-related evidence. */ It addresses this kind of evidence in the context of framing the language of a search warrant or discovery request, conducting a warrantless search, effecting a valid seizure, laying a proper foundation for admissibility, selecting appropriate witnesses and preserving the chain of custody.

In proving a computer crime, one must recognize that even if the prosecution's case in chief wisely avoids testimony embroiled in the complexities of computer technology, the defense strategy will likely depend on these very complexities to implant doubts favorable to the defendant in the minds of judges and jurors unschooled in computer terminology. To meet such a strategy, the prudent prosecutor needs to be prepared to fend off challenges to the trustworthiness of the government's evidence couched in technical jargon.

The following summarizes precautions that should be taken in seizing and preserving computer-related evidence, and in preparing to deal with highly technical issues:

- Computer-generated evidence must often be seized at a computer center or a remote terminal location where the evidence can be easily altered or destroyed (by writing over the electronic or magnetic storage medium or using an erasing device). Therefore, special attention should be given to whether exigent circumstances exceptions are applicable to preserve evidence. In this regard, care should be taken not to alert the perpetrator too soon, given the sophisticated techniques available to purge electronic or magnetic impulses.

- Because computer crime cases invariably involve seizing information residing on magnetic devices, satisfying the particularity requirements of a search warrant can be difficult - given that in a typical computer facility magnetic tapes and disks are indistinguishable by sight except to the extent they have been labeled externally. Extra precautions might be required to preserve the chain of custody.

- Technical terms in general, and computer-related terms in particular, are often susceptible to varying interpretations - including terms statutorily defined. This

---

*/ A Table of Authorities is included as Appendix B.

fosters inconsistencies offered by opposing technical experts, making it imperative that the prosecutor and investigators become familiar with these terms and their possible meanings in the context of the facts of the case.

- In attacking the veracity and relevance of computer products, the defense can challenge: 1) sources of input data; 2) processes employed to transcribe input to necessary form; 3) computer programs that create and maintain data files; 4) computer programs that access or manipulate data; 5) computer programs that produce printed or displayed output; and 6) even off-the-shelf operating systems software. Therefore, assistance of technicians familiar with these elements should be enlisted early in development of prosecution strategy.

- Of particular importance in presenting computer crime evidence is the choice of expert witnesses. Care should be taken to understand when a records custodian is needed rather than a computer programmer, and vice versa. Also, a computer programmer may not be the best choice to explain discrepencies in computer output that requires the expertise of a trained accountant or auditor. The witnesses should become familiar with statutory definitions of technical terms as well as with pertinent provisions of the Federal Rules of Evidence, and be prepared to reconcile possible conflicting technical interpretations.

As with any issues dealing with highly technical subject matter, judges and jurors depend heavily on counsel and their witnesses for explanations of concepts and terminology. Therefore, prosecutors of crimes dealing with computer-related evidence are well-advised to heed the above precautions and gain familiarity with pertinent court decisions.

1. SEARCH AND SEIZURE

a. Search Warrants

Federal Rules of Criminal Procedure, Rule 41(b), states in pertinent part:

> A warrant may be issued under this rule to search for and seize any (1) property that constitutes the commission of a criminal offense; ... or (3) property designed or intended for use or which is or has been used as the means of committing a criminal offense. ...

The Supreme Court, in Warden v. Hayden, 387 U.S. 294, 87 S.Ct. 1642 (1967), expanded the kinds of property to be seized under a warrant to include "mere evidence." 1/ Although Rule 41 is not to be interpreted as precluding issuance of a warrant to search for "evidence," United States v. Voegele, 246 F.Supp. 7 (D.Mich. 1972), Rule 41 was amended in 1972 to specifically authorize a warrant "to search and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States." [Emphasis added.] (The ability to seize mere evidence could be crucial in targeting computer-related items.)

(1) Intangible Property

Property is defined in Rule 41(h) "to include documents, books, papers and any other tangible objects." [Emphasis added.] This would seem to preclude seizure of "intangible" items such as information in electronic or magnetic form. However, in United States v. New York Telephone Co., 434 U.S. at 169, 98 S.Ct. at 370, the court held that:

> [a]lthough Rule 41(h) defines property "to include documents, books, papers and any other tangible objects," it does not restrict or purport to exhaustively enumerate all the items which may be seized pursuant to Rule 41. ... Rule 41 is not limited to tangible items. ...

The court was quite explicit in stating that "Rule 41 is sufficiently broad to include seizures of intangible items such as dial impulses recorded by pen registers as well as tangible items," and that the "definition of the term 'property' in the Rule places no limits on the objects of a proper search and seizure, but is merely illustrative." 434 U.S. at 170, 98 S.Ct. at 371, citing Link v. Wabash Railroad Co, 370 U.S. 626, 633 n. 8, 82 S.Ct. 1386, 1390 (1962) (applying the analogous provision of Fed.Rule Civ. Proc. 83).

1/ Citing Zurcher v. Stanford Daily, 436 U.S. 547, 98 S.Ct. 1970 (1978), United States v. New York Telephone Co., 434 U.S. 159, 98 S.Ct. 364 (1977). See also New Jersey v. T.L.O., 469 U.S. 325, 105 S.Ct. 733 (1985), Payton v. New York, 445 U.S. 573, 100 S.Ct. 1371 (1980).

The New York Telephone case was cited in United States v. Freitas, 800 F.2d 1451 (9th Cir. 1986), in upholding seizure of "information" obtained by surreptitious entry to merely observe the status of a suspected clandestine laboratory for an illegal drug. (Freitas also cited United States v. Kahn, 415 U.S. 143, 154-55, 94 S.Ct. 977, 983-84 (1974), which held that reasonable seizure of "conversations" does not violate the Fourth Amendment.)

In another pen register case, Michigan Bell Tel. Co. v. United States, 565 F.2d 385 (6th Cir. 1977), the court stated that "[c]ommon sense dictates that, as technology makes possible the seizure of intangibles, the courts should not limit the scope of Rule 41, but rather should interpret the rule so as to effectuate its purpose." Citing Katz v. United States, 389 U.S. 347, 355-56, 88 S.Ct. 507 (1967), and Osborn v. United States, 385 U.S. 323, 329-30, 87 S.Ct. 429 (1966), in which the Supreme Court held that valid federal warrants could be issued for search and seizure of intangible objects, namely, "oral communications."

In United States v. Horowitz, 806 F.2d 1222 (4th Cir. 1986), the FBI executed a search warrant having alleged probable cause to believe that government contract pricing information illegally sold by the defendant to his employer's competitor was stored on the competitor's computer magnetic storage devices. The warrant authorized search of a commercial building to seize property "including computer magnetic storage devices, computer keypunch cards and computer print-outs" containing the pricing information. The defendant had supplied the information from his home in another state through a computer terminal which he claimed gave him a reasonable expectation of privacy. His claim was based on the theory that the search at issue was not the search of the building, but of the "intangible space where images and sounds are recorded in a computer disc or tape," that this space was an "electronic filing cabinet" extension of his office, and that the government violated his expectation of privacy by "playing" the tapes without obtaining a second warrant.

The court disagreed, stating that the defendant "has proved no interest in the tapes, the information recorded on them, or in the premises upon which the tapes were stored," and that his willful disclosure of the information to the company "vitiates any reasonable expectation of privacy he may have once had." [Emphasis added.] Id., at 1226. Although the court did not find it necessary to consider whether the warrant was sufficient to encompass the seizure of property in the form of information recorded on magnetic tapes, it nevertheless believed the warrant to be adequate. Id., at 1226.

It goes without saying that value can be attached to intangibles such as information contained on magnetic storage media (e.g., tapes or disks). This can be particularly important in establishing a prima facie case for a specific offense. For example, in United States v. Berwitt, 619 F.2d 649 (7th Cir. 1980), lost profits to copyright holders of illegally copied record albums were properly presented to

the jury to establish the statutory minimum for a felony theft. 2/

(2) Particularity Requirement

"The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one 'particularly describing the place to be searched and the persons or things to be seized,'" therefore the scope of a search warrant is defined by the object of the search and the place where there is probable cause to believe it will be found. Maryland v. Garrison, ___ U.S. ___ , 107 S.Ct. 1013, 1017 (1987). Problems can arise when computer records are presumed to be included in specifying "records" as objects of a search without further description. However, the use of computers to store and maintain information has become so common that the lack of further description, although perhaps unwise, is not likely to be fatal in an otherwise valid seizure. 3/

In United States v. Musson, 650 F.Supp. 525 (D.Colo. 1986), the scope of a search warrant was limited to documents and "records" in the name of, or for the benefit of, named individuals and entities. The defendant challenged the seizure of computer disks not described in the warrant. The court upheld the seizure, adopting the following reasoning expressed in United States v. Reyes, 798 F.2d 380 (10th Cir. 1986) regarding seizure of a cassette tape: 4/

2/ The trial judge instructed the jury that what was stolen was "the fixation of recorded sounds, not the tangible component parts of the tapes," and allowed expert testimony regarding the valuation of the tapes in terms of lost profits to the copyright holders.

3/ Also, Fed. Rules of Evid., Rule 1001(1) states in pertinent part:

> "Writings and recordings" consist of letters, words, or numbers, or their equivalent, set down by ... magnetic impulse, mechanical or electronic recording, or other form of data compilation.

4/ The contention that the search warrant was overbroad was rejected because there was probable cause to believe that a complex scheme pervaded every aspect of the defendant's enterprise. Citing, United States v. Offices Known as Fifty State Distributing Co., 708 F.2d 1371 (9th Cir. 1983), cert. denied, 465 U.S. 1021, 14 S.Ct. 1272 (1984), United States v. Brien, 617 F.2d 299 (1st Cir. 1980), cert. denied, 446 U.S. 919, 100 S.Ct. 1854. See also United States v. Accardo, 749 F.2d 1477,1479 n.3 (11th Cir. 1985), cert. denied, ___ U.S. ___, 106 S.Ct. 314 (1985), United States v. Wuagneux, 683 F.2d 1343 (11th Cir. 1982), cert. denied, 464 U.S. 814, 104 S.Ct. 69, Andresen v. Maryland, 427 U.S. 463, 481 n.10, 96 S.Ct. 2737, 2749 n. 10 (1975).

> [I]n the age of modern technology and commercial availability of various forms of items, the warrant could not be expected to describe with exactitude the precise form the records would take. ... [I]n modern times because "business records are increasingly being kept on audio or video tape ... the law enforcement officers knew that the records they were seeking might well be contained on [the] tape."

However, other courts may choose to be less flexible in interpreting the use of the term "records" to include computer records.

The particularity requirement has been met in conjunction with a pervasive criminal scheme in warrants including objects to be seized described as "computer records or printouts relating to customer accounts," United States v. Sawyer, 799 F.2d 1494 (11th Cir. 1986), and as "computer hardware, floppy discs, tapes or other retention media, software-user manuals and access discs, (and) internal instructions for computer use." Rickert v. Sweeney, 813 F.2d 907 (8th Cir. 1987), where an IBM-PC computer and printer were seized. 5/ However, absent a pervasive criminal scheme, the courts are reluctant to relax the particularity requirement of a warrant that provides insufficient guidance to the search officer as to what items among many should be seized. Application of Lafayette Academy, Inc., 610 F.2d 1 (1st Cir. 1979). 6/

In Lafayette Academy, a warrant authorizing seizure of, inter alia, "computer tapes/discs, computer operation manuals, computer tape logs, Computer tape layouts, (and) computer tape printouts," limited only by the qualification that the items be evidence of violations of cited criminal fraud and conspiracy statutes, failed to "describe the 'things to be seized' with the particularity required by the fourth amendment." Id., at 3. The same conclusion was reached in Voss v. Bergsgaard, 774 F.2d 402 (10th Cir. 1985), where the warrant included for seizure "[o]ne Alpha Micro computer central processing unit, approximately four Alpha Micro computer terminals, computer printers, and computer manuals, logs, printout files, operating instructions, including coded and hand-written notations, and computer storage materials, including magnetic tapes, magnetic disks, floppy disks, programs, and computer source documentation." 7/

5/ Reversed and remanded for determination of the scope of probable cause in a sealed affidavit.

6/ Citing United States v. Klein, 565 F.2d 183 (1st Cir. 1977) regarding curing this deficiency with a properly incorporated affidavit.

7/ In Roberts v. United States, 656 F.Supp. 929 (S.D.N.Y. 1987), computer hardware, software and floppy disks were among items ordered returned under Rule 41(e). However, see United States v. Smith, 686 F.2d 234 (5th Cir. 1982), where a warrant directing seizure of "recorded videotapes, electronic video recording and playback equipment" was unsuccessfully challenged as being impermissibly general.

Corporate tax records are commonly maintained on computer storage media, prompting one court to make it clear that this does not result in added protection from scrutiny. See United States v. Davey, 543 F.2d 996 (2d Cir. 1976), where Internal Revenue Code § 7602, compelling production of "such books, papers, records, or other data ... as may be relevant or material to the inquiry," was interpreted to include records on computer tapes. The court stated that "[i]n this era of developing information-storage technology there is no reason to adopt a construction that would immunize companies with computer-based record-keeping systems from IRS scrutiny. Such would not be in keeping with Congress' intention in enacting the statute."

(3) Overbroad Warrants

In seizing large volumes of information, meeting the particularity burden becomes increasingly difficult as the dimension or extent of a search increases; however, "the magnitude of the search is not enough by itself to establish a constitutional violation." United States v. Heldt, 668 F.2d 1238, 1254 (D.C.Cir. 1981). The burden is lessened somewhat by the Supreme Court's recognition that "a complex criminal investigation may require piecing together '[l]ike a jigsaw puzzle' a number of items of evidence that may not appear incriminating when taken alone," United States v. Sawyer, supra, at 1508, citing Andresen v. Maryland, supra, at 481 n. 10, and by the Andresen court's admonishment that "[t]he complexity of an illegal scheme may not be used as a shield to avoid detection when the State has demonstrated probable cause to believe that a crime has been committed and probable cause to believe that evidence of this crime is in the suspect's possession." See also United States v. Wuagneux, supra, at 1349.

Despite this loosening of the particularity requirement, absent a showing that an illegal scheme pervades the whole enterprise, courts are reluctant to permit seizure of all the records of an organization - even if the alleged illegal activity constitutes "a large portion, or even the bulk" of the organization's operation. Voss v. Bergsgaard, supra, at 406. This judicial attitude presents a frustrating obstacle to obtaining a warrant to seize electronically stored records under certain circumstances. An example of such circumstances is the case where targeted records are being created by an employee of the provider of computer services unbeknownst to his employer, and these records are dispersed among hundreds of computer tapes or disks containing legitimate business records maintained for customers of the service.

Use of a computer expert with the cooperation of the service manager to surreptitiously determine how to identify the sought after records without disrupting the service runs the very high risk of alerting the suspect employee, resulting in "electronic erasure" of the evidence. On the other hand, seizure of all tapes and disks for the purpose of duplicating them for off-site analysis can require shutting down the service for many hours or days, causing a major disruption to the service and to the business operations of its customers. This dilemma is probably insurmountable, despite the flexibility attributed

to the particularity requirement in Wuagneux, supra, at 1349:

> ... It is universally recognized that the particularity requirement must be applied with a practical margin of flexibility, depending on the type of property to be seized, and that a description of the property will be acceptable if it is as specific as the circumstances and the nature of the activity under investigation permit.

See United States v. Musson, supra, at 535.

The magnitude of a search such as the one posited might possibly be reduced to a judicially acceptable size by limiting the warrant to a specific category of information maintained by the service provider, such as all tapes and disks containing records of accounts of specified types of customer organizations. This could result in making it possible to seize and duplicate the targeted tapes and disks in a few hours during a time that is least disruptive. Although the description of the items to be seized is still rather general, "in circumstances where detailed particularity is impossible 'generic language suffices if it particularizes the types of items to be seized.'" [Emphasis added.] Williams v. Kunze, 806 F.2d 594, 598 (5th Cir. 1986), citing United States v. Webster, 734 F.2d 1048, 1055 (5th Cir. 1984). Such a description would not be deemed overbroad so long as it is not broader than what was justified by the showing of probable cause upon which the warrant was based. Id., at 598-99.

(4) Warrantless Searches

It is well settled that there are circumstances in which a warrant requirement is inappropriate, in particular when "the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search." O'Conner v. Ortega, __ U.S. __, 107 S.Ct. 1492, 1499 (1987) (quoting Camara v. Municipal Court, 387 U.S. 523, 533, 87 S.Ct. 1727, 1733 (1967)). However, the courts have vigilantly circumscribed exceptions to the Fourth Amendment warrant clause, expressing "a strong preference for warrants," United States v. Leon, 468 U.S. 897, 914, 104 S.Ct. 3405, 3416 (1984), 8/ declaring that "in a doubtful or marginal case a search under a warrant may be sustainable where without one it would fall." Id., at 914 (quoting United States v. Ventresca, 380 U.S. 102, 106, 85 S.Ct. 741, 744, (1965) and citing Aguilar v. Texas, 378 U.S. 108, 111, 84 S.Ct. 1509, 1512 (1964)).

8/ With this caveat, the court went on to uphold the seizure of evidence based on reasonable reliance on a search warrant ultimately found to be invalid. As a general rule, the judgment of a magistrate is required to determine if there is probable cause for a search, and "[o]nly in exigent circumstances will the judgment of the police as to probable cause serve as sufficient authorization for a search." [Emphasis added.] Chambers v. Maroney, 399 U.S. 42, 51, 90 S.Ct. 1975, 1981 (1970).

Among the many valid grounds for a warrantless search (e.g., knowing, voluntary consent; incident to a lawful arrest; reasonable suspicion to "stop and frisk;" to protect or preserve life; etc.), the "exigent circumstances" exception based on threatened destruction of evidence is apt to become particularly common in investigating a computer crime. Given that objects identified for seizure will often include information contained on magnetic storage devices, there is the real threat that suspected magnetic tapes or disks will be erased, written over, altered or rendered unreadable - with little or no means of proving the targeted evidence ever existed.

In United States v. Simmons, 444 F.Supp. 500, 506 (E.D.Penn. 1978), a warrant issued to search the first story of a building included as objects of the search alphabetized computer printouts of traffic violators and computer tapes containing traffic violator information. The validity of the warrant was upheld based on sufficiency of the agents' affidavit. However, the court went on to state that even if the affidavit had been insufficient, there was a sufficient basis for a warrantless search based on the doctrine of exigent circumstances. This was because the agents had reliable information that documents were being destroyed inside the premises. 9/

Where there is reason to believe that incriminating evidence exists in a computer storage device, failure to discover it surreptitiously does not, in itself, obviate probable cause for a search warrant. In United States v. Benevento, 649 F.Supp. 1379, 1384, (S.D.N.Y. 1986), a warrant was issued based on an agent's expert opinion that the existence of computers and computer pulse telephone lines in the homes of significant drug traffickers might prove useful in managing data concerning criminal transactions. The subsequent search and seizure was upheld despite the absence of a statement by the agent that wiretaps on the computer pulse lines failed to pick up evidence of criminal activity. The court was influenced by the fact that the suspects had such computer pulse lines, which "supported the government's position that the Beneventos were sophisticated computer users who possessed the requisite skill and equipment to use computers in managing a criminal enterprise," making it "all the more likely that incriminating records might be found at their homes."

9/ Citing United States v. Montiell, 526 F.2d 1008, 1010 (2d Cir. 1975), United States v. Rubin, 474 F.2d 262, 268 (3rd Cir. 1973), cf. Chapman v. United States, 365 U.S. 610, 615, 81 S.Ct. 776 (1961), United States v. Jeffers, 342 U.S. 48, 52, 72 S.Ct. 93, 96 (1951), Johnson v. United States, 333 U.S. 10, 14-15, 68 S,Ct. 367 (1948). The court further held that issuance of a warrant before a seizure is effected does not alter the fact that a search was justified by exigent circumstances. United States v. Simmons, supra, at 506. Citing United States v. Allen, 566 F.2d 1193 (3rd Cir. 1977), United States v. Helberg, 565 F.2d 993 (8th Cir. 1977). See also United States v. Chadwick, 433 U.S. 1, 97 S.Ct. 2476 (1977), United States v. La Monte, 455 F.Supp. 952 (1978).

A common repository for one's personal effects (such as luggage) is "inevitably associated with the expectation of privacy." Arkansas v. Sanders, 442 U.S. 753, 762, 99 S.Ct. 2586, 2592 (1979). See also United States v. Chadwick, supra. It is not clear whether this is intended to extend to information contained on a computer tape or disk seized during a warrantless search and absent exigent circumstances for obtaining a printout of its contents. (Although, this is suggested by the dicta quoted earlier in Horowitz.) In United States v. Blair, 493 F.Supp. 398 (D.Md 1980), a warrantless search of a boat resulted in seizure of marijuana and a camera containing a roll of exposed but undeveloped film. When the film was developed, the prints disclosed scenes implicating the defendants in the marijuana smuggling scheme charged. (An analogy can be drawn with a seized computer tape or disk whose contents are later "printed out" by government agents.)

Concurring with the holding in various Circuits that "a warrant is required only if the defendant had a reasonable expectation of privacy" in a package or container, Id., at 416, and adopting the reasoning in the United States v. Hilton, 619 F.2d 127 (1st Cir. 1980), Id., at 416, the court held that although a roll of undeveloped film "may be a protected res under the rule of Arkansas v. Sanders," Id. at 416, the defendants must show they have a possessory or proprietary interest in the film for their motion to suppress to succeed. Id., at 417. Citing Rakas v. Illinois, 439 U.S. 128, 130-31 n.1, 99 S.Ct. 421, 423-24 (1978).

With the growing use of computers as a means of communicating and storing private messages, coupled with the proliferation of personal computers or PC's, investigators are cautioned against intruding on a suspect's expectation of privacy by seizing magnetic tapes or disks and later obtaining printouts without a warrant (leading to the suppression or return of important evidence). In United States v. Turk, 526 F.2d 654 (5th Cir. 1976), officers legally searched a car without a warrant, seizing cocaine and firearms. After arresting the car's occupants, the officers removed, among other objects, two cassette tapes from the car. Upon playing the tapes at the station, they discovered that one of them was a private telephone conversation between one of the individuals arrested and the defendant, Turk. Although the court found the seizure of the tape to be lawful, it ruled unlawful the warrantless playing of the tape. Id., at 666. 10/

In investigating computer crimes involving government employees, supervisors of the employees should be cautioned that "[s]earches and seizures by government employers or supervisors of the private property of their employees ... are subject to the restraints of the Fourth Amendment," O'Conner v. Ortega, supra, at 1497, citing New Jersey v.

10/ In addressing Turk's standing to suppress the evidence, the court stated that "when officials intrude into a tangible or intangible area in which an individual has a 'reasonable expectation of privacy,' that individual is a 'victim' of a search." [Emphasis added.] Id., at 663. Citing Alderman v. United States, 394 U.S. 165, 171-80, 89 S.Ct. 961 (1969), United States v. Hunt, 505 F.2d 931, 935-41 (5th Cir. 1974).

T.L.O., supra, at 334-35, providing such employees a reasonable expectation of privacy at least in their desk and file cabinets. Id., at 1499. See Doe v. U.S. Air Force, 812 F.2d 738 (D.C. Cir. 1987) (where during investigation of unauthorized use of a government computer, a computer diskette was seized from the plaintiff's desk at his duty station.)

b. Wiretapping and Electronic Surveillance

In Lopez v. United States, 373 U.S. 427, 441, 83 S.Ct. 1381, 1389 (1963), Chief Justice Warren, in a concurring opinion, warned that:

> " ... the fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual; ... indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments ... ."

However, the Lopez court pointed out that the Supreme Court has upheld electronic eavesdropping where devices have been used by government agents to overhear conversations that are otherwise beyond the reach of the human ear, insisting only "that the electronic device not be planted by an unlawful physical invasion of privacy." Lopez v. United States, supra, at 438-39 of 373 U.S., 1387-88 of 83 S.Ct. (See Katz v. United States, supra, where attaching an electronic listening and recording device to a telephone booth constituted a Fourth Amendment violation.)

Prior to enactment of Title I of the Electronic Communications Privacy Act of 1986, the courts strictly construed the definition of "intercept" set forth in 18 U.S.C. 2510(4) to exclude forms of surveillance that were not shown to be an "aural acquisition of the contents of any wire or oral communication through the use of any electronic mechanical or other device." 11/ To support its holding that a telex message is not an "aural acquisition" under Title III of the Omnibus Crime Control and Safe Streets Act, the Court in United States v. Gregg, 629 F.Supp. 958, 962 (W.D.Mo. 1986), cited United States v. Seidlitz, 589 F.2d 152, 157 (4th Cir. 1978), which held that Title III is inapplicable to interception of communication between two computer systems via telephone lines.

11/ United States v. New York Tel. Co., supra (citing congressional intent expressed in Senate Report No. 1079, 90th Cong., 2d Sess., at p. 90 (1968), which states that "[o]ther forms of surveillance are not within the proposed legislation" which "is intended to protect the privacy of the communication itself and not the means of the communication.") See also United States v. Giordano, 416 U.S. 505, 553, 94 S.Ct. 1820, 1844 (1974), United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986), United States v. Torres, 751 F.2d 875 (7th Cir. 1984) (where the court held that televising a man while he is silently making a bomb is a "visual observation," and not an "aural acquisition.")

To account for technological advances in communications, Title I of the Act amends § 2510(4) to read as follows:

> ... "intercept" means the aural or other acquisition of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device; [Emphasis added.]

This amendment makes it clear that, except as otherwise provided, "it is illegal to intercept the non-voice portion of a wire communication. For example, it is illegal to intercept the data or digitized portion of a voice communication." Sen. Rep. No. 99-541 at p. 13. 12/

New subsection (12) of § 2510 defines "electronic communication" to mean:

> ... any transfer of signs, signals, writings, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate or foreign commerce ...

This includes electronic mail, digitized transmissions, and video teleconferences. Sen. Rep. No. 99-541 at p. 14.

The increasing use of electronic mail as a means of personal communication can raise interesting interception questions. Such "mail" usually involves an electronic "mailbox" located in a third-party central computer queried with a remote terminal by the authorized addressee through any one of a number of telecommunications systems (including ordinary telephone lines). (The mailbox can also be located in storage media owned or controlled by either the sender or receiver.) In any case, an interception can be effected by tapping the mailbox, the telecommunications system, or the sending or receiving device (e.g., a remote terminal). A "transfer" has taken place from the moment a key is pressed to send information into an intermediate storage device (including a computer's main memory), resulting in that information being "transmitted" by a "wire, radio, electromagnetic, photoelectric or photooptical system."

Until case law develops around electronic mail intercepts, cases involving interception of telephonic conversations should be effective

---

12/ The Act further amends § 2516 to include as offenses for which an interception may be authorized "any felony violation of sections 2511 and 2512 (relating to intertception and disclosure of certain intercepting devices)," and adds a provision permitting government attorneys to authorize an application to a Federal judge for an order approving interception of electronic communications that "may provide or has provided evidence of a Federal felony."

in supporting legal arguments by analogy. 13/ For example, suppose a prosecutor wants to introduce the contents of a diskette containing electronic mail copied on the diskette by the recipient unbeknownst to the sender who assumed the mail was being printed, read and destroyed shortly after receipt. The mail discussed criminal activities and the interception had a criminal purpose. The recipient moves to have the evidence suppressed as an "aggrieved person" of an unlawful interception (i.e., made for the purpose of a criminal act). United States v. Underhill, 813 F.2d 105 (6th Cir. 1987) would be a case in point.

In Underhill, two of the defendants taped telephone conversations with their codefendants regarding illegal gambling operations. The codefendants were not aware of the taping, which was done to settle any future disputes about terms of betting transactions. The defendants that did the intercepting claimed that since the recordings were made for the purpose of committing a criminal act, the interception was unlawful therefore the evidence should be suppressed. One of the other defendants based his suppression motion on the fact that he did not consent to the interception of his conversations. The district court granted the suppression motions (based on the exclusionary provision of 18 U.S.C. § 2510).

The circuit court reversed. Agreeing that a private interception that otherwise would be lawful is rendered unlawful if made for the purpose of committing a criminal act, 14/ the court stated that "Title III provides protection to the victims of unlawful interceptions, not the perpetrators," 15/ and that "Congress did not intend

---

13/ However, it should be noted that new subsection 2518(c) "provides that with respect to the interception of electronic communications, the remedies and sanctions described in this chapter are the only remedies and sanctions available for nonconstitutional violations of this chapter involving such communications. In the event that there is a violation of law of a constitutional magnitude, the court involved in a subsequent trial will apply the existing Constitutuinal law with respect to the exclusionary rule," and not the rule in Title III of the Omnibus Crime Control and Safe Stre ts Act of 1968, to the interception of electronic communications. Sen. Rep. 99-541 at 23.

14/ Id., at 108. The court pointed out that the fact that the intercepted conversations discussed illegal gambling has no bearing on the legality of the interception; that "[i]t is settled that the legality of an interception is determined by the purpose for which the interception is made, not by the subject of the communications intercepted." Citing United States v. Truglio, 731 F.2d 1123, 1131 (4th Cir.), cert. denied, 469 U.S. 862, 85 S.Ct. 197 (1984).

15/ Citing Gelbard v. United States, 408 U.S. 41, 92 S.Ct. 2357 (1972), in which the court quoted Sen. Rep. No. 1097 to emphasize the point: "The perpetrator must be denied the fruits of his unlawful actions in civil and criminal proceedings." Id., at 50 of 408 U.S., 2362 of 92 S.Ct.

for § 2515 to shield the very people who committed the unlawful interceptions from the consequences of their wrongdoing." The court held that two of the defendants waived their right of privacy in these communications by their deliberate act of having them recorded, while the other was deemed a co-conspirator who had waived his right to privacy in communications used in furtherance of a conspiracy. Id., at 112.

The Underhill scenario could just as well have been an electronic mail interception, where instead of recording oral conversations on tape recorder cassettes, the interceptions were accomplished by directing electronic communications to a computer disk or diskette for storage.

An interesting electronic communication intercept analogy could be drawn from the Freitas case, supra. In that case, information obtained by surreptitious entry and mere observation of an illegal operation was held to be a valid seizure. It would seem that Freitas would apply to a search executed under a warrant where there is probable cause to believe that records of an illegal activity were being kept on the premises and, after a surreptitious entry, agents simply read information currently being displayed on a remote terminal video screen which turns out to be electronic mail used for a criminal purpose. The agents return later under an extension of the warrant to seize computer diskettes which contain more incriminating mail that the sender, a co-conspirator, was led to believe was being erased from the video screen immediately upon being read by the intended addressee without being copied onto diskettes.

The initial observation of the video screen would be considered a permissible seizure of "intangible" property under Freitas, while the reading of that and the other "mail" would be a valid intercept of electronic communications under the Underhill analogy. 16/

Seizing electronic communications can pose special problems, particularly if a computer or telecommunications equipment must be tampered with or removed. It is well settled that the courts are authorized - "in certain specified circumstances - to approve electronic surveillance without limitations on the means necessary to its accomplishment, so long as they are reasonable under the circumstances."

16/ The courts regard the showing of exigent circumstances required for a warrantless search to avoid notice, as here, as "more important in eavesdropping, with its inherent dangers, than that required when conventional procedures of search and seizure are utilized." Berger v. State of New York, 388 U.S. 41, 60, 87 S.Ct. 1873, 1884 (1967). See United States v. Costello, 610 F.Supp. 1450, 1465 (D.C.Ill. 1985) (which states that the legislative history of 18 U.S.C. §§ 2518(1)(c) and (3)(c) were enacted to satisfy the "special Facts" or "exigent circumstances" requirement of Berger.) Also, the particularity requirement is "especially great in the case of eavesdropping," requiring a recording device to be authorized "under the most precise and discriminate circumstances." Id., at 56 of 38 U.S., 1882 of 87 S.Ct.

[Emphasis added.] Dalia v. United States, 441 U.S. 236, 249, 99 S.Ct. 1682, 1689 (1979). In fact, it is acknowledged that "officers executing search warrants on occasion must damage property in order to perform their duty." Id., at 258 of 441 U.S., 1694 of 99 S.Ct.. However, it would seem that the courts would frown on damage caused by an agent to expensive computer and telecommunications equipment, or to valuable business records, because the agent failed to get proper technical assistance: (Not to mention the risk of losing important evidence!) The fact that the courts have registered approval of procedures "whereby law enforcement officers bring in lay experts to facilitate the on-site search for documents containing complex or technical subject matter" 17/ would seem to apply equally to the handling of sensitive electronic equipment and magnetic storage media.

Additionally, satisfying the edict of 18 U.S.C. § 2518(5) that an interception "shall be conducted in such a way as to minimize the interception of communication not otherwise subject to interception" can be particularly difficult regarding interception of electronic communications such as electronic mail. For example, identification of the communicating parties may be purposely routinely omitted in the communications - making it impossible to limit the interception to communications involving specified individuals. However, see Scott v. United States, 436 U.S. 128, 139-40, 98 S.Ct. 1717, 1724-25 (1978) (which required only that the monitoring be reasonable in light of all the facts and circumstances), cited by United States v. Van Horn, 789 F.2d 1492 (11th Cir. 1986).

Senate Report No. 99-541 at 16-17 provides the following clarification of congressional intent regarding Title I communications:

- An aural transfer means any transfer containing the voice at any point between and including the points of origin and reception.
- Voices transferred over a paging system are protected.
- Computer-generated or otherwise artificial voices are not aural, and thus not part of a wire communication, but part of an electronic communication.
- The transmission of data over the telephone is an electronic communication.
- In the transmission of a closed circuit television picture of a meeting using wires, microwaves or another method of transmission, the transmission itself is an electronic communication.

17/ United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), citing Forro Precision, Inc. v. IBM Corp., 673 F.2d 1045, 1053-54 (9th Cir. 1982), United States v. Wuagneux, supra, at 1353.

- Interception of a closed circuit television picture at any point without consent or a court order is an unlawful interception.

- If law enforcement officials install their own camera and create their own closed circuit television picture of a meeting, the capture of the video image is not an interception because their is no intercept of the contents of the electronic communication. However, interception of the audio portion of the meeting constitutes interception of an oral communication.

c. Seizure of Stored Wire and Electronic Communications

Title II of the Electronic Communications Privacy Act is modeled after the Right of Financial Privacy Act, 12 U.S.C. 3401 et seq., "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." Sen Rep. 99-541 at 3. To this end, the Act, inter alia, makes it unlawful to: 1) intentionally access without authorization a facility through which an electronic communication service is provided; or 2) intentionally exceed an authorization to access such a facility - and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.

New Section 2510(17) defines "electronic storage" to mean: 18/

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
>
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; ...

and Section 2710(2) defines the term "remote computing service" to mean "the provision to the public of computer storage or processing services by means of an electronic communications system." 19/

18/ "The term covers storage within the random access memory of a computer as well as storage in any other form including storage of magnetic tapes, disks or other media. Thus, for example, section 2701's prohibitions against unauthorized access to wire or electronic communications while they are in electronic storage would prohibit unauthorized access to such a communication while it is stored on magnetic tape or disk. The section 2701 prohibitions similarly would apply to information held on magnetic tape or disk pursuant to an agreement to provide remote computing services." Sen. Rep. 99-541 at 13.

19/ Section 2710 adopts the definitions of terms in § 2510 of Chapter 119 as those terms are used in Chapter 121.

A remote computing service, as defined by the Act, retains customer deposits of personal or proprietary information in electronic storage, along with records of these deposits, in much the same way that a bank retains customer deposits of money (or its equivalent) and associated records. Prior to enactment of the Financial Privacy Act, the Supreme Court held that a bank customer had no protected Fourth Amendment interest in his bank records - following the established principle that communication to a third party of even confidential information results in forfeiture of Fourth Amendment rights in that information. United States v. Miller, 425 U.S. 435, 440, 96 S.Ct. 1619, 1622 (1976). The Miller court further concluded that "the issuance of a subpoena to a third party does not violate the rights of a defendant even if a criminal prosecution is contemplated at the time the subpoena is issued." Id., at 444 of 425 U.S., 1624 of 96 S.Ct. 20/

The Financial Privacy Act was enacted in response to the Miller decision, according customers of financial institutions certain rights to be notified and to challenge administrative subpoenas of financial records. SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 745, 104 S.Ct. 2720, 2727 (1984). However, absent a statutory provision to the contrary, a government agency is not required to notify the "target" of a nonpublic investigation when a subpoena is issued to a third party. Id., at 742-43 of 467 U.S., 2725 of 104 S.Ct. 21/

Section 2704 of the Electronic Communications Act provides for requiring the remote computing service provider to create a backup copy of the contents of electronic communications sought by the government in order to safeguard against destruction of or tampering with evidence. After-the-fact notice to the subscriber or customer that a backup was made is required, unless notice is delayed pursuant to § 2705(a). It is significant to note that § 2705(b) clarifies the "target" notification issue settled in O'Brien regarding a third party subpoena by providing under specified circumstances that:

> [a] governmental entity ... may apply for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed ... not to notify any other person of the existence of the warrant, subpoena, or court order. ... [Emphasis added.]

20/ Citing California Bankers Assn. v. Schultz, 416 U.S. 21, 53, 94 S.Ct. 1494, 1513 (1974), Donaldson v. United States, 400 U.S. 517, 537, 91 S.Ct. 534, 545 (1971).

21/ See also In Re Grand Jury Subpoena (Maltby), 800 F.2d 981, 983 (9th Cir. 1986), Spannaus v. Federal Election Com'n, 641 F.Supp. 1520, 1528 (S.D.N.Y. 1986) (holding that there was no notice requirement when a discovery request is issued to a third party).

Given the ease with which information can be deleted from a computer file by the "target" of an investigation or his confederates (either on request or by direct access), these provisions can prove to be of particular import for agents seizing electronic communications retained by a remote computing service.

2. DISCOVERY

Federal Rule of Criminal Procedure, Rule 16(a)(1)(C) provides for pretrial disclosure of evidence in the form of documents and tangible objects by the government, while Rule 16(b)(1)(A) provides for similar disclosure by the defendant. Rule 16 "establishes the Government's reciprocal right of pretrial discovery," which "arises only after the defendant has successfully sought discovery" under the rules. United States v. Nobles, 422 U.S. 225, 95 S.Ct. 2160 (1975). 22/

The courts have long encouraged pretrial discovery of computer programs and related materials, recognizing that the use of "computerized data" can impede effective cross-examination "because of the difficulty of knowing the precise methods employed in programming the computer as well as the inability to determine the effectiveness of the persons responsible for feeding data into the computer." United States v. Cepeda Penes, 577 F.2d 754, 760-61 (1st Cir. 1978), citing United States v. Dioguardi, 428 F.2d 1033, 1038 (2d Cir. 1970), cert. denied, 400 U.S. 825, 91 S.Ct. 50 (1970). 23/

In Dioguardi, the court strongly admonished the prosecutor for failure to provide the defendant with a pretrial opportunity to examine a computer program used to analyze data and produce printouts that were the basis for a government witness' testimony:

22/ However, see United States v. Escremera, 531 F.2d 1103 (2d Cir. 1976), cert. denied, 425 U.S. 979, 96 S.Ct. 2184 (1976), where during a pretrial hearing, the government, in response to a motion for discovery, consented to the production of evidence rather than awaiting a court order and later moved for reciprocal discovery against the defendant. The court upheld the government's motion, stating that "[t]he government's voluntary turnover of desired material to defendant must be deemed to have been based upon the implied condition that the defense would reciprocate, if necessary, at a later date." Citing cf. United States v. Milano, 443 F.2d 1022, 1027, n. 1 (10th Cir. 1971), cert. denied, 404 U.S. 943, 92 S.Ct. 294 (1971). See also United States v. Thuna, 103 F.R.D. 182 (D.C.Puerto Rico 1984), where reciprocal discovery was upheld based on defendant's informal requests during meetings at which Rule 16(a)(1)(C) materials were produced by the government.

23/ See also United States v. Liebert, 519 F.2d 542, 547 (3rd 1975), citing Manual for Complex Litigation in 1 J. Moore Federal Practice, pt. 2, § 2.715 (2d ed. 1974), United States v. Russo, 480 F.2d 1228 (6th Cir. 1973), United States v. Dioguardi, supra, Chesapeake and Ohio Ry. Co. v. United States, 704 F.2d 373, 379 (7th Cir. 1983), citing Dioguardi, Perma Research and Development v. Singer Co., 542 F.2d 111, 125 (2d Cir. 1976), citing Dioguardi and Russo, City of Cleveland v. Cleveland Electric Illuminating Company, 538 F.Supp. 1257, 1266 (N.D.Ohio 1980), citing Cepeda Penes.

> ... the defendants were entitled to know what operations the computer had been instructed to perform and to have the precise instruction that had been given. It is quite incomprehensible that the prosecution should tender a witness to state the results of a computer's operations without having the program available for defense scrutiny and use on cross-examination if desired. We place the Government on the clearest possible notice of its obligation to do this and also of the great desirability of making the program and other materials needed for cross-examination of computer witnesses, such as flow-charts used in the preparation of the programs, available to the defense a reasonable time before trial. See United States v. Kelly, 420 F.2d 26 (2d Cir. 1969). 24/

In reaching the same conclusion, the Russo court relied on United States v. Stifel, 433 F.2d 431 (6th Cir. 1970) and United States v. Kelly, supra (both of which involved neutron activation tests rather than computer programs), and quoted the Manual for Complex and Multidistrict Litigation:

> It is essential that the underlying data used in the analyses, programs and programming method and all relevant computer inputs and outputs be made available to the opposing party far in advance of trial. This procedure is required in the interest of fairness and should facilitate the introduction of admissible computer evidence. Such procedure provides the adverse party and the court with an opportunity to test and examine the inputs, the program and all outputs prior to trial. (p. 88).

United States v. Russo, supra, at 1241, 1243. In ruling against the defendant's objection to admission of "computerized statistics," the court concluded that "appellant had ample notice of the nature of the statistical evidence which the prosecution planned to use and chose to attempt to discredit this evidence by means of cross-examination rather than availing himself of discovery and use of expert witnesses of his own choosing." Id., at 1243.

24/ Despite the strong reproachment, the court held that the government's conduct was not reversible error because there was no "appreciable risk that prejudice resulted." See also United States v. Robinson, 783 F.2d 64, 69 (7th Cir. 1986) (where the government's failure to produce a computer program was insufficient by itself to require exclusion of chemical test results or to fatally prejudice the defendant's case), citing United States v. Bastanipour, 697 F.2d 170, 176-77 (7th Cir. 1982), cert. denied, 460 U.S. 1091, 103 S.Ct. 1190 (1983), United States v. Koopmans, 757 F.2d 901, 906 (7th Cir. 1985), citing Bastanipour.

In addition to considering the pretrial discovery (or lack thereof) issue, the Dioguardi court rejected the defendant's contention that the computer program was producible under the Jencks Act 25/ after direct examination of the witness (because it did not qualify as a "statement or report" as defined by the Act). United States v. Dioguardi, supra, at 1038, citing Palermo v. United States, 360 U.S. 343, 79 S.Ct. 1217 (1959). Also, the Jencks Act does not apply to computer printouts and programs used to complete "peer-group" analyses prepared for and presented at trial by investigators. United States v. Alexander, 789 F.2d 1046, 1049 (4th Cir. 1986), citing United States v. Dioguardi, supra, at 1037-38, and failure to specifically request production of computer materials before trial results in waiver of a Rule 16 claim. Id., at 1049, citing United States v. Russo, supra, at 1241-43. 26/

Prosecutors are cautioned that information produced in the ordinary course of government business does not automatically transform into attorney work-product when subjected to analysis by specially designed computer programs during an investigation. For example, in State of Colo. v. Schmidt-Tiago Const. Co., 108 F.R.D. 731 (D.Colo. 1985), the defendant filed a motion to compel discovery of computer printouts that the state claimed were privileged as attorney work-products under Civ. Rule of Proc. 26(b). Despite the fact that the information in the printouts were the result of a "complex, state of the art computerized analysis of bids for contracts on highway construction projects," the court concluded that "the computer program established by the department of highways and the Attorney General was for the use in the regular course of business."

The state's computer printouts were deemed discoverable because the information was "simply computerized for easier reading and evaluation." Id., at 734-35. Because of this characterization, it is likely that the court would have reached the same conclusion under Crim. Rule of Proc. 16(a)(2). (The court also noted that the state failed to specifically designate what documents are work-product, having raised both a work-product and attorney-client privilege. Id., at 733-34. The court found no facts to support the attorney-client privilege.)

25/ United States Code Title 18, Section 3500 (The Jencks Act) provides in pertinent part that in a criminal prosecution, "[a]fter a witness called by the United States has testified on direct examination, the court shall, on motion of the defendant, order the United States to produce any statement ... of the witness in the possession of the United States which relates to the subject matter as to which the witness has testified."

26/ Although the defendant "might have challenged the peer-group testimony at trial by objecting to its character as computer study evidence and thereby requiring the government to introduce the underlying data and programs as a foundation for the study results, but failed to do so." Id., at 1049. (Defendant's claim that the material was exculpatory as Brady material was also rejected by the court. Id., at 1050.)

A motion for discovery of computer materials can be quite technical, requiring the assistance of a computer professional for proper descriptive language. The following is an extract from such a motion filed by the Department of Justice under Crim. Rule of Proc. 16 in United States v. United States Gypsum Company, et al., Crim. Action No. 1042-73, Supplemental to Civ. Action No. 8017:

> With respect to all reports, summaries, charts, tables and statistical analyses which respondents intend to produce at trial prepared in whole or in part through the use of computer processing, petitioner further moves this court for an order directing the respondents to produce for inspection and copying at least (90) days in advance of trial the following:
>
> 1. All data bases used in the creation of reports, summaries, charts, tables or statistical analyses, including but not limited to all relevant business master files, transaction files and any special files created for the purpose of preparing said reports, summaries, charts, tables or statistical analyses. For all special files, each file's record selection criteria shall be furnished. Such data bases should be furnished, if available, on 9-track magnetic tape and recorded at a density 1600 B.P.I. [bits per inch]. Each reel of magnetic tape should be externally marked so that identification of the reel with the characteristics produced pursuant to point 2 infra is expedited.
>
> 2. All books, papers, documents and tangible objects which describe the physical attributes of the reel of magnetic tape containing the data bases requested in paragraph 1, including:
>
> (Detailed technical items listed.)
>
> 3. All books, papers, documents and tangible objects which describe the structure of records in the data bases requested in Paragraph 1, including:
>
> (Detailed technical items listed.)
>
> 4. All books, papers, documents and tangible documents which describe the data processing equipment (hardware) at any data processing facility used by respondents for any processing of the data bases requested in Paragraph 1, including:
>
> (Detailed technical items listed.)
>
> 5. All books, papers, documents and tangible objects which describe the computer programs (software) used to process the data bases requested in Paragraph 1, including:
>
> (Detailed technical items listed.)

(For a complete reprint of this and other motions and pleadings, see Young, Kris and Trainor, Editors, Use of Computers in Litigation, p. 383, a Professional Education Publication of the American Bar Association (1979).)

3. ADMISSIBILITY

The electronic recording of information means to store computer processed information in storage media such as magnetic disks or tapes, where the information is represented in the storage media in the form of "machine-readable" codes or patterns imprinted on magnetizable surfaces by electronic impulses. Although the information is stored or "filed" electronically in these media, the files themselves are in reality magnetic files. In any case, such files are considered "writings or recordings" in Federal courts. 27/

Magnetic files are called "machine-readable" because they can be copied into a computer for processing and interpreted for printing out in human readable form on paper or microfilm, or on a video display screen (or even converted to audio form through a "talking" terminal). Admissibility of these files (or printouts thereof) can present special problems in establishing their genuineness or trustworthiness.

a. The Best Evidence Rule

Before the courts, an "original" of a record is the record itself, which can pose a problem regarding computer-produced records in the face of the "best evidence rule." This rule, rigidly applied in the absence of a qualifying rule or statute, precludes admissibility of anything but the original document to prove its content. Recognizing the impracticality of the rule when applied to computer files, many states and the Federal government have adopted definitions that consider computer printouts as originals, provided that they have been shown to accurately reflect the information in the magnetic files. 28/

27/ Fed. Rules of Evid., Rule 1001(1) states in pertinent part:

> "Writings and recordings" consist of letters, words, or numbers, or their equivalent, set down by ... magnetic impulse, mechanical or electronic recording, or other form of data compilation.

28/ Fed. Rules of Evid., Rule 1001(3) states in pertinent part:

> An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it ... . If 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.

Absent such a rule, at least one court has taken the view that printouts of records stored in magnetic media are admissible because they are "unavailable and useless except by means of the printout sheets." King v. State ex. rel. Murdock Acceptance Corp., 222 So.2d 393, 398 (Miss. 1969).

Fed. Rule of Evid. 1002 states that "[to] prove the contents 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." The Federal Rules do indeed provide otherwise, resulting in considerable relaxation of the best evidence rule. 29/ In addition, the courts have long recognized admissibilty of computer printouts as probative evidence, subject to the same scrutiny for trustworthiness as business records:

> [a] major "witness" confronting (the defendant) will be computer printouts indicating that the IRS has no record of having received his returns. ... The introduction of a computer printout is admissible in a criminal trial provided that the party offering the computer information is trustworthy and the opposing party is given the same opportunity to inquire into the accuracy of the computer and its input procedures as he has to inquire into the accuracy of written business records. 30/

29/ With regard to duplicates and public or official records, the rule states in pertinent part:

> A "duplicate" is a counterpart produced by the same impression as the original, ... or by mechanical or electronic re-recording, ... or by other equivalent techniques which accurately reproduce the original. [Emphasis added.] Fed. Rule of Evid. 1001(4).
>
> 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. Fed. Rule of Evid. 1003.
>
> The contents of an official record, or of a document authorized to be filed and actually recorded or filed, including data compilations in any form, if otherwise admissible, may be proved by copy, certified by a witness who has compared it with the original. If a copy which complies with the foregoing cannot be obtained by the exercise of reasonable diligence, then other evidence of the contents may be given. [Emphasis added.] Fed. Rule of Evid. 1005.

These rules would seem to consider as duplicates, or copies of official records, additional printouts of the same information contained in a magnetic file produced at different times (as well as carbon, photostatic or xerographic copies).

30/ United States v. Liebert, supra, at 548, citing United States v. De Georgia, 420 F.2d 889 (9th Cir. 1969) (where computerized records of a car rental company were admitted for the purpose of showing that a particular automobile was not rented during a particular time period).

b. Authentication

Any tangible thing offered as evidence is subject to challenge regarding its genuineness. 31/ Computer-produced evidence is no exception. Fed. Rule of Evid. 901(b) lists examples of authentication requirements. Of particular note regarding computer evidence is example (9):

> Evidence describing a process or system used to produce a result showing that the process or system produces an accurate result. [Emphasis added.]

This would seem to particularly include evidence describing a computer "process" or "system" to show that a computer printout is accurate.

In United State v. Croft, 750 F.2d 1354, 1364 (7th Cir. 1984), it was not error when the district court failed to allow the defendant access to the computer program that produced the printouts admitted into evidence under Rule 803(6). The court noted that the printouts were "simply computer compilations of payroll data...(containing) no calculations or studies that relied upon a complex and intricate computer program. Instead, the relevant payroll evidence was simply transferred from payroll data sheets to a computer disk for convenient storage in the computer and easy retrieval." Id., at 1365. The court was satisfied that the foundation laid by testimony of the person responsible for maintaining and supervising the payroll process established trustworthiness of the input data. Id., at 1365 n. 7. Hence, the genuineness of the printout was accepted as equivalent to the genuineness of the input data, and the "computer program was of little if any importance." 32/ Id., at 1365.

Similarly, in United States v. Vella, 673 F.2d 86, 90 (5th Cir. 1982), the defendant attacked admissibility of telephone bills prepared with computers, arguing that failure to establish that the computers were in proper working order denied him of confrontation rights. The court held that "computer evidence is not intrinsically unreliable," citing United States, v. Fendley, 522 F.2d 181,187 (5th Cir. 1975), Olympic Insurance Co. v H. D. Harrison, Inc., 418 F.2d 669, 670 (5th Cir. 1969), and that "failure to certify the brand or proper operating condition of the machinery involved does not betray a circumstance of preparation indicating any lack of trustworthiness." (A telephone company employee had testified as to the precise manner in

---

31/ Fed. Rule of Evid. 901(a) states:

> The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

32/ Apparently the court reasoned that, in light of the description of the way the data was processed, in these particular circumstances the printouts spoke for the accuracy of the computer program.

which the billing data are compiled, and the defense had previously examined the employee outside the jury's presence.)

The Croft and Vella analyses clearly distinguish between authenticity or genuineness of computer printouts and trustworthiness of the process that produces them, a distinction that is explicitly supported by the following statement in United States v. Downing, 753 F.2d 1224 (3rd Cir. 1985):

> ... The question whether "a particular machine works as intended" is a question distinct from one directed toward "the authentication of a process generally." Saltzburg & Redden, Federal Rules of Evidence Manual 702 (3d ed. 1982). Rule 901(b)(9) speaks only to the former question. See McCormick on Evidence 885 n. 6 (3rd ed. 1984) ("The emphasis of Rule 901 is upon showing that the offered item (e.g., computer printout) is what it is claimed to be, i.e., that it is genuine ... rather than that what is in the (computer) is correct.").

(It is important to note that in both Croft and Vella, a proper foundation was laid for introduction of the printouts.)

As with other kinds of evidence, admissibility by the court of computer-produced evidence is not tantamount to a mandatory presumption of trustworthiness. In rejecting the defendant's claim, the Vella court simply found that his "arguments for a level of authentication greater than that regularly practiced by the company in its own business activities goes beyond the rule and its reasonable purpose to admit truthful evidence. ... At best, the arguments go to the weight that should be accorded the evidence, not its admissibility." Citing United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977), cert. denied, 434 U.S. 940, 98 S.Ct. 432 (1978). See also Zenith Radio Corporation v. Matsushita Electric Industrial Co., Ltd., et al., 505 F.Supp. 1190, 1219 (E.D.Penn. 1980), citing United States v. Goichman, 547 F.2d 778, 784 (3rd Cir. 1976) (requiring only a prima facie showing that a document offered into evidence is what its proponent claims, whereupon the burden of going forward with respect to authentication shifts).

c. Hearsay

Fed. Rule of Evid. 801(c) defines hearsay as:

> ...a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted.

A "statement" is defined to include a written assertion. Fed. Rule of Evid. 801(a). Hearsay is not admissible in Federal court except as provided by the Federal Rules of Evidence "or by other rules prescribed by the Supreme Court pursuant to statutory authority or by Act of Congress." Fed. Rule of Evid. 802.

As was pointed out earlier, a computer printout (or output readable by sight) is regarded as an original writing or recording. Fed. Rule of Evid. 1001(3). In any case, it is an out-of-court "statement" and if offered to prove the truth of its contents it is considered hearsay and treated accordingly regarding its admissibility. As with other "writings" or "records," computer printouts not offered to prove the truth of their contents are not hearsay. (For example, if offered to support testimony that incomplete information was knowingly submitted for computer processing. United States v. Evans, 572 F.2d 455 (5th Cir. 1978), cert. denied, 439 U.S. 870, 99 S.Ct. 200 (1978).)

Among the exceptions enumerated in Fed. Rule of Evid. 803, Rule 803(6) regarding records of a regularly conducted activity is particularly relevant to computer printouts, given the common practice of maintaining business records on computers. (This rule and the related Business Records Act are discussed in a separate subsection.) The other exceptions have no special significance regarding computer-produced evidence.

d. Business Records or Records of a Regularly Conducted Activity

The Business Records Act, 28 U.S.C. § 1732, provides for admission of records produced in the regular course of business. The Act states in pertinent part:

> If any business, institution, member of a profession or calling, or any department or agency of government, in the regular course of business or activity has kept or recorded any memorandum, writing, entry, print, representation or combination thereof, of any act, transaction, occurrence, or event, and in the regular course of business has caused any or all of the same to be recorded, copied, or reproduced by any...process which accurately reproduces or forms a durable medium for so reproducing the original, the original may be destroyed in the regular course of business unless its preservation is required by law. Such reproduction, when satisfactorily identified, is as admissible in evidence as the original in any judicial or administrative proceeding whether the original is in existence or not... . The introduction of a reproduced record...does not preclude admission of the original. ... 33/

In Russo, appellant attacked the admission under §1732 of an annual statistical computer printout produced by Blue Shield of Michigan, claiming, inter alia, that it did not qualify as a business record

---

33/ It should be noted that "[t]he best evidence rule has repeatedly been held inapplicable to records admitted under the Business Records Act." United States v. Miller, 500 F.2d 751 (5th Cir. 1974), citing United States v. Anderson, 447 F.2d 833, 839 (8th Cir. 1971), United States v. Vandersee, 279 F.2d 176, 180 (3rd Cir. 1960), United States v. Kimmel, 274 F.2d 54, 57 (2d Cir. 1960).

and that it was not prepared at the time the acts it purports to describe were performed or within a reasonable time thereafter. In upholding admissibility of the printout, the court stated:

> Computer printouts are not mentioned in the Federal Business Records Act. However, no court could fail to notice the extent to which businesses today depend on computers for a myriad of functions. Perhaps the greatest utility of a computer in the business world is its ability to store large quantities of information which may be quickly retrieved on a selective basis. Assuming that properly functioning computer equipment is used, once the reliability and trustworthiness of the information put into the computer has been established, the computer printouts should be received as evidence of the transactions covered by the input.
>
> .....
>
> It would restrict the admissibility of computerized records too severely to hold that the computer product, as well as the input upon which it is based, must be produced at or within a reasonable time after each act or transaction to which it relates. At 1240.
>
> .....
>
> The Act should never be interpreted so strictly as to deprive the courts of the realities of business and professional practices. Harris v. Smith, 372 F.2d 806 (8th Cir. 1967). 34/

See also United States v. Scholle, supra, at 1124, United States v. Fendley, supra, at 187, United States v. De Georgia, supra, United States v. Kim, 595 F.2d 755, 764 f.n. 43 (D.C. Cir. 1979).

Fed. Rule of Evid. 803(6) provides in pertinent part:

> The following are not excluded by the hearsay rule, even though the declarant is available as a witness:
>
> .....
>
> (6) Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and

---

34/ United States v. Russo, supra, at 1239-40.

> if it was the regular practice of that business activity to make a memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of the information or the method or circumstances of preparation indicate lack of trustworthiness. [Emphasis added.]

As with the Business Records Act, "computer data compilations may constitute business records for purposes of Fed.R.Evid. 803(6) and may be admitted at trial if a proper foundation is established." United States v. Croft, 750 F.2d, supra, at 1364. 35/ The common standard for determining admissibility of computer records under Rule 803(6) follows: "Computer business records are admissible if (1) they are kept pursuant to a routine procedure designed to assure their accuracy, (2) they are created for motives that tend to assure accuracy (e.g., not including those prepared for litigation), (3) they are not themselves mere accumulations of hearsay." United States v. Sanders, 749 F.2d 195, 198 (5th Cir. 1984). 36/ (It is noteworthy that the Scholle court used the specific inclusion of "data compilation" in Rule 803(6) to support the contention that computer printouts are covered under the Federal Business Records Act. United States v. Scholle, supra, at 1124.)

In rejecting the defendant's argument that the computer printouts in question were records prepared for litigation (hence not business records), the Sanders court pointed out that although the printouts themselves may have been made in preparation for litigation, the data contained in the printouts were the results of business transactions that were neither added to nor modified after the transactions took place. The court concluded that "[i]t is not necessary that the printout itself be ordered in the ordinary course of business, at least when the program that calls forth the data only orders it rather than sorting, compiling or summarizing the information." [Emphasis added.] United States v. Sanders, supra, at 198.

35/ Citing United States v. Young Bros., Inc., 728 F.2d 682, 694 (5th Cir. 1984), cert. denied, ___ U.S. ___, 105 S.Ct. 246 (1984), Rosenburg v. Collins, 624 F.2d 659,665 (5th Cir. 1980), United States v. Scholle, supra, at 1124-25, Annot., 7 A.L.R.4th 8, 15 (1981).

36/ Quoting from Capitol Marine Supply, Inc. v. M/V ROLAND THOMAS II, 719 F.2d 104 (5th Cir. 1983). See also United States v. Miller, supra, 500 F.2d at 754, citing Sabatino v. Curtiss v. National Bank of Miami Springs, 415 F.2d 632, 637 (5th Cir. 1969).

4. LAYING A PROPER FOUNDATION

Laying a foundation is "the practice or requirement of introducing evidence of things necessary to make further evidence relevant, material or competent... ." Black's Law Dictionary. Fed. Rule of Evid. 104 states in pertinent part:

> (a) Questions of admissibility generally
>
> Preliminary questions concerning the qualification of a person to be a witness, the existence of a privilege, or the admissibility of evidence shall be determined by the court, subject to the provisions of subdivision (b). In making its determination it is not bound by the rules of evidence except those with respect to privileges.
>
> (b) Relevancy conditioned on fact
>
> When the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfullment of the condition.
>
> .....
>
> (e) Weight and credibility
>
> This rule does not limit the right of a party to introduce before the jury evidence relevant to weight or credibility.

Heretofore, discussions centered on admissibility of computer-produced evidence in terms of the intrinsic nature or character of the evidence. Laying a foundation that will qualify the evidence as being what it is purported to be can be an even greater burden to overcome.

Business records exceptions notwithstanding, laying a foundation for computer-produced records can be particularly difficult:

> Even where the procedure and motive for keeping business records provide a check on their trustworthiness..., the complex nature of computer storage calls for a more comprehensive foundation. Assuming properly functioning equipment is used, there must be not only a showing that the requirements of the Federal Business Records Act have been satisfied, but in addition the original source of the computer program must be delineated, and procedures for input control including tests used to assure accuracy and reliability must be presented. 37/

37/ United States v. Scholle, supra, at 1125.

However, a more recent decision downplays the difference between computer records and other records, which probably reflects the increased use of computers in creating and maintaining business records:

> ... While the suggestion has been made that there are unique foundation requirements for the admission of computerized business records under 803(6), see generally United States v. Scholle. ... this court has previously held that "computer data compilations ... should be treated as any other record of regularly conducted activity." 38/

Russo summarizes what is required in laying a proper foundation for computer-produced business records:

> ... [T]he foundation for admission of (computerized records) consists of showing the input procedures used, the tests for accuracy and reliability and the fact that an established business relies on the computerized records in the ordinary course of carrying on its activities. The (opposing) party then has the opportunity to cross-examine concerning company practices with respect to the input and as to the accuracy of the computer as a memory bank and retriever of information. ... [T]he court (must) " be satified with all reasonable certainty that both the machine and those who supply its information have performed their functions with utmost accuracy." ... [T]he trustworthiness of the particular records should be ascertained before they are admitted and ... the burden of presenting an adequate foundation for receiving the evidence should be on the parties seeking to introduce it rather than upon the party opposing its introduction. ... 39/

a. Witness Selection

Care must be taken to select a witness "competent" to testify in laying the foundation for admissibility of computer-produced evidence. The court in Fendley emphasized that the "preparer" of a record is not required to establish its authenticity: 40/

38/ United States v. Vella, supra, at 90, citing Rosenburg v. Collins, supra, at 665. (For an extensive argument calling for a more comprehensive burden to qualify computer records, see Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 7 Computer/Law Journal 23, 70 (Summer 1986).

39/ United States v. Russo, supra, at 1241, citing De Georgia, supra. See also, United States v. Weatherspoon, 581 F.2d 595, 598 (7th Cir. 1978).

40/ United States v. Fendley, supra, at 185.

> ... A witness laying the foundation for admissibility of a document as a business record need not have been the preparer of the document. United States v. Gremillion, 464 F.2d 901, 906 (5th Cir. 1972) -- for indeed this Court stated that:
>
> "Section 1732 was adopted in part to eliminate the requirement that the entrant appear to authenticate the record."
>
> United States v. Miller, supra, 500 F.2d at 754.
>
> "[T]he person who actually keeps the books and records and makes the entries need not testify if a person does testify who is in a position to attest to the authenticity of the records." United States v. Dawson, 400 F.2d 194, 199 (2d Cir. 1968). ... [N]othing in the Business Records Act requires either that the foundation witness be able to personally attest to the accuracy contained in the document, or or that he have personally prepared the document. In fact, (this) requirement (has) been frequently held to have been specifically eliminated by 28 U.S.C. § 1732. 41/

In Croft, the court upheld admission of computer printouts based on testimony of the Director of Payroll and Benefits Services of a university, whose office maintained and supervised payroll data compiled and printed out by computer. He was able to testify that:

1) the printouts were made contemporaneously with or near the time the payroll data became available;

2) the printouts were kept in the regular course of business, and it was the regular practice of the university to make such printouts;

3) the payroll data information entered into the computer and compiled in the printouts was reviewed and audited for errors throughout the year by his staff; and that

4) the university relied on the printouts to complete more than 60,000 W-2 employee payroll forms annually. 42/

In Russo, the foundation was laid by testimony of the Director of Service Review of Blue Shield of Michigan, who described the overall claims processing procedures, and the vice president of Michigan Blue

---

41/ Citing United States v. Miller, 500 F.2d, supra, United States v. Germillion, supra, United States v. DeFrisco, 441 F.2d 137 (5th Cir. 1971).

42/ United States v. Croft, supra, at 1364-65.

Shield in charge of all computer functions, who described the computer equipment used and its particular functions in the procedures in question. In rejecting the defendant's claim that no proper foundation was laid, the court pointed out that "[t]he witnesses...were qualified as experts by education, training and experience and showed a familiarity with the use of the particular computers in question. The mechanics of input control to assure accuracy were detailed at great length as was the description of the nature of the information which went into the machine and upon which the printout was based." 43/

In Weatherspoon, the court found that: "Pursuant to the testimony of a VA supervisory employee who was familiar with the preparation and use of the printouts, the Government showed to the satifaction of the trial court (1) what the input procedures were, (2) that the input procedures were accurate within two percent, (3) that the computer was tested for internal programming errors on a monthly basis, and (4) that the printouts were made, maintained and relied on by the VA in the ordinary course of its business activities." 44/

Particular care should be taken to have the foundation witness prepared to testify in detail as to the preparation and control of the input data. In Scholle, the printouts were the product of a computer system called STRIDE that "computerizes" the physical characteristics of seized and tested drugs, based on input including "types of drugs, their potency, components, dilutants, location collected, data analyzed, packaging information and price." The computer data was retrieved on a daily basis by the Section Chief of the Investigative Service Section of the Drug Enforcement Administration, who was called as a witness to explain the printouts. The court "recognized the propriety of treating routinely made and recorded laboratory analyses of drugs as business records admissible under the Federal Business Records Act" 45/ and upheld admission of the printouts, but in so doing had qualms with the adequacy of the foundation concerning the trustworthiness of the input data submitted by the field offices:

> In this case (the witness), being the founder of STRIDE and qualified by training, experience and position to testify about the system, adequately established that the disputed printouts reflected drug analyses computerized routinely during the regular course of business at the Drug Enforcement Administration, and also described in detail the source of the information upon which the printout was based. The government presented very little evidence concerning the mechanics of how input from eight widely dispersed laboratories is controlled or tested for its accuracy and reliability.

43/ United States v. Russo, supra, at 1233-34, 1241.

44/ United States v. Weatherspoon, supra, at 598.

45/ United States v. Scholle, supra, at 1124, citing United States v. Parker, 491 F.2d 517, 520 (8th Cir. 1973).

> ... In evaluating the admission of the disputed printout, we must consider the reliability of what goes into the computer as well as the reliability of what comes out. [Emphasis added.] 46/

b. CHAIN OF CUSTODY

Crimes involving computers invariably require the seizing of materials difficult to describe to persons unfamiliar with computer terminology and with the particular processes that produced the materials. Hence, special care should be exercised in preserving the chain of custody, which requires that the object offered as evidence must be supported by testimony that the object is the one involved in the incident, and that its condition is substantially unchanged.

In United States v. Lane, 591 F.2d 961, 962 (D.C.Cir. 1979), the court outlined principles governing chain of custody challenges:

> Tangible evidence of crime is admissible when shown to be "in substantially the same condition as when the crime was committed." And it is to be presumed that the integrity of the evidence routinely handled by governmental officials was suitably preserved "[unless the accused makes] a minimal showing of ill will, bad faith, evil motivation, or some evidence of tampering." If, however, that condition is met, the Government must establish that acceptable precautions were taken to maintain the evidence in its original state.
>
> The undertaking on that score need not rule out every conceivable chance that somehow the identity or character of the evidence underwent change. "[T]he possibility of misidentification and adulteration must be eliminated," we have said, "not absolutely, but as a matter of reasonable probability." So long as the court is persuaded that as a matter of normal likelihood the evidence has been adequately safeguarded, the jury should be permitted to consider and assess it in the light of surrounding circumstances.

See United States v. Anderson, 654 F.2d 1264, 1267 (8th Cir. 1981). The showing that the evidence is "in substantially the same condition as when the crime was committed" becomes more difficult when it is not apparent by sight that the item offered is what it is purported to be and when the item cannot be marked or initialed directly on its surface.. An example of such evidence is a quantity of seized heroin,

---

46/ United States v. Scholle, supra, at 1125.

which not only cannot be distinguished by sight or marked on its surface, but must be analyzed by a chemist qualified to testify that it is indeed heroin.

Although computer tapes and removable disks are distinguishable as such, they are nothing more than containers of data or information in the same sense that a plastic bag is a container of heroin, and like heroin, they cannot be marked or initialed on their (read/write) surface. (At least not without probably rendering them unreadable!) Just as the heroin must be verified by a chemical expert, computer printouts must be verified by a computer expert as representing the contents of the seized tapes or disks.

In a narcotics case, it is important to show that there was no break in the chain of custody prior to analysis by the chemist so that any contention that the evidence was altered attacks the credibility of the chemist and of the officers that handled the narcotics and thus goes to the weight, not the admissibility, of the evidence. United States v. Wood, 695 F.2d 459, 462 (10th Cir. 1980). See also United States v. Gay, 774 F.2d 368, 374 (10th Cir. 1985). It would seem that the same principle applies to computer storage media, i.e., an attack on the credibility of the computer expert and the officers handling the evidence would not affect its admissibility. "Absent some showing by the defendant that the exhibits have been tampered with, it will not be presumed that the investigators who had custody of them would do so." Id. See also United States v. Gatewood, 786 F.2d 821, 825 (8th Cir. 1986). "In order to find the evidence admissible, the court must conclude that it was reasonably probable that the evidence had not been altered since the occurence of the crime." United States v. Williams, 809 F.2d 75, 89 (1st Cir. 1986).

In a typical computer facility, magnetic tapes and disks are indistinguishable by sight except to the extent they have been labeled externally. Although tapes and disks are normally labeled internally, a computer process is required to print or display such labels. In seizing a large quantity of tapes or disks, it is not feasible to depend on internal labeling to preserve the chain of custody. The enormity of the physical and technical problems involved in seizing voluminous computer storage devices is illustrated in the Equity Funding case, a notorious case of fraud where much of the incriminating evidence was stored on computer tapes.

Equity Funding Corporation of America is a diversified financial services company based in California. In March 1973, trading in Equity Funding securities was halted by the New York Stock Exchange and the Securities and Exchange Commision (SEC). In a subsequent action brought by the SEC, Equity Funding consented to a decree enjoining the continuation of an alleged scheme to defraud investors. The scheme involved inflating assets and earnings "by creating and selling to reinsurers bogus life insurance policies in order to present to the investing public an image of a successful, growing and prosperous

enterprise. The alleged fraud, facilitated by the use of computers, enabled Equity Funding to overstate its assets and record non-existent assets, which eventually appeared in its financial statements." [Emphasis added.] In Re Equity Funding Corporation of America Securities Litigation, No. 142, 375 F.Supp. 1378, 1380-81 (Judicial Panel on Multidistrict Litigation 1974). (Shortly after the consent decree, the company went into Chapter X bankruptcy. It had almost 10,000 shareholders who had purchased approximately $500 million worth of securities in the corporation. 47/)

The following describes how seizure of the tapes was effected:

> In the Equity Funding case, upon receiving the consent of the trustee in bankruptcy, the FBI physically seized and sealed off the computer area. But unless policyholders, shareholders, and bondholders were to be wiped out, the company had to continue its day-to-day operations. Before any tape could be removed, there was a a mammoth task of copying a duplicate for every tape on the premises. The trustee hired a recognized computer expert to do the copying. The setting was carefully controlled, and all copying was done on Equity Funding's own computer equipment. The original tapes were transported to an off-site vault.
>
> It is important to have a computer expert participate at every step of the way. To avoid deterioration of the tapes, they had to be stored under controlled temperature and humidity conditions. Some 3000 reels of tape were involved. Here again, with that mass of material an expert was necessary to give advice even as to such elementary matters as stacking the tapes in a way to avoid warpage or other damage that might render them unreadable.
>
> The U.S. Attorney's Office double-padlocked the vault, posted a 24-hour guard, restricted access to the tapes, and utilized a sign-in log for all people entering and leaving the vault area.
>
> At the time of the initial seizure, FBI agents scratched their initials and the date onto each tape canister. Most of the tapes were already numbered serially. The original numbering system was retained, with new numbers assigned to tapes that had not yet been numbered.
>
> The agents compiled a separate log book to keep track of each tape, the recovery date, and the particular

---

47/ In Re Equity Funding Corporation of America Securities Litigation, No. M.D.L.-142-MML., 438 F.Supp. 1303, 1314 f.n. 5 (C.D.Calif. 1977).

agent who took initial possession of the reel. The log book would have been available to refresh the memory of government witnesses or to serve as "past recollection recorded" in a subsequent trial. 48/

Apart from the technical details that must be addressed in investigating and prosecuting a case involving evidence contained in voluminous computer storage devices such as in the Equity Funding fraud, considerable cost can be expected for the services of computer experts and for computer processing that may be required to analyze the evidence. The assistance of a cooperative victim and the use of experts and computer facilities of government agencies might substantially minimize this cost.

48/ Krauss and MacGahan, Computer Fraud and Countermeasures, at p. 324 (1979). The description is based on the work of Edward H. Coughran of the University of California at San Diego, and author of Computer Abuse and Criminal Law (1976).

CHAPTER V: MAKING THE CASE */

This chapter delineates some of the methods and precautions that investigators should consider in dealing with a computer-related crime. It provides a step-by-step process for approaching such crimes and dealing with the uniqueness of computer-related evidence.

The procedures described below are intended to guide the investigator in planning a computer-related investigation and in successfully handling computer evidence. They are neither all-inclusive nor offered as a set of minimum standards. Instead, they represent a compendium of suggested approaches and methods based on experience of investigators and prosecutors from various federal, state and local agencies. The extent to which a particular procedure is applicable will obviously vary, depending on factors such as the degree of technical sophistication of the subject, complexity of the equipment, nature of the crime, and individual circumstances.

1. PRELIMINARY INVESTIGATIVE MATTERS

The initial allegation of a computer crime may come about as a seemingly trivial matter that appears to be simply a technical problem. As in any other type of investigation, actions taken will depend upon how detailed and specific the information is and upon the reliability of information sources. Thus, the information must be thoroughly researched to determine if it supports the allegation, and, if necessary, the sources must be revisited for addititional information.

Once an allegation is determined to be well-founded, the pending investigative steps must be carefully planned, keeping in mind the perishability of magnetic or electronic records and that such records may only be available for a very short time. Also, the crime may still be in progress, and it may be a decoy or a cover-up for another larger crime. To assure that pertinent facts are documented and material evidence is gathered and properly preserved, the following actions and procedures should be considered:

a. Substantiate the allegation.

b. Consult with a computer expert, as appropriate.

---

*/ This chapter consists primarily of material contributed by the Air Force Office of Special Investigations, Computer Crime Division, with additions provided by the Federal Computer Crime Investigations Committee based on extensive editing of the Air Force material.

c. Prepare an investigative plan that sets forth the scope of the investigation and serves as a guide in determining how much technical assistance will be needed. The investigative plan should include the following information:

- WHO was involved as a victim, suspect, witness, or informant?
- WHERE did the described event occur? (Location is very important!)
- WHEN did the event occur?
- WHY did the incident occur?
- HOW was the incident committed?
- WHAT laws or regulations were possibly violated?

d. Depending upon the nature of the allegation and scope of the investigation, consult with an appropriate prosecutor concerning the elements of proof, evidence needed, and parameters of a prospective search.

Investigative reports should define the role of any technical experts involved in the case.

2. COMPUTER SURVEILLANCE TECHNIQUES

The investigator should be aware of the different means of capturing or monitoring computer data and the legal issues involved in computer surveillances. Always check with the prosecutive authority prior to the execution of a computer surveillance. Depending on particular circumstances and the effects of the Electronic Communications Privacy Act of 1986, such a surveillance may require the same approval as an interception of aural communication.

Since computer systems differ in methods and forms of data transmission, ample time should be alloted for planning and testing a chosen surveillance technique. The following are some of the more common techniques available:

- Hard Wire Video Capture: The investigator hard wires directly from the subject computer to a monitor terminal in the observation post, permitting information retrieved from the subject computer by a perpetrator to be observed and automatically recorded.

- Microwave Video Capture: This is basically the same as the hard wire video technique, except that the video signal is captured from the subject computer through microwave transmission rather than direct wiring. This method should not be used if it is suspected that classified information is on subject computer (because it would be subject to easy interception).

- Electronic Emanations Capture: This technique is very difficult to employ because the video signal is captured without direct access to the subject computer. It involves electromagnetic emissions emanating from the computer through walls and can be effected from a parking lot outside of the building housing the computer if circumstances are right.

- Use of a Data Line Analyzer: This involves use of a hardware device that allows the user to view the data that a computer is sending to a terminal, or vice versa, in "real time." That is, the investigator can view on the monitor screen actual data as it is being keyed by the perpetrator through a terminal, or being sent to him from the computer. The analyzer can be attached directly to a terminal, a computer, or a transmission line, or indirectly through any

of these devices. When used on a transmission line, the presence of the analyzer will normally not be known by the users on either end of the line. Additionally, the analyzer will allow the capture on magnetic tape of everything, or portions of the tranmission for playback at a later time. Finally, the analyzer will provide information on the exact type of transmission (needed for line analysis).

3. PLANNING A COMPUTER CRIME SEARCH AND SEIZURE

Once the allegation has been substantiated, the prosecutor should be contacted to determine if there is probable cause for a search. A key fact in any search is ownership or rightful occupancy of the premises to be searched, and ownership or rightful possession of the items to be seized. Different search and seizure rules apply depending on whether the premises and computer storage devices containing pertinent data or software are government or privately owned or leased, and whether the data or software is government or privately owned or licensed. Because of the technical orientation of a computer-related crime investigation, presenting a proper technical perspective in establishing probable cause becomes crucial to securing a search warrant.

As much as possible should be learned about the suspect, including his "M.O." and technical capabilities, the nature of the crime, and the type of equipment used. Following is a list of factors, questions and actions that should be considered in preparing for a search and possible seizure of computer-related evidence, recognizing that in many cases it may be impossible to identify specific items prior to an actual search:

a. Source Information

- What kind of machine is the subject computer? (Digital, analog, mainframe, PC, make and model, brand name)
- What kind of storage media is used? (Magnetic disk, magnetic tape)
- How much data will have to be reviewed?
- What software packages are used on the subject computer?
- Who owns the subject computer?
- Who has access to the computer and data, and how is access effected?
- Are there any changes to the operating system that might be trapdoors?
- Can the information sources be used to acquire incriminating evidence?
- What is the time of operation of the subject computer?

- What is the nature and frequency of illegal activity?

b. Case Agent Information

- What laws or regulations were violated?
- What are the elements of proof for the violations?
- Is the timing of the search important?
- Is the seizure going to include hardware or software, or both?
- How many agents will be needed for the search?
- Do the agents need a specific briefing on the handling of computer evidence?
- Will computer experts be needed to assist in the search and seizure?
- If seizing data in machine-readable form, what software packages will be needed to analyze it?
- Is compatible hardware available for analysis of seized data?
- What is expected to be found?
- What quantity of data is expected to be found?
- How much time is contemplated for analysis of data?
- Is there another way to capture the data?

c. Records Checks of Subjects and Incidentals

d. Communication Service Records

- Number of lines and types of service (call forwarding, speed-dial option, etc.) available to the perpetrator or subject computer
- Data Commmunications Services subscribed to (i.e., CompuServe, The Source, GTE Telenet, etc.)
- Long distance dialing company records. (Could have multiple long distance carriers.)

- Network management system audit trails

e. Pen Register or Dialed-Number Recorder (DNR)

- Documents telephone access code abuses
- Can identify additional subjects
- Can provide indication of extent of use of computer in hacking cases

f. Surveillance

- Surveillance of subject computer
- Surveillance of suspect to learn personal habits, most likely times of computer usage, and other traits indicating possible criminal activity or patterns
- Use of computer surveillance techniques (outlined earlier)

g. Computer Crime Scene Kit and Associated Supplies

When a computer related search and seizure is to be undertaken, the common crime scene kit will probably not contain the supplies and tools necessary. An agent conducting a computer search will need to develop a Crime Scene Kit that may include all or some of the following:

- Evidence tags
- Evidence tape
- Marking devices
  - Etching tool
  - Permanent ink marker
  - Felt tip pens
- Storage Media: (Attempt to identify storage media type used on target system prior to search)
  - Standard and high-density 5 1/4 inch floppy diskettes (100)
  - Standard and high-density 3 1/2 inch diskettes (40)

  - Magnetic tape reels
  - Tape cassettes
  - 8 inch diskettes

- Printer paper and printer ribbons
- Portable pen register/DNR
- Appropriate utility programs. (See Appendix D)
- Write protect tabs for floppy diskettes
- Colored gum labels
- Cardboard boxes
- Trash bags
- Fiber tape
- Funds to purchase additional supplies
- Tool kit
- Evidence containers - various types
- "Sterile" operating system disks
- Computer system and applications manuals for target system
- Packing materials
- Spare batteries - various sizes

h. The investigator should consider having the following support available:

- Camera support (video equipment; still and polaroid cameras; photographer)
- Technical expert familiar with the type of computer being searched or seized
- Dedicated evidence custodian
- Laptop computer and/or tape recorder for on-scene evidence inventory

4. EXECUTION OF A MICROCOMPUTER SITE SEARCH

In executing a search of a microcomputer site for evidence of a computer crime, the following procedure is recommended (which is also applicable to some minicomputer sites):

a. Move subjects and all other persons away from all telephone and computer equipment immediately.

b. Do not allow anyone to disconnect power, touch the keyboard of any device, or take any other action that may alter the subject computer's current state.

c. If appropriate, video tape the site (without audio) for purposes of documenting the system equipment configuration and wiring scheme, and the condition of the site upon arrival. (Still-photographs should be taken to record equipment serial numbers and wiring schematics).

d. Begin systematic evaluation of computer site.

- Determine whether computer system is operating. (Blank screen does not necessarily mean system is off)
- If there is a modem, disconnect it from the telephone wall jack
- Identify all connections to peripheral equipment and disconnect all remote access to the system
- Observe and photograph computer monitor
- Attempt to identify remote users of system
- Locate printouts and miscellaneous papers containing incriminating information

e. Secure above items utilizing proper evidence handling procedures and pack in transport cartons. (Plastic evidence containers should not be used to package magnetic media!)

f. If auto-dialer (speed dialer, or programmable telephone) is identified:

- Do not disconnect from its power source
- Connect a DNR to the telephone or auto-dialer. (It is recommended that the DNR search be conducted on-site, using A.C. power)

- Conduct a number-pad test. (Do not start test with numbers 0 or i!)

- Place pretext outgoing calls through each auto-dial memory storage button, or re-dial button, allowing the DNR to capture a printed record of the stored telephone number or access code resident in memory. (If telephone equipment manuals are found, consult them before downloading memory: many telephones have more than one "layer" of memory accessible through each button)

- Upon successful completion of above, replace any existing batteries with new batteries, disconnect the equipment, and pack for transport. (Battery replacement may not preserve memory in some equipment. Therefore, if possible, the memory should be downloaded before disconnecting from the power source)

g. Preparing computer for transport

- Locate peripheral equipment and determine system configuration and wiring scheme

- Determine if a hard disk drive or "hard card" is present

- Before transporting hard disk drives, the read/write heads must be secured to prevent damage. Some computer systems utilize a command that, when executed, secures the heads. Others must be secured mechanically. (See the manufacturer's operating manual to determine the proper procedure for each system)

- Protect floppy disk drives according to manufacturer's recommendations: some suggest inserting a new diskette in the drive slot, others do not. (As with hard drives, each manufacturer's instructions may be found in the system manual)

- Write protect all magnetic media. (Some diskettes require tabs to cover notch in sleeve, others have sliding notch covers on the sleeve)

- Label disks and diskettes, mark as evidence and place in non-plastic evidence containers.

- Label the wires connecting various devices at both ends to aid in the reassembly of the system at a later time

- Photograph the labelled equipment and wires before disconnecting

- Disassemble, tag, and inventory the equipment

- Carefully pack seized devices in suitable containers for transport

- Care should be taken to assure that computer equipment and magnetic media are transported in dust-free, climate-controlled environments. Temperature extremes may render magnetically-stored evidence unreadable, and various types of contamination can damage electronic equipment

Although various considerations sometimes make it necessary to conduct the actual search of the computer and magnetic storage media on-site (e.g., where records are stored on equipment owned by a non-target third party), it is preferable when possible to remove the equipment and storage media for analysis, documentation, and preparation of evidence and discovery copies. (Procedures for analysis of evidence are discussed in a later section.)

Although some of the procedures listed above are applicable to mainframe system searches, the complexity and diversity of mainframes make it difficult to develop uniform guidelines for effecting a search of such systems. Since each mainframe system is configured to meet the particular needs of an organization, identifying items to be seized and effecting their seizure will likely require assistance from the manufacturer and/or vendor who installed the system, from trustworthy insiders, or outside experts. It should be recognized that such searches and seizures demand an enormous amount of prior investigation and planning, and can require a significant investment of personnel and financial resources during the actual search and subsequent evidence analysis.

(Appendix C contains sample language for search warrant affidavits involving: 1) removal of a system from business premises; 2) the taking of software; 3) operation of a DNR/pen register; 4) explanation of operation of a voice-mail system; and 5) "blue box" hacking computer and programs.)

5. COLLECTION AND PRESERVATION OF COMPUTER EVIDENCE

Investigation of computer-related crimes more often than not involves highly technical matters, making it imperative during a search that appropriate steps be taken to ensure both the proper handling and preservation of evidence. There are seven recognized considerations involved in the care and handling of evidence:

- Discovery and Recognition
- Protection
- Recording
- Collection
- Identification
- Preservation
- Transportation

Each of these is discussed below in the context of a computer-related crime investigation.

a. DISCOVERY and RECOGNITION - The investigator's capability to discover and to recognize the potential source of evidence. When a computer is involved, the evidence is probably not apparent or visible. Nevertheless, the investigator must recognize that computer storage devices are nothing more than electronic or magnetic file cabinets and should be searched if it would normally be reasonable to search a file cabinet.

b. PROTECTION - The physical condition of evidence collected and seized is a major concern. Care should be taken to protect the area where evidence is located. Documents should be handled so as not to destroy latent prints or identifying characteristics. 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.

c. RECORDING - The alleged crime scene should be properly recorded. The use of a video camera to videotape computer equipment, workstations, etc., and related written documentation at the crime scene is highly encouraged. Remember to photograph the rear side of the computer (particularly the cable connections).

d. COLLECTION - Collecting computer-related evidence is somewhat different than collecting other forms of evidence. When collecting such evidence, take the following precautions:

- When collecting evidence, go after original books, records, magnetic storage media or printouts where possible

- Be aware of degaussing equipment. A degausser is an electronic appliance that creates a strong magnetic field which can be used to effectively erase a magnetic tape or disk. When collecting this type of evidence, ensure that any degaussing equipment is secured or rendered inoperative

- Documents and paper should be handled with cloth gloves, placed in an evidence container and sealed

- It is vital to seize all storage media, even ones that purportedly have been erased. Technical personnel may still be able to capture data thought to have been erased or determine that the erasures never occurred. (Disk operating system "delete" commands do not actually erase disk sectors, but merely make them available to magnetically write new information over existing information)

e. IDENTIFICATION - Identification of computer evidence is usually more difficult than other forms of evidence, requiring special knowledge of the thing being marked.

- Information on the evidence tag should include the hardware identification and operating system used to produce the tapes, disks, printouts, etc. (E.g. IBM PC/XT with PC-DOS version 3.2)

- Do not write on a magnetic disk surface

- Diskettes should be marked only with a felt tip pen or a label that has been filled-out, then attached

- Printouts should be marked with permanent marking pens

- Reel to reel magnetic tapes can be marked on the non-shiny side, within the first 10-15 feet (leader part)

f. PRESERVATION - Computer evidence can be very volatile. For example, evidence can be lost by turning the computer's power off prematurely.

- Remove evidence as soon as possible to prevent tampering. Tapes and disks can be erased or damaged quickly and easily

- Write-protect magnetic media as soon as possible to prevent deliberate or inadvertent alteration of evidence

- Store magnetic media at proper temperature (40-90 degrees F) and humidity (20%-80%) in a dust-free environment. Tobacco smoke is also damaging. Avoid placing near strong magnetic fields (e.g., (telephones, radio transmitters, photocopiers, or degaussers)

g. TRANSPORTATION - Particular care should be taken in the handling of computer evidence while in transit. (See subsection on preparing computer for transport, supra.)

- Transport magnetic media at the proper temperature and humidity

- Do not take magnetic media through metal detectors, conveyor belts or x-ray machines. This equipment generates strong magnetic fields that could destroy computer evidence

(Appendix D contains specific steps suggested for gathering and processing computer evidence to preserve its admissibility and veracity.)

6. COMPUTER DISK ANALYSIS

Magnetic disks have displaced magnetic tapes as the most common repository of machine-readable information. The following analogy illustrates the capacity of computer disks:

a. A typical paperback book consists of:

300 pages
36 lines per page
60 characters per line
648,000 characters per book

b. Capacity of computer disks commonly found on microcomputers:

3 1/2 inch microdiskette
720,000 characters - 1 paperback book

5 1/4 inch diskettes
360,000 characters - .5 paperback book
1,200,000 characters - 2 paperback books

10 megabyte hard disk or cartridge
10,000,000 characters - 15.4 paperback books

20 megabyte hard disk or cartidge
20,000,000 characters - 31 paperback books

90 megabyte hard disks
90,000,000 characters - 138.9 paperback books

c. Computer disks found on Large and Mini Mainframe computer systems:

360 megabyte disk packs
360,000,000 characters - 556 paperback books
1,000 megabyte (gigabyte) disks
1,000,000,000 characters - 1543 paperback books

As is apparent, computers can store vast amounts of information. In planning a search or seizure of computer data, consideration must be given to the amount of time involved in analyzing and reviewing the seized storage media. During one case, it took eleven investigators seventeen days to review and analyze 400 floppy diskettes, 45 ten megabyte disks, and 20 reels of magnetic tape.

There are numerous software packages available to analyze

disks containing data produced by most commonly used computers and their standard software packages. These packages can find hidden files, recover files that have been deleted, and recover some data that has been previously formatted.

The following are a few of the disk analysis software packages currently available:

- IBM Compatible (Z-150s, Z-200s, Z-248s)
  - . PC TOOLS; Norton Utilities; Mace; XTREE
- Z-100
  - . ZDump; Norton Utilities
- Apple IIe
  - . Beagle Brother Utilities
- Atari
  - . Hippo Utilities
- Commodore
  - . Clone

Following are suggested steps in gathering and analyzing magnetic evidence:

- Make two backup copies of storage media: one which may be given to the subject and another to be used as a "working copy" for review and analysis. Originals (or their equivalent) should be sealed and stored in an appropriate storage facility. Generally, as with audio tape, analysis and transcription should <u>not</u> be performed from the original media
- Display and obtain printout of directories (from hard disk, floppy diskette, etc.)
- Review files and identify potentially incriminating information. (In case of search warrant, identify records authorized to be seized)
- Copy potentially incriminating files (or records authorized to be seized) to floppy diskette, or print out
- Utilizing special utility programs, examine hard disk, diskettes, etc., for hidden or "deleted" files: if they

exist, they can be recovered, copied to diskette, or printed out

- If erased files are recovered, locate incriminating information and copy to diskette or print out

- Prepare separate "evidence diskette" containing only relevant files or records authorized to be seized, make two copies (working copy and discovery copy), seal original copy containing total contents and store in evidence facility. As necessary, make printouts from working copy. (The total contents backup will be available to meet a challenge as to accuracy of printouts offered from the evidence diskette)

- Document all steps taken in the course of review and analysis: contents of directories, files reviewed and copied, utility programs used, etc. This can be done by keeping notes, or by dictating a taped record. Keep a record listing from which disk, diskette, etc., each file or document was obtained

7. USING A COMPUTER AS AN INVESTIGATIVE TOOL

Computers can be used to collect and compile large amounts of data and provide statistics, reports and graphs to assist the investigator in analysis and decision-making. In deciding whether to employ computer resources to assist in an investigation, the following requirements analysis factors should be carefully considered:

- Is automation necessary or appropriate
- What output is desired
- What software is available
- What hardware is available
- What data elements are required based on output requirements
- Who will do the data entry (usually not the case agent)
- How many records will have to be entered
- What data elements are required in the reports
- If there are calculated fields in the report, can the software create those fields
- Who needs the report (Agent? Prosecutor?)
- Will the hardware handle the number of records required
- Will the software handle the number of records required
- What is the security classification of the data to be entered
- How much time is there for development
- How long will it take to enter all of the data
- Will an existing investigative tool suffice
- What is the volume of data elements required and their characteristics (alpha, numeric, field size)
- Design of input/output screen layout

- Design of report formats and sequence of data presentation
- Design of menus to drive the system
- Design of a backup system
- Development of a user's guide (documentation)
- Training of prospective system users

APPENDIX A

SUBPOENA SCHEDULE: SAMPLE LANGUAGE.

SCHEDULE */

I

DEFINITIONS

(j) "Subject of inquiry" means any data appearing on any invoices for the sale of _____ to any customers in the region in the subpoena period.

(k) "The subpoena period" means the period from January 1, 1983 until the date of the company's compliance with the subpoena.

(l) "Application system" means an organized collection of computer programs, data files, and procedures to be used to perform electronic data processing tasks on a computer.

(m) "Central processing unit" means the portion of a computer that includes the arithmetic, control, and storage units to be used to interpret and execute computer programs.

(n) "Computer operating system" means an organized collection of computer programs to be used to provide basic instructions for the operation, control, and management of the sequencing and processing of tasks (including the use of any computer storage media or peripheral devices) by a computer.

(o) "Computer program" means a set of statements or

---

*/ Excerpts from a subpoena schedule prepared by the Antitrust Division, Litigation II Section.

instructions to be used directly or indirectly in a computer to bring about a result.

(p) "Computer storage medium" means a device onto which data can be entered in machine readable form, held, and subsequently retrieved by a computer (e.g., a magnetic disc or tape).

(q) "Data file" means an organized collection of data records stored in and retrievable from a computer storage medium.

(r) "Data record" means an organized collection of data fields stored in and retrievable from a computer storage medium that a computer reads from that medium as an integral unit.

(s) "Data field" means a specific area within a data record in which a particular category of information is stored.

(t) "Identity" means:

(1) for an application system, computer operating system, or computer program, its common name, the name and address of its principal developer, the name and address of the vendor, its version and type, its release number and date, its programming language, and the identity of each central processing unit with which it can operate;

(2) for computer hardware other than a computer storage medium, its function (e.g., central processing unit), the name and address of its manufacturer, and its model, series, and version;

(3) for a computer storage medium, its type (e.g., magnetic disc, magnetic tape), the name and address of its manufacturer, its model, series, and version, and its volume serial number (or other specific identifier).

IV

DATA PROCESSING DOCUMENTS TO BE PRODUCED

1. For each computer storage medium that contains any data that is a subject of inquiry, documents sufficient to show:

(a) the identity of that medium;

(b) a general description of, and all time periods and geographic regions covered by, all such data that is contained on that medium, and each purpose for which the company used any of such data in the subpoena period;

(c) the sequence of data files on that medium, and for each such data file,

(1) its common name and its technical name;

(2) a general description of all information in it;

(3) its location on that medium;

(4) its length or range of lengths in bytes;

(5) its format (e.g., fixed, fixed blocked, variable);

(6) its block size;

(7) its organization (e.g., QSAM, BDAM, ISAM);

(8) for each primary or alternate key, a description of that key and the length and position of that key;

(9) if that data file contains any data that is a subject of inquiry,

a) a general description of, and all time periods and geographic regions covered by, all such data contained in that data file;

b) the sequence of data records in that data file, and for each such record,

(i) its common name and its technical name;

(ii) a general description of, and all time periods and geographic regions covered by, all information in that data record;

(iii) its location on that medium;

(iv) its length or range of lengths in bytes;

(v) the sequence of data fields in that data record, and for each such data field,

(A) its common name and its technical name;

(B) a specific description of, and all time periods and geographic regions covered by, all information in that data field;

(C) for each code by which information was entered in that data

field, the translation and expanded description of that code;

(D) its location on that medium;

(E) its length or range of lengths in bytes;

(F) its format (e.g., fixed, variable);

(G) its data type (e.g., character, zoned decimal, packed, binary);

(H) if it is a key,

(aa) whether the key was created as part of the file organization;

(bb) whether the key was created as part of an external index file (e.g., created by an application system);

(cc) whether the key is required;

(I) each of its validation criteria (e.g., alpha only, numeric range checks, cross field validation), and for each such criteria and for each validation check related thereto, the actual values for that validation check;

(d) for each data file, data record, or data field referred to in paragraph IV 1.c.(9) of this subpoena, to which access is limited by any security procedures,

(1) the identity of that data file, data record, or data field;

(2) a description of all security procedures limiting access to that data file, data record, or data field;

(3) a means to permit access to that data file, data record, or data field;

(e) for each data file on that medium that contains any data that is a subject of inquiry and from which the company cannot now retrieve all of such data,

(1) its common name;

(2) its length or range of lengths in bytes;

(3) its location on that medium;

(4) a specific description of, and all time periods and geographic regions covered by, all data that is a subject of inquiry contained in that data file that the company cannot now retrieve from that data file;

(5) the time period during which the company could retrieve all such data from that data file;

(6) each reason why the company cannot now retrieve all such data from that data file.

2. For each application system the company used in the subpoena period to process any data that is a subject of inquiry:

(a) documents sufficient to show the identity of that application system;

(b) each document that constitutes or contains any user manuals or other information or instructions for the use of that application system;

(c) for each organizational unit of the company that used that application system in the subpoena period to process any such data, documents sufficient to show,

(1) the name and address of that organizational unit;

(2) for each individual who supervised in the last two years the use of that application system in that organizational unit to process any such data, the name, and the current or last known home and business addresses and telephone numbers, of that individual;

(d) for each computer program the company used in or with that application system to process in the subpoena period any data that is a subject of inquiry,

(1) each document that constitutes or contains any user manuals or other information or instructions for the use of that program;

(2) documents sufficient to show,

a) the identity of that computer program;

b) for each data file containing any such data that the company created or used with that computer program in that application system in the subpoena period, the common name of that data file;

(e) for each central processing unit the company used with that application system to process in the subpoena period any data that is a subject of inquiry, documents sufficient to show,

(1) the identity of that central processing unit;

(2) for each computer operating system the company used with that central processing unit to utilize that application system to process in the subpoena period any such data, the identity of that computer operating system.

3. For each data file that contains any data that is a subject of inquiry:

(a) documents sufficient to show for each individual who supervised in the last two years the entering of any such data into that data file, the name, and the current or last known home and business addresses and telephone numbers, of that individual;

(b) each document that constitutes or contains any keying or coding manuals that relate to the entering of such data into that data file.

4. Each document that is a computer storage medium to be identified by documents in response to paragraph IV 1.(a) of this subpoena, above, along with each of its labels.

5. Each document that is a computer storage medium containing any computer programs to be identified by documents in response to paragraph IV 2.(d)(2)a) of this subpoena.

APPENDIX B

TABLE OF AUTHORITIES FOR CHAPTER IV CITATIONS

STATUTES

RULES

APPENDIX C

SEARCH WARRANT AFFIDAVIT: SAMPLE LANGUAGE */

Sample 1: Experienced computer investigator's rationale for removing system from business premises and for taking software

.... . On _____ 1988 _____ returned to the _____ and was able to observe the back of the counter and the computer system. He saw two devices beneath the counter, and while unable to get close enough to exactly identify them, stated that he believed that one might be a hard disk drive and the other a modem (a device for computer communications over telephone lines).

Affiant interviewed Special Agent George Mehnert, employed in the Special Investigations Division of the Arizona Attorney General's Office. Mehnert informed affiant that in connection with his employment, he uses computer systems, as well as conducting computer related investigations. In the last two years Mehnert has supervised or participated in several executions of search warrants for computer stored records and evidence. Mehnert informed Affiant that because computer stored data is vulnerable to destruction through error, electrical outages and other causes, most computer users keep "backup copies" of their data and programs. These copies may be found on floppy diskettes, tape cassettes and other storage media. Mehnert stated that even if data is erased or deleted from the system itself, it might be found on the backup copies.

Mehnert stated that when records are stored on floppy disks or in a hard disk, even when they appear to have been erased or deleted, they may still be retrievable. Mehnert is familiar with the methods of restoring "lost" data commonly employed by computer users and has used those methods himself. Mehnert has also used the assistance of a computer expert in several cases in order to obtain the contents of computer stored evidence.

Mehnert stated that conducting a search of a computer system, documenting the search and making evidentiary copies is a lengthy process. It is necessary to determine that no security devices are in place which could cause the destruction of evidence during the search. In some cases it is impossible even to conduct the search without expert assistance. Since computer evidence is extremely vulnerable to tampering or destruction, removal of the system from the premises will assist in retrieving

---

*/ Excerpts from affidavits provided by the Office of the Attorney General for the State of Arizona.

the records authorized to be seized, while avoiding accidental destruction or deliberate alteration of the records. It would be extremely difficult to secure the system on the premises during the search, especially when it is connected by modem to communications lines. Destruction or alteration could be performed from a location remote from the premises during the search.

Mehnert stated that the accompanying software must also be seized since it would be impossible without examination to determine that it is standard, commercially available software. It is necessary to have the software used to create data files and records in order to read the files and records.

Mehnert stated that in his experience there are other memory storage devices involving similar problems, such as telephones with programmable memories, and "credit card computers" used to store calendars, telephone numbers and addresses, and even financial records. ....

Sample 2. Operation of DNR/pen register; explanation of operation of voice-mail system; "blue box" tone hacking of computer and computers

.... involved in that case had stated that her source of stolen telephone authorization calls was someone who called himself "Freddie the Frog" at telephone number 602-_____ . This is the same telephone number obtained from the trap-and-trace installed in December.

Sandquist contracted with Mountain Bell for a dialled number recorder (DNR) to be installed on 602-_____, and the DNR was attached on January 20, 1988 by Kenneth Nelson, Assistant Staff Manager, Mountain Bell Security. A dialled number recorder captures the electronic impulses travelling over telephone line as the numbers on a telephone are dialled or pushed. The device records the numbers dialled or pushed on a paper tape for review, but does not record the voice communication.

An initial review of the DNR tapes revealed that 12 long-distance calls were completed through the Sprint network between January 27 and February 10, 1988 from telephone number 602-_____, using five different Sprint customer authorization codes. All five codes belong to Sprint customers, and all five accounts have suffered fraudulent charges posted to those accounts by persons not authorized by the customer to use the code. When a code is identified by Sprint as having been stolen, that code is removed from the system and the legitimate customer is issued a new authorization code. Losses attributable to theft of the code are borne by U.S. Sprint; the customer is not held responsible for unauthorized toll charges.

The DNR also revealed that several other long-distance carriers are being used to place calls from 602-_____. MCI access number 602- _____ was called 25 times on February 8 and 9, 1988. After checking their records, MCI informed Sandquist that they do not have a customer by the name of _____, nor do they have a customer assigned the telephone number 602-_____. While the investigation is still continuing, the DNR tapes also indicate use of the ALLnet communications network.

Kenneth Nelson also reported that the DNR tapes showed at least 53 calls between January 27 and February 1, 1988 to 1-800-_____, a number subscribed to by _____, Pennsylvania. A second _____ number, 1-800-_____, was dialled 101 times between February 8 and February 11, 1988. Nelson contacted the company, and was informed by _____, Security Representative, Risk Management Department, that these two numbers provide access through several telephone lines into the _____ proprietary voice-mail system, and that the company had recently been suffering abuse of the system.

2. Affiant interviewed _____ and _____, Manager, Telecommunications Information Systems, both employed by _____ . They provided the following information:

The _____ voice-mail system allows authorized _____ employees to obtain a "voice mailbox" which is capable of performing several functions. Among these are the ability to receive and store messages from callers, to send messages to other boxes on the system, and to send messages to a pre-selected group of boxes. These functions are achieved by pushing the appropriable numerical commands on a telephone keypad for the desired function. To leave a message, the caller dials one of the two "800" numbers listed above, and hears a message identifying the system as the _____ voice-message system. The caller is then instructed to enter the number of the box he wishes to reach. The caller enters a four-digit number, and hears whatever greeting the box owner has chosen to leave. The caller can exercise several options, one of which is to leave a message after the tone. In this respect, the voice-mail system operates much like a telephone answering machine. Rather than being recorded on audio tape, however, the message is stored in digitized form by the computer system. The entire voice-message system is actually a computer system accessible through telephone lines. The messages are stored on large-capacity computer disks.

An outside caller needs to know only the assigned box number in order to leave a message for a _____ employee. In order to retrieve the messages or to delete them from the system, however, the person to whom the box is assigned must have both the box number and a confidential password -- the password ensures privacy of the communications by acting as a "key" to "unlock"

the box and reveal its contents. The employee to whom the box has been assigned also has the ability to change his password, thereby preventing access to the box contents by anyone who may have learned his password.

_____ stated that since December, 1987 they have been receiving reports from authorized users of abuse of the system. Among the abuses complained of were harassing, obscene, anti-Semitic and threatening messages left in various boxes, and the "taking over" of several boxes by unknown persons who somehow obtained the passwords, gained access to the boxes, then changed the passwords to deny access to the assigned users. In one box, _____ proprietary financial data had been left for a _____ employee: that box was accessed, and the message contents were disseminated by means of messages left in other stolen boxes.

_____ also reported a significant increase in use of the system during this period. While they do not yet know the full extent of _____ losses, the company pays AT&T the charges for use of their two "800" numbers which provide access into the voice-mail system. In addition, the unauthorized users have interrupted service to _____ employees and have occupied a significant portion of the system's available disk storage capacity.

When information obtained from the DNR installed on 602-_____ was relayed to them, they obtained access to some of the stolen boxes, and heard messages announcing Sprint, MCI and Allnet authorization codes.

3. For the last three years, affiant has been employed in the Computer Crime section of the Maricopa County Sheriff's office. During that time, affiant has investigated over thirty cases involving the theft of long-distance telephone services and unauthorized access to computer systems. Affiant has also received training in the investigation of computer fraud and "hacking" (the unauthorized invasion of computer systems by various means) from the International Association of Chiefs of Police and the Federal Bureau of Investigation.

Through his experience, affiant has learned that persons engaged in the theft of long-distance communication services and dissemination of stolen authorization codes commonly employ computer communications devices, computer bulletin boards and voice-mail systems to facilitate the dissemination of stolen codes and other information. Affiant has found that in virtually all cases, both communications-service abusers and computer hackers maintain either written or computer-stored records of the access numbers, authorization codes, passwords, and other information relating to these activities.

Affiant is also aware that a dialled number recorder, in

addition to recording numbers punched or dialled from the telephone facility on which it is installed, records any transmission of the special signalling tones which are used to control communications networks and other associated automatic billing systems. Through Kenneth Nelson and "Sandy" Sandquist, affiant learned that on more than one occasion, the DNR installed on 602-_____ recorded the use of the special signalling tone, indicating that that signal had been trasnmitted from that telephone facility. Through his experience, affiant has learned that the special signalling tone can be generated by an electronic tone-generating device known as a "blue box," or by a personal computer and computer software which enables the computer to generate the tone signal through a communications device (a modem or accoustic coupler) connecting the computer to the telephone line. In his past investigations, affiant has frequently found that persons stealing communications services have possessed a personal computer and the necessary software which would allow them to manipulate communications networks by means of the special signalling tone.

4. R.E. "Sandy" Sandquist stated that for the last four years, he has been employed full-time by GTE and Sprint to investigate telecommunications fraud. He stated that in 1987, he investigated over a half-dozen cases in which search warrants were executed, and in every one of these cases, records were found which related to the theft of services. In each case in which the special signalling tones (or "blue box" tones) had been used, a computer with tone-generating software was found.

Based upon all the foregoing, affiant believes that probable cause exists for the issuance of a search warrant for the residence located at _____, Phoenix, Arizona.

_____

WILLIAM F. NIBOUAR, Sergeant
Maricopa County Sheriff's
Office

Subscribed to and sworn before me this _____ day of _____

_____

JUDGE, MARICOPA COUNTY
SUPERIOR COURT

APPENDIX D

SUGGESTED METHODS FOR PROCESSING COMPUTER EVIDENCE

(a) CASSETTE TAPE

- Keep away from magnetic fields
- Write protect cassette
- Initial and date plastic surface
- Affix identifing gummed label
- Place tape in evidence container
- Fill out evidence tag
- Make two copies of tape at earliest convience, store original in evidence facility

(b) CASSETTE TAPE DRIVE

- Photograph tape drive and cables
- Remove cassette tape from drive
- Process tape as evidence (noting location where discovered)
- Check monitor for processing prior to powering cassette drive off
- Initial and date tape drive
- Label all associated cables and wires at both ends before disconnecting
- Fill out evidence tag, including serial numbers

(c) CARTRIDGE DISKS

- Keep away from magnetic fields
- Write protect cartridge
- Initial and date plastic surface
- Affix identifing gummed label
- Place cartridge in evidence container
- Fill out evidence tag
- Make two copies of disk at earliest convience, store original in evidence facility

(d) CARTRIDGE DISK DRIVES

- Photograph disk drive and cables
- Remove disk from drive
- Process disk as evidence (noting location where discovered)
- Check monitor for processing prior to powering drive off
- Secure read/write heads. Some use a command others

must be secured mechanically. (See operating manual)
- Initial and date drive
- Label all associated cables and wires at both ends before disconnecting
- Fill out evidence tag, including serial numbers

(e) CARTRIDGE TAPES

- Keep away from magnetic fields
- Write protect cartridge
- Initial and date plastic surface
- Affix identifing gummed label
- Place tape in plastic bag
- Fill out evidence tag
- Make two copies of tape at earliest convience, store original in evidence facility

(f) CARTRIDGE TAPE DRIVES

- Photograph tape drive and cables
- Remove cartridge tape from drive
- Process tape as evidence (noting location where discovered)
- Check monitor or console for processing prior to powering cassette drive off
- Initials and date tape drive
- Label all associated cables and wires at both ends before disconnecting
- Fill out evidence tag

(g) CABLES/WIRES

- Photograph all cabling before disconnecting
- Label both ends of each cable describing connectors (to assist in reassembly)
- Label the connectors that the cable connected to
- Fill out evidence tag
- Place coiled cables in evidence container and seal

(h) PAPER: CODING SHEETS, FLOW CHARTS, MANUALS, NOTES, ETC.

- Sheets should be handled with gloves
- Dust surfaces for latent fingerprints
- Date and initial all loose sheets or top sheet of pad
- Fill out evidence tag
- Place sheets in evidence container and seal

(i) COMPUTER PRINTOUTS OR LISTINGS

- Printouts should be handled with gloves
- Dust surfaces for latent fingerprints
- Date and initial all loose sheets or top sheet of continuous listing
- Fill out evidence tag
- Place sheets in evidence container and seal

(j) PC/CPU (Central Processing Unit)

- Determine if hard disk drive/hard card internal. (See hard drive)
- Check monitor for processing prior to handling
- Photograph front and rear including cabling
- Label cables and ports
- Initial and date CPU
- Fill out evidence tag
- Wrap in plastic trash bag
- Place in box or crate for transporting

(k) CRT (Monitor/TV)

- DO not power off until currently displayed screen is photographed
- Photograph the back of CRT including cabling
- Label cables at both ends as well as connector ports
- Initial and date CRT
- Fill out evidence tag
- Wrap in plastic trash bag
- Place in box or crate for transporting

(l) FLOPPY DISKETTE

- Keep away from magnetic fields
- Write protect diskette
- Initial and date using laundry marker (corners only), or label completed before attaching
- Affix identifying gummed label
- Place diskette in evidence container. (Do not use plastic bag)
- Fill out evidence tag
- Make two copies of diskette at earliest convience, store original in evidence facility

(m) EXTERNAL FLOPPY DISKETTE DRIVES

- Photograph diskette drive and cables
- Process drive as evidence (noting location where discovered)

- Check monitor for processing prior to powering diskette drive off
- Secure read/write heads. Some use a command; others must be secured mechanically. (See operating manual)
- Initial and date into bottom of diskette drive
- Label all associated cables and wires at both ends before disconnecting
- Fill out evidence tag, including serial numbers
- Wrap drive in plastic trash bag
- Place drive in box or crate for transporting

(n) PRINTERS AND GRAPHICS PLOTTERS

- Note and record DIP switch settings
- Remove ribbons, initial and date on ribbon container. (Do not touch ribbon surface. NOTE: like typewriter ribbons, computer printer ribbons may contain last documents printed)
- Complete evidence tag
- Place in plastic bag or evidence container
- Initial and date printer or plotter
- Label all associated cables and wires at both ends before disconnecting
- Fill out evidence tag, including serial numbers
- Wrap device in plastic trash bag
- Place device in box or crate for transporting

(o) EXTERNAL/REMOVABLE HARD DISK DRIVE

- Photograph drive and cables
- Process drive as evidence (noting location where discovered)
- Check monitor for processing prior to powering drive off
- Dust all hard surfaces for latent fingerprints
- Secure read/write heads. Some use a command, others must be secured mechanically. (See operating manual)
- Initial and date drive
- Label all associated cables and wires at both ends before disconnecting
- Fill out evidence tag, including serial numbers
- Wrap drive in plastic trash bag
- Place drive in box or crate for transporting

(p) KEYBOARD

- Photograph front and rear including cabling
- Label cables and ports
- Initial and date

- Fill out evidence tag, including serial numbers
- Wrap in plastic trash bag
- Place in box or crate for transporting

(q) EXTERNAL MODEMS OR ACOUSTIC COUPLERS

- Disconnect from telephone connection
- Photograph front and rear including cabling
- Label cables and ports
- Initial and date
- Fill out evidence tag, including serial numbers
- Wrap in plastic trash bag
- Place in box or crate

(p) REEL TO REEL TAPE

- Keep away from magnetic fields
- Write protect tape
- Initial and date on first 10-15 feet (leader) of tape using ball point (not felt tip) pen
- Affix identifing gummed label (on reel only)
- Place tape in evidence container
- Fill out evidence tag
- Make two copies of tape at earliest convience

(q) REEL TO REEL TAPE DRIVE

- Photograph tape drive, cables, and toggle switch settings (inside cabinet)
- Remove tape from drive
- Process tape as evidence (noting location where discovered)
- Initial and date tape drive
- Label all associated cables and wires at both ends before disconnecting
- Complete evidence tag, including serial numbers

NOTE: Magnetic or electronic evidence may be found on other devices, such as cassette recorders and tapes, programmable wrist watches, calculators, typewriters and telephones. Depending upon the capabilities of the particular device, it may be possible to copy the evidence to magnetic media or paper tape, or to photograph visual displays.