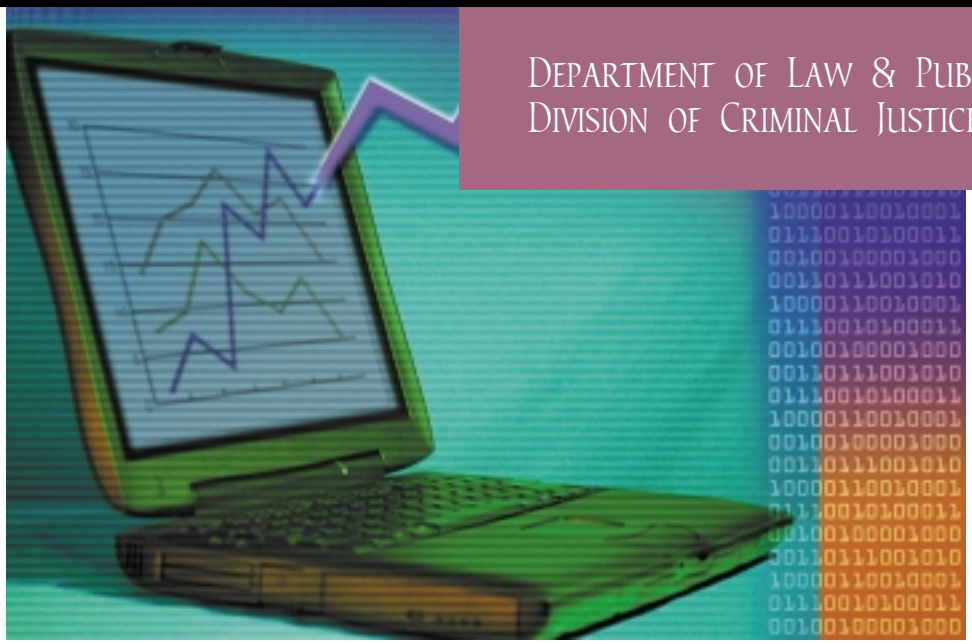
New Jersey

Computer Evidence Search & Seizure Manual



Department of Law & Public Safety
Division of Criminal Justice

LAPS

New Jersey

Computer Evidence Search & Seizure Manual

Department of Law & Public Safety
Division of Criminal Justice

April 2000

State of New Jersey
DEPARTMENT OF LAW AND PUBLIC SAFETY
OFFICE OF THE ATTORNEY GENERAL
PO BOX 080
TRENTON, NJ 08625-0080
(609) 292-4925

CHRISTINE TODD WHITMAN
Governor

JOHN J. FARMER, JR.
Attorney General

April 2000

To All Law Enforcement:

Re: Computer Evidence Search and Seizure Manual

Dear Law Enforcement Personnel:

I am pleased to provide you with this new manual that provides details regarding the search and seizure of computers and computer-related evidence.

The proliferation of personal computers and the explosive growth of the Internet have major implications for the law enforcement community. Just as technology has changed the nature of communications and commerce, it has similarly provided new avenues for criminal activity and victimization. Paper records of illegal transactions have given way to electronic data files; threats are now often conveyed by email; personal identities are stolen and used for illicit purposes; and chat rooms provide would-be-sex offenders with new opportunities to lure minors.

Fortunately, law enforcement's ability to navigate this fast-changing terrain continues to outpace the expectations of criminals using computers. There is no better example of this than the recent, successful investigation of the "Melissa" virus case. Working in cooperation with federal, county and local law enforcement agencies, expert investigators and prosecutors from the Division of Criminal Justice's Computer Analysis and Technology Unit (CATU) and the Division of State Police's High Technology Crime and Investigations Support Unit (HCTU) identified the creator of the virus and arrested the suspect in less than 72 hours. During those 72 hours, however, the virus caused more than $80 million in damages and shut down e-mail systems around the world. If the law enforcement community had not responded as proficiently as it had, the damage from the virus could have been catastrophic.

The "Melissa" virus case underscores the point that in order for law enforcement agencies to stay ahead of computer criminals, we must work together. Criminal Justice's CATU and State Police's HCTU are integral participants in the Attorney General's Internet Working Group, a group brought together by my office to coordinate the high-technology resources of all the divisions of the Department of Law and Public Safety and to pursue an integrated approach to Internet and advanced technology issues. Similarly, the Statewide Computer Crime Task Force brings together State, county and local law enforcement agencies to train prosecutors in the areas of computers, computer forensics, the Internet and the legal issues associated with the investigation, presentation and admissibility of digital and electronic evidence.

In the spirit of this cooperative effort, I pledge to you the resources of the Department of Law and Public Safety in the fight against the emerging threats of computer and high-technology crime. This Computer Evidence Search and Seizure Manual will provide important guidance to you as police and prosecutors involved in the investigation and prosecution of cases along the new frontiers of high technology.

Without doubt, however, new technologies are emerging rapidly. The law that governs the search and seizure of computers and computer-related evidence are likely to continue to develop as well. It is important, therefore, that local and county law enforcement agencies continue to work closely with the experts in my Department so that, collectively, we can bring the best resources together to bear down on those who would use technology to advance their illicit purposes.

Respectfully submitted,

John J. Farmer, Jr.
Attorney General

TABLE OF CONTENTS

I. SEIZING COMPUTER EVIDENCE 3

A. WARRANT-BASED SEARCHES & SEIZURES OF COMPUTER EVIDENCE 3
1. Probable Cause Requirements 7
a. Probable Cause to Believe That a Crime has been Committed and That the Items Described in the Warrant are Connected to Criminal Activity 7
b. Probable Cause to Believe That the Materials to be Seized are to be Found at the Place to be Searched 8
2. Particularity Requirement 10
a. Generally 10
b. Description of the Place to be Searched 11
(1) Tangible Objects 11
(2) Intangible Objects 11
(3) Multiple Locations 12
c. Description of the Items to be Seized 14
(1) Tangible Objects 15
(2) Intangible Objects 15
d. Summary 17
3. Deleted, Encrypted or Password-Protected Data 18
4. When to Serve the Warrant 21
5. "No Knock" Authority 22
6. On-Site/Off-Site Searches 23
7. Authorization to Take Computer Peripherals and Documentation 32
8. Supplemental Warrant Applications 34

B. Warrantless Searches & Seizures 35
1. Plain View 36
2. Exigent Circumstances 38
3. Consent 40
a. Scope of Consent 40
b. Who May Consent 41
(1) Family Members and Cohabitant 42
(2) Employers 44
c. Passwords and Encrypted Documents 45
d. Networks 46

II. SEARCH EXECUTION 47

A. SEIZING COMPUTER EVIDENCE 47

B. SEIZING COMPUTER STORAGE DEVICES WHERE THE WARRANT ONLY AUTHORIZES THE SEIZURE OF RECORDS 50

C. THE WARRANT SPECIFICALLY PERMITS THE SEIZURE OF COMPUTER RECORDS BUT AN ON-SITE REVIEW IS IMPRACTICAL 50

D. DOCUMENTING THE SEARCH AND SEIZURE OF COMPUTER EVIDENCE 53

III. SPECIAL WARRANTS: THE IMPLICATIONS OF THE WIRETAP ACT, THE ELECTRONIC COMMUNICATIONS PRIVACY ACT, AND THE PRIVACY PROTECTION ACT 54

A. ELECTRONIC SURVEILLANCE ORDERS 55
1. Requirements 55
2. Type of Communication to be intercepted 56
3. Circumstances Under Which a Wiretap Order Should be Sought in Connection With a Computer 57

B. STORED ELECTRONIC COMMUNICATIONS 57

IV. PRIVACY PROTECTION ACT AND NEWSPERSON'S SHIELD 64

A. PPA Cases 66

B. Conclusion 68

V. REVIEW AND ANALYSIS OF COMPUTER EVIDENCE 68

VI. ADMISSIBILITY OF COMPUTER EVIDENCE 75

A. BEST EVIDENCE RULE 76

B. AUTHENTICATION 78

C. CHAIN OF CUSTODY 80

VII. CONCLUSION 80

APPENDIX

A. Table of Authorities

B. Computer Search Checklist

C. Sample Warrant Language

D. Sample Search Warrant Affidavit

E. Sample Subpoena Language

F. Communication Information Orders

G. Sample Communications Data Warrant Affidavit

ACKNOWLEDGMENT

The members of the Computer Crimes Committee include Assistant Attorney General John J. Smith, Jr., and Deputy Attorneys General Karen Fiorelli, John F. Kennedy and Christopher G. Bubb. Members of the Computer Crime Committee of the New Jersey Prosecutor's Association include the Honorable Glenn Berman, Prosecutor of Middlesex County; the Honorable John B. Dangler, Prosecutor of Morris County; and William Schmidt, Prosecutor of Bergen County.

Assistant Attorney General Ronald Susswein, Deputy Director of Policy of the Division of Criminal Justice and Deputy Attorney General Joie Piderit also rendered invaluable assisted in the preparation of the Manual.

FOREWORD

Just as technology has exponentially increased the level of communication and commerce, it has similarly expanded opportunities for criminal activity and victimization. The Internet can be used to commit crimes ranging from the release of a computer virus resulting in world wide catastrophic damage to industrial espionage, from simple assaults to acts of terrorism, from child pornography to luring and sexual assault on children. Apart from the breadth of potential misconduct, the unique nature of the Internet presents challenges not evident in the traditional law enforcement milieu, such as questions of jurisdiction, evidence access and preservation, applicability of current laws, vulnerability of a virtually unlimited victim pool, and practical obstacles to the identification of perpetrators.

No better example can be found than in the Attorney General's successful prosecution of the creator of the Melissa virus. In March of 1999, the State Police, the Division of Criminal Justice, the Monmouth County Prosecutor's Office and the Newark Office of the Federal Bureau of Investigation completed the successful investigation of the creator of the "Melissa" computer virus, and arrested the suspect in less than 72 hours. The virus caused damage in excess of $80 million and shut down e-mail systems around the world.

This technological revolution has created a fundamental challenge to law enforcement in the manner in which evidence of a crime is seized, analyzed and

presented in court. The Computer Evidence Search and Seizure manual is designed to provide guidance on how to deal with this new evidence.

In addition to this Manual, the Department of Law and Public Safety provides other resources to assist law enforcement in New Jersey in dealing with the new and emerging threat posed by high technology crimes. The Division of Criminal Justice has established the Computer Analysis and Technology Unit to investigate and prosecute high technology crime committed in this State. The Division's goal is to provide assistance on the myriad legal issues that are presented by computer-related crime.

The Division of State Police has established the High Technology Crime and Investigations Support Unit to investigate traditional crimes involving computers. The unit also investigates crimes that have developed with the advances of technology. All of the resources of the Department of Law and Public Safety are available to assist law enforcement throughout New Jersey.

I. SEIZING COMPUTER EVIDENCE

A. WARRANT-BASED SEARCHES & SEIZURES OF COMPUTER EVIDENCE

A major investigative objective prior to executing any search warrant is to identify, as fully as possible, the target(s), the crime(s), the computer system(s) and the software employed by the target(s). It is preferable to know as precisely as possible what computers and computer hardware, software programs, networks, etc., will be encountered so that the search warrant execution team is prepared to conduct the search. Including precise information about the computer system to be searched in the affidavit of probable cause and search warrant will also aid the prosecutor in defending a later challenge to the search and seizure.

As with any search and seizure, it is always preferable to obtain a search warrant, if possible. A seizure pursuant to a valid search warrant is presumed to be valid and deference will be given to the issuing judge's finding of probable cause. State v. Novembrino, 105 N.J. 95, 120 (1987). In doubtful or marginal cases, a warrant-based search may be upheld where a warrantless one would fail. State v. Demeter, 124 N.J. 374 (1991).

Computer-related crime and the role of the computer in more traditional crimes is an emerging area in the law. While judges, prosecutors and investigators are well-acquainted with routine search warrant applications for evidence of traditional crimes,

they may not be as familiar with computer crimes or how computers may be used to perpetrate traditional crimes. Awareness of these issues is increasing through the use of specially designated Wiretap and Communications Data Warrant Judges and the Computer and Telecommunication Coordinator Program which includes at least one prosecutor from every County. However, it is the affiant's job to inform the judge. Therefore, to assist the court in deciding whether a warrant should issue, the affiant will need to present the relevant information in a manner that allows the judge to understand the technical computer references contained in the affidavit and the technical aspects of the investigation.

The first step in drafting a search warrant application involving the seizure of computers is to consider the role that the computer plays in the offense. Situations where seizure is justified can involve computer equipment or information that is stolen or purchased with the proceeds of some separate illicit activity; computers that are the tools used to commit the offense; or computers that serve as a storage cabinet for information concerning illegal activities.[1] Therefore, the affiant should first ask himself whether the

---

[1] R. 3:5-2 permits the seizure of "any property." The Rule provides:

> A search warrant may be issued to search for and seize any property including documents, books, papers and any other tangible objects, obtained in violation of the penal laws of this State or any other state; or possessed, controlled, designed or intended for use or which has been used in connection with any such violation; or constituting evidence of or tending to show any such violation.

computer equipment or information is (1) contraband; (2) the fruits of a crime; (3) an instrumentality of the offense; and/or (4) evidence of a crime. R. 3:5-2.[2] Understanding the role the computer plays in the offense will assist the affiant in pinpointing and articulating those facts that are critical to establishing probable cause to believe that a crime has been committed, particularly describing the place to be searched, and identifying the items that are subject to seizure (i.e., equipment, software, manuals and information).

Clearly computer hardware (the central processing unit [CPU], hard disk drive, floppy disk drive, mouse, modem, fax peripheral, CD ROM, laser disc, scanner, and printer), is "property," which includes "tangible objects." Although intangibles are not specifically included in the examples of property which may be seized, the Rule states that any property may be seized and there is no indication that the listing in R. 3:5-2 is intended to be an exhaustive one.

Federal courts have construed Fed. R. Crim. P. 41, the similarly worded counterpart to R. 3:5-2, to allow seizures of intangibles and specifically, electronic information. In United States v. New York Tel. Co., 434 U.S. 159, 169 (1977), an electronic surveillance case, the Supreme Court stated that Fed. R. Crim. P. 41 is not limited to tangible items, but is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause. See Michigan Bell Tel. Co. v. United States, 565 F.2d 385, 389 (6 Cir. 1977); Application of United States for an Order Authorizing the Installation of a Pen Register, Touch Tone Decoder and a Terminating Trap, 458 F. Supp. 1174 (W.D. Pa. 1978). See also United States v. Villegas, 899 F.2d 1324 (2d Cir. 1990), cert. denied, 498 U.S. 991 (1990); United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986), cert. denied, 479 U.S. 827 (1986).

[2]Computers and the data they contain are most often seized as evidence of a crime. Computers, peripherals and stored electronic data may also be seized pursuant to the forfeiture statutes, N.J.S.A. 2C:64-1 et seq. Prosecutors and investigators should consider Chapter 64 forfeiture possibilities with each search and seizure of computers. A more thorough treatment of Chapter 64 forfeiture is beyond the scope of this work.

Determining the computer's role also will force the affiant to address other critical issues prior to execution of the warrant. Among those issues is whether he can justify, based upon probable cause or practical considerations, seizing the subject's computer equipment and if so which of those components, such as the monitor or external memory would be covered. In drafting and executing a warrant, the recommended approach is to seize a component only if there is an independent reason justifying the seizure of that particular item. As will be discussed in more detail below, these reasons may include: (1) probable cause to believe that a particular component is subject to seizure under R. 3:5-2; and/or (2) the particular component is needed to safely, efficiently and successfully conduct the search.

Although computer searches and seizures may be more complex due to the technology involved, they are not constitutionally different from searches and seizures of traditional types of evidence. United States v. Upham, 168 F. 3d. 532 (1st Cir. 1999), cert. denied, __ U.S. ___, 119 S.Ct. 2353, 144 L.Ed. 249 (1999). Thus, an application for a warrant authorizing the search and seizure of computer equipment or information must satisfy the threshold requirements found in the federal and state constitutions.

1. Probable Cause Requirement

a. Probable Cause to Believe That a Crime has been Committed and That the Items Described in the Warrant are Connected to Criminal Activity

As for search warrants in general, an affidavit submitted in support of a warrant for the seizure of computer evidence must provide sufficient facts to establish a fair probability that a crime has been committed and that the items described in the warrant are connected to that criminal activity. However, where computer evidence is the object of a search, as a practical matter it is useful to allege additional facts which tie the crimes which are the subject of the warrant to the use of computers. In order to make this showing, the affiant should explain clearly the role of the computer in the offense that is under investigation.

An investigator's conclusions from the facts, based on his or her specialized training and experience, may be essential to establish probable cause to believe that a crime has been committed or that evidence of it may be found on a targeted computer. Cf. Ottensmeyer v. Chesapeake & Potomac Tel. Co., 756 F.2d 986 (4th Cir. 1985) (involving telecommunications fraud); United States v. Steerwell Leisure Corp., Inc., 598 F. Supp. 171 (W.D.N.Y. 1984) (involving copyright infringement of electronic video games). In order to justify a reviewing court's reliance on the special experience of an officer, care should be taken in drafting the warrant to ensure that the affidavit thoroughly sets forth: (1) all specialized training that the affiant may have received in either the use of

computers or investigation of computer crime; and (2) the affiant's law enforcement experience in general and specifically as it relates to investigations where computers were involved in the commission of the offense (i.e., type and number of investigations).

b. Probable Cause to Believe That the Materials to be Seized are to be Found at the Place to be Searched

The affiant will also be required to factually establish that the materials described in the warrant are to be found at the premise to be searched. In other words, the affidavit must establish a nexus between the criminal act and the target location. In drafting this portion of the affidavit, it is not necessary establish conclusively that the property being sought will be located in a certain place within the premise to be searched.

Whether the search involves computer equipment or information, reliable information in the affidavit stating that the items to be seized have been observed at the search site will establish probable cause. The more difficult situation is where such personal observation is lacking. In that case, it will be necessary for the affiant to provide other facts, such as that the items sought are records of a particular business, from which it can be inferred that the objects of the search will likely be found at the target location. The affiant also should consider citing tax laws and regulations, professional licensing regulations and other laws that require record keeping to establish that certain records should be at a particular location. See Andreson v. Maryland, 427 U.S. 463, 478, n. 9 (1976) (holding that records kept in the ordinary course of business may reasonably be expected to be maintained at business offices). In making this determination, a court can

also rely on the affiant's experience concerning where the particular objects of the search are normally kept. 2 W. LaFave, Search and Seizure: A Treatise on the Fourth Amendment, § 3.7(d) at 379 (3d ed. 1996) ["W. LaFave"].

2. Particularity Requirement

a. Generally

There are two separate but related issues which must be addressed in each search warrant in order to satisfy the particularity requirement found in the State and Federal Constitutions. First, the warrant must particularly describe the place to be searched. Second, the warrant must particularly describe the items to be seized. State v. Wright, 61 N.J. 146, 149 (1972).

In the relatively few cases that have addressed the issue of particularity in the context of computer search and seizures, defendants have not prevailed on those challenges. Nevertheless, the amount of information that can be stored on a computer system continues to increase in exponential proportions. As a result, particularly describing the items to be seized in a search warrant will become even more critical because computer searches and seizures increasingly will involve the seizure of non-evidential information which is intermingled with evidential information. Particularly describing the place to be searched has been further complicated by networking. Networked computer systems located at a search site can access information subject to seizure from other computers or servers located in different rooms, buildings, states and countries. In light of these realities, computer search warrants should be drafted with an awareness that particularity challenges to computer searches are likely to intensify and take on increased significance. See, e.g., In re Subpoena Duces Tecum, 846 F. Supp. 11,

12-14 (S.D.N.Y. 1994) (where the court quashed a grand jury subpoena for computer disks as over broad, reasoning that in order to avoid retrieval of irrelevant documents the subpoena should have specified certain categories of information rather than merely specifying the method of storage).

b. Description of the Place to be Searched

A search warrant must sufficiently describe the place to be searched so that the executing officer can reasonably ascertain its identity and location from the language of the warrant itself. Steele v. United States, 267 U.S. 498, 503 (1925).

(1) Tangible Objects

Property descriptions for searches and seizures of tangible computer equipment are not conceptually difficult since these items occupy physical space, which lends itself to description. Therefore, particularly describing the location of tangible computer equipment which is subject to seizure should be no different from describing the locations where other tangible evidence, such as narcotics, may be found.

(2) Intangible Objects

The increased use of networking has complicated the task of particularly describing the place to be searched when law enforcement intends to seize intangibles, such as computer data. In a networked environment, a computer containing relevant information may be connected to other computers and servers in a local-area network (LAN) spread throughout a floor, building or campus. LANs can be further connected to

wide-area networks (WAN), which span more than one physical location, or to global area networks (GAN) such as the Internet. Therefore, information that is particularly described in a warrant may be stored at the search site or at a remote location accessible to anyone within the network. Networking is not limited to large institutions. Individuals who own home computers can be connected to a network simply by adding a modem which can enable them to store information at some remote location. Therefore, it is critical to obtain intelligence prior to the execution of a search warrant concerning the type of computer equipment located at the search site and whether it is networked. Like hardware, however, if you can determine where the information is situated, particularly describing its location is no different than in any other type of search warrant.

(3) Multiple Locations

What if, prior to or during execution of a warrant, the executing officers decide to use computers located at the search site to access information situated in a server or computer at another location? Assuming that the computer or server is located in another room or office within the building being searched, the property description in the warrant should be sufficient to cover the search. See State v. Schumann, 156 N.J. Super. 563 (App. Div. 1978) (warrant to search entire residence and outbuildings upheld on showing that drug suspect had access to entire premises).

But what if the computer or server is located in a different building within the state? No authority was located which decided whether a second warrant is necessary.

The issue appears to be whether electronic information which is stored at a remote location but which may be accessed by a computer at the search scene is located only at the remote location or whether such information is located at both locations.[3] Because the issue has not been decided, a second warrant should be obtained.

When the server is located outside of the state, the issue of jurisdiction arises. That is, a New Jersey court can not authorize a search outside the territorial limits of New Jersey. See R. 3:1-2; N.J. Const. (1947), art. 6, § 3, ¶ 2 (providing that "the Superior Court shall have original jurisdiction throughout the State in all causes"). A search warrant should be obtained in the appropriate jurisdiction. Note that some jurisdictions require that the underlying crime or evidence thereof relate to a prosecutable offense under the laws of that jurisdiction. The state should request the assistance of the appropriate state or federal prosecutor's office and provide that office with the facts supporting probable cause to search the desired location and any other necessary

[3]Some support exists, by analogy, for the proposition that such a search and seizure occurs at the place where the information was accessed. In regard to wiretap interceptions, United States v. Rodriguez, 968 F.2d 130 (2d Cir. 1991), cert. denied, 506 U.S. 847 (1992), holds that a wiretap occurs in two places, the location where the telephone call was placed and the location where the law enforcement officers overheard the conversation. Hence, the interception may be authorized by a court of either jurisdiction. Similarly, the 1999 amendments to the New Jersey Wiretap Statute defines the "point of interception" as, "the site at which the investigative or law enforcement officer is located at the time that the interception is made." If this reasoning is applied to computer searches and seizures, it may be argued that electronic information is located both at the location of the server and at the location of the computer that can access it. Thus, a warrant to search the computer that can access the information may be found to be sufficient. A second search warrant is still advised, however, because a court may not be convinced that the situations are analogous.

information. The prosecutor's office will process the application and search warrant in accordance with the laws of their jurisdiction.

c. Description of the Items to be Seized

If there is probable cause to believe that evidence of a crime is to be found at a particular place, the affiant should be able to explain to the judge with some specificity what those items are. United States v. Lamb, 945 F. Supp. 441, 457 (N.D.N.Y. 1996). This requirement limits the possibility that members of law enforcement will engage in general searches and the seizure of items upon the mistaken assumption that they fall within the warrant. Marron v. United States, 275 U.S. 192 (1927). These dangers are particularly heightened in computer searches given the massive storage capacities of hard drives, disks and other storage media. See Voss v. Bergsgaard, 774 F.2d 402 (10th Cir. 1985) (warrant was over broad in that it authorized an unconstitutional "all records" search). It is not possible to discuss the particularity requirement in such a way as to provide a concrete description for every situation which may arise. The requisite degree of particularity will vary depending upon the extent of probable cause, the circumstances of each case, and the nature of the conduct under investigation. See State v. Wright, 61 N.J. at 149.

(1) Tangible Objects

In those situations where the State wants to seize tangible computer equipment, the description contained in the warrant should focus on the particular component involved and should be as specific as the circumstances permit. See State v. Tunnel Citgo Services, Inc., 149 N.J. Super. 427, 431 (App. Div. 1977) (holding that in order to satisfy the particularity requirement the description of items to be seized need only be as specific as the circumstances will allow). For example, where the object of the search is a stolen computer, the victim will likely be able to provide a very detailed description of the item. In other situations, however, it may only be possible to provide a more generalized description. Hence, if the target of an investigation has been using his computer to distribute child pornography on the Internet but investigators have never been inside his home, it is not possible to describe the target's computer equipment with the same degree of particularity as in the case of a stolen computer. In this situation, however, the affiant can explain in the affidavit the minimal amount of equipment necessary to commit this crime. A general description of this equipment should be sufficient since it is as specific as the circumstances allow.

(2) Intangible Objects

Information located on computer data storage media should be described with the same degree of specificity as documents which are stored in filing cabinets or drawers. "Descriptions [of records] so sweeping as to authorize a general, exploratory search have

been condemned[.]" 2 W. LaFave, § 4.6(d) at 570. Nonetheless courts have approved generic descriptions of documents where the identity of the items could not be more specifically described at the time the warrant was issued. See State v. Tunnel Citgo Services, Inc, 149 N.J. Super. at 431. Moreover, the particularity requirement is somewhat relaxed where a complex investigation is involved. United States v. Henson, 848 F.2d 1374, 1383 (6th Cir. 1988), cert. denied, 488 U.S. 1005 (1989). Therefore, if the affiant knows exactly which documents are sought, they should be described with as much specificity as possible, including the date, author, subject, type of document, etc. If the affiant knows the general nature of the information sought, the description of the documents may be more general but it must be accompanied by some type of limiting phrase consistent with the scope of probable cause. Like drafting any other warrant, a warrant authorizing the seizure of documents found on computer storage media should be tailored according to the scope of probable cause and the nature of the conduct under investigation.

Courts have held that as long as a warrant particularly describes the documents or information to be seized, it need not describe how these materials are stored (i.e., on computer storage media).[4] The more prudent course, however, is to particularly describe

[4]United States v. Musson, 650 F. Supp. 525, 532 (D. Colo. 1986) (warrant that described the items to be seized as documents in the names of certain individuals or entities permitted the search and seizure of 54 computer disks that could contain such materials); United States v. Sissler, No. 1:90-CR-12, 1991 WL 239000 (W.D. Mich. Aug. 30, 1991) (unpublished decision), aff'd, 966 F.2d 1455 (6th Cir. 1992), cert. denied, 506 U.S. 1079 (1993) (warrant that described the items to be seized as records of

the contents of the documents to be seized and more generally describe the computer storage media on which these materials may be found. In re Application of Lafayette Academy, Inc., 610 F.2d 1 (1st Cir. 1979). Further, it is important to recall that the state will want to retain all original data storage media which contain any of the evidence described in the warrant, even though the data storage media may contain other data outside the scope of the warrant. See sections IV and V, infra. Therefore, the warrant should be drafted to authorize the state to seize not just the particularly described documents, but also any data storage medium which contains any of the particularly described documents so that there is no question that the storage medium itself may be seized.

d. Summary

The search warrant affidavit therefore should include an explanation of why there is probable cause to believe that the relevant information is subject to seizure under R. 3:5-2; an explanation of why there is probable cause to believe that the relevant information may be found at the place to be searched; a particular description of the place to be searched, and the type of information sought (i.e., tax records, records relating to drug distribution, etc.); if possible, a description of the form which the relevant records

---

drug transactions also authorized the search and seizure of 500 computer disks and three personal computers that could contain such materials); United States v. Reyes, 798 F.2d 380, 382-83 (10th Cir. 1986) (warrant that described the items to be seized as "drug trafficking records, ledgers, or writings identifying cocaine customers" also authorized the search and seizure of a cassette tape containing discussions concerning the sale of drugs).

may take or the manner in which the records may be stored (i.e., hard copy, electronic form such as disks, cd's, hard drives, electronic tape media, photographic form, etc.); and, in appropriate cases, an explanation justifying the seizure of hardware, software and manuals necessary for off-site searches for information. See infra sections IA6 (On-Site/Off-Site Searches), IIA7 (Authorization to Take Equipment), and IIC (On-Site Review is Impractical).

3. Deleted, Encrypted or Password-Protected Data

Members of law enforcement have access to software programs designed to retrieve data that has been deleted but not overwritten. The normal command used to delete a file from a disk (either a floppy or a hard drive), does not, itself, eliminate the information in the file from the disk. This command merely deletes the name of the file from the directory or index of files in the computer's memory. As a result, the files remain on the disk until subsequent usage requires the storage space occupied by the "deleted" file, at which time the file is overwritten by the new data and thereby is erased.

Does the seizure of computer evidence pursuant to a validly issued warrant carry with it the right to use available scientific methods to retrieve data which was intentionally deleted by the user, without obtaining a second warrant? What about encrypted or password-protected data? One court specifically addressed this issue with respect to intentionally deleted data and held that a warrant generally authorizing the search of a computer was sufficient to authorize police to recover deleted data.

Commonwealth v. Copenhefer, 526 Pa. 555, 562, 587 A.2d 1353 (1991) (holding that the seizure of deleted files pursuant to the original warrant was constitutional since defendant's attempt to secrete evidence was not equivalent to a legally protected expectation of privacy). See also United States v. Simpson, 152 F.3d 1241, 1248 (10th Cir. 1998) (warrant authorizing seizure of computer and diskettes adequate to authorize search of the hard drive); Commonwealth v. McEnany, 446 Pa. Super. 609, 621, 667 A.2d 1143 (1995) (additional warrant not required to search the memory chip of a cellular phone seized pursuant to a search warrant because police are authorized to use technologically advanced analysis techniques on validly seized physical evidence) app. dism., 547 Pa. 159, 689 A.2d 223 (1997); State v. Petrone, 161 Wis.2d 530, 544-45, 468 N.W.2d 676, 681 (1991) (rolls of undeveloped film seized pursuant to a warrant could be developed without obtaining a second warrant). Accord State v. Reldan, 100 N.J. 187, 195 (1985) (an analysis of the reasonableness of the methods used in the search focuses on whether they were consistent with the object of the search).

Although Copenhefer has been criticized for its failure to cite any pertinent case law in support of its dismissal of the defendant's Fourth Amendment challenge, See Krivulka, Constitutional Law -- Limits of Privacy Expectations Within Seized Electronic Data, 65 Temp. L. Rev. 645, 655 n. 97 (1992), it can be argued that its holding is supported by Reldan and the line of state and federal cases upholding the constitutionality of searches of containers uncovered during a lawful search. Searching a deleted file on a

data storage medium is analogous to searching a locked briefcase, filing cabinet or room found in a house. It is well-settled that law enforcement officers who find a container while executing a warrant at a location do not need to obtain a second warrant to search the container if it is reasonable to believe that objects named in the initial warrant could be found therein. United States v. Ross, 456 U.S. 798, 824 (1982).

Recently in United States v. Upham, 168 F. 3d. 532 (1st Cir. 1999), cert. denied, __ U.S. ___, 119 S.Ct. 2353, 144 L.Ed. 249 (1999) the Court upheld the seizure of deleted files from a computer even though their seizure was not specified in the warrant, The Court reasoned that the recovery of deleted images on a computer was no different than decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note. The Court noted that search warrants primarily concentrate on identifying what may be searched and whether there is sufficient cause for the invasion of privacy, rather than the mechanics of the search warrant execution. Id. at 5.

"Although Article I, ¶ 7 of the New Jersey Constitution may very well afford our citizens greater protection against unreasonable searches and seizures than does the Fourth Amendment (See State v. Hempele, 120 N.J. 182 (1990) and cases cited therein) neither public policy nor New Jersey decisional law compel a result different from the federal authorities cited above." State v. Jackson, 268 N.J. Super. 194 (Law Div. 1993) (warrant to search a third floor attic for evidence of violations of the Controlled

Dangerous Substance Act authorized search of a locked safe found hidden in a cardboard box that was located in a locked storage closet).

Based upon this analogous precedent, it appears that if a valid search warrant authorizes the search of data storage media for particularly described information, then the search of a deleted, encrypted or password-protected file on a data storage medium found at the search location is within the scope of the warrant, because it is reasonable to believe that the object of the search will be found therein. Whenever practicable, the application and search warrant should contain language pertaining to the seizure of encrypted and deleted information. See Sample Warrant in Appendix.

4. When to Serve the Warrant

It sometimes may be desirable to conduct a search for computer evidence when the subject is not at the search site. For example, the investigator may have information suggesting that the subject will destroy computer evidence if he is present during execution of the warrant. In those cases the state may seek permission, based upon good cause, to execute the warrant at any time of the day or night. See R. 3:5-5(a). As a result, the affidavit should provide a factual basis as to why the presence of computer users might lead to the destruction of valuable evidence.

5. "No-Knock" Authority

Technically adept suspects may rig their computers in an effort to hide or destroy evidence. Two common methods involve hot-keys and time-delay functions. A hot-key program destroys data, usually by overwriting or reformatting a disk, when a certain key is pressed. (Experts can sometimes recover data which has been overwritten or deleted.) A time-delay program monitors keyboard activity and starts to destroy data if no key is pressed within a certain period of time. The suspect then could admit the investigators, but delay them from reaching the computer, to allow the destruction process to occur.

If investigators have specific, articulable facts which show that the particular targets of the search may destroy data, or which make a no-knock warrant appropriate for some other reason, the investigators should include those specific facts in the affidavit and seek a no-knock warrant. See State v. Jones, 143 N.J. 4, 18 (1995); State v. Fair, 45 N.J. 77, 86 (1965). Even without prior court authorization, investigators can execute a warrant without knocking if the circumstances they find when executing the warrant fall within one of the categories enumerated in State v. Jones, 143 N.J. at 18. See State v. Love, 233 N.J. Super. 38, 43 (App. Div. 1989), certif. denied, 118 N.J. 188 (1989). Otherwise, the warrant should be executed in the normal manner, with the computer evidence specialist detailed to promptly assess the computer system for the possibility of data destruction.

6. On-Site/Off-Site Searches

Since computers and computer peripherals store large volumes of information in the form of electronic data, it may be impossible or impractical to identify which electronic data stored within a computer is within the parameters of a search warrant on site during its execution.[5] Also, depending on the systems encountered, it may be technically impossible to copy the information without seizing the computer and peripherals for later analysis.[6] See United States v. Hunter,13 F.Supp.2d 574, 583-84 (D. Vt. 1998).

Therefore, it often will be necessary to seize computer hardware (the computer and its peripheral devices) for an off-site search to determine (1) what specific electronic data is stored within the computer; and (2) whether the electronic data seized by taking the computer, its peripheral hardware, floppy disks, etc., is within the parameters of the search warrant.

---

[5]Note that there may be instances where it is appropriate to seize all records of a business, and thus, all records on the computer would be within the scope of the warrant. Where fraud so pervades a business that all records may be evidential of the crime, courts have upheld a seizure of all business records. See, e.g., United States Postal Service v. C.E.C. Services, 869 F.2d 184 (2d Cir. 1989); United States v. Brien, 617 F.2d 299, 308-09 (1st Cir. 1980), cert. denied, 446 U.S. 919 (1980).

[6]Another reason for seizing the computer equipment will be to allow a computer expert to examine the equipment to determine whether the system was operating properly at the time the data stored within it was created. This may defeat claims that the data stored within was created through equipment malfunction or error.

It does not appear that any New Jersey appellate court has addressed the Fourth Amendment issues raised by seizing computers and stored electronic data for an off-site search. Several federal cases, discussed further below, have examined the issue, and they suggest the following approach. United States v. Upham, 168 F. 3d. 532 (1st Cir. 1999), cert. denied, __ U.S. ___, 119 S.Ct. 2353, 144 L.Ed. 249 (1999); United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996); and United States v. Kimbrough, 69 F.3d 723 (5th Cir. 1995), cert. denied, 517 U.S. 1157 (1996). First, the affidavit of probable cause should include specific facts justifying the off-site search. These should include facts specific to the computer or business to be searched and general facts related by an investigator trained in computer evidence recovery, regarding the necessity of examining data in a controlled lab. The warrant should authorize seizure and off-site searching. See Section II C (relating to when On-Site review is impractical).

Second, regardless of whether the warrant specifically permits an off-site search, if evidence is seized for off-site searching, reports must be written detailing the facts and circumstances that necessitated the action. See Section II D (relating to documenting searches). Courts will consider the following circumstances, among others, in assessing the reasonableness of the seizure:

a. The practicalities of searching voluminous records on-site as opposed to off-site;

b. The means and methods of executing the search by law enforcement -- did the searchers conduct a general search and simply take everything, or were any efforts made to review material, such as non-computerized evidence, and leave behind those materials which were clearly not within the scope of the search warrant?

c. Whether the affidavit of probable cause offers any factual basis upon which the judge could sanction the seizure and off-premises search?

d. Whether there is any evidence that the targets intentionally mislabeled files, computer disks, etc., so law enforcement had to examine each one to determine whether it was evidential?

e. Whether the targets used passwords, codes, etc., that prevented law enforcement from searching on-site?

f. The amount of time which would be required to conduct the search on-site; and

g. The quantity of items seized and searched off-site that were returned to the target/defendant and the time that elapsed between the seizure and the return of these items.

Federal cases supporting this approach are discussed below.

In United States v. Upham, 168 F. 3d. 532 (1st Cir. 1999), cert. denied, __ U.S. ___, 119 S.Ct. 2353, 144 L.Ed. 249 (1999). Customs agents investigating child pornography obtained a warrant to search a home for "any and all computer software and

hardware, . . . computer disks, disk drives . . . and any and all visual depictions in any format or media of minors engaging in sexually explicit conduct." The Court found: (1) that the warrant was not over broad, stating that the seizure and subsequent off-site search of the computer and all available disks was the narrowest definable search and seizure reasonably likely to obtain the evidence sought; that a sufficient chance of finding some needles in the computer haystack was established by the probable cause showing in the warrant application; and that the search of a computer and co-located disks was not inherently more intrusive than the physical search of an entire house for a weapon or drugs. Id. at 3.

Turning to whether the off-site search of the computer was appropriate, the Court noted that had the images been easily obtained though an on-site inspection, there might have been no justification for allowing the seizure of all the computer equipment. However, since the scope of the search included deleted images on a "well-laden" hard drive, and the mechanics of retrieving such images could not have been done at the search warrant location, removal of the computer to an off-site location was appropriate.

In United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996), FBI agents investigating child pornography obtained several search warrants. One warrant was obtained to search America Online (AOL) offices in Vienna, Virginia for records of 78 subscribers' accounts including Lamb's. Another warrant was obtained to search Lamb's home. The warrants sought floppy disks, stored e-mail messages, all stored files in

original format in individual files and any print-outs of same, image files[7] and files pertaining to log-on activities of the 78 targets, in addition to business records, actual and screen names, account numbers, addresses and phone records, among other items. The defendant generally alleged that the searches violated the Fourth Amendment apparently on the grounds (although the precise grounds were not clearly stated in the opinion) that the items sought were not relevant to the crime, were not potentially evidence or instrumentalities thereof and were not particularly described.

In upholding the search of AOL's records, the Court noted that the language of the affidavit and warrant did not limit the agents to seizing only image files or image files relating to child pornography, and concluded:

> [The] actual content of a computer file can usually not be determined until it is opened with the appropriate application software on [another] computer. The agents who were tasked to obtain account records related to seventy-eight individuals were not obligated to identify the contents of computer files on AOL's premises. [Citation omitted.] Because there was probable cause to believe that stored files in the accounts of the suspects contained evidence of the crime, viz. the depictions of child pornography themselves, the warrant properly authorized the search and seizure of these particular items. [United States v. Lamb, 945 F. Supp. at 459.]

With respect to the search warrant executed by the FBI at defendant's home, which apparently included a search and seizure of the defendant's computer, the Court rejected

---

[7]Image files are photographs or videotapes that are scanned or transferred to a computer by a number of technological means. These files can then be transmitted over a modem to other computers. Another program known as a viewer is required to display the image files on the monitor. Image files can include any picture, not only pornography.

defendant's argument "that the seizure of the computer is not the seizure of 'evidence' or 'instrumentalities', but rather that the material on the hard drive is the material that is the instrumentalities and fruits." In other words, the Court rejected the defendant's contention that the FBI could not seize the computer but could only seize the "material on the hard drive," i.e., the electronic data, because only the electronic data was evidence.

Specifically, the Court addressed the defendant's argument by stating:

> First, the computer may very well be an instrumentality of the crime, if it were the one being utilized to send and receive the image files of child pornography over AOL. And second, if some of the image files are stored on the internal hard drive of the computer, removing the computer to an FBI office or lab is likely to be the only practical way of examining its contents. This court has learned that FBI procedure for examining what is stored in a computer involves making a backup copy of the entire hard drive of the system. They then may run programs to recover deleted files. All the image files would have to be viewed in order to see if they contain the proscribed depictions. Like viewing the 31 seized files, examining the computer is not a task that can easily or pragmatically be done at the premises being searched, as is explained by Agent Pollitt in Agent Dwyer's affidavit. Computers [sic] image files and videotapes are different media than magazines. While agents may be able to determine if the latter contain child pornography depictions simply by flipping through the pages, newer technology presents different exigencies. [Id. at 462-63 (emphasis added).]

Prosecutors and investigators should note that the Lamb Court specifically referred to the fact that the FBI agent explained in the affidavit of probable cause that it was impractical to examine the computer on the premises and the examination would have to be done off-site.

Similarly, in United States v. Kimbrough, 69 F.3d 723 (5th Cir. 1995), cert. denied, 517 U.S. 1157 (1996), another child pornography case, U.S. Customs agents obtained search warrants for computer evidence.[8] Kimbrough challenged the execution of the search warrant on the grounds that the agents executing the search warrant did not review each video tape, audio tape and document but seized the items for an off-site search.

In response to this challenge, the Court noted that: (1) a significant number of documents were left on the scene after initial review showed that they were outside the scope of the warrant; and (2) the defendant did not point to specific examples of seized items that would demonstrate an absence of the executing officers' good faith belief that the items were described in the warrants. Id. at 728.

[8]The Court noted that the U.S. Customs agents sought, "Tapes, cassettes, cartridges, streaming tape, commercial software and manuals, hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media-floppy disks, CD ROMs, tape systems and hard drive, other computer related operational equipment, and other similar materials in addition to, magazines, photographs, negatives, photographic slides, video cassette tapes or other visual depictions or equipment used to visually depict a minor engaging in sexually explicit conduct, and, bills, correspondence, receipts, ledgers, Postal receipts and telephone records all of which show orders and deliveries to or from any known foreign or domestic distributor of child pornography." Id. at 727.

In a case involving a search warrant for both marijuana and records, United States v. Sissler, No. 1:90-CR-12, 1991 WL 239000 (W.D. Mich. Aug. 30, 1991) (unpublished decision), aff'd, 966 F.2d 1455 (6th Cir. 1992), cert. denied, 506 U.S. 1079 (1993), the Court rejected defendant's claim that the officers disregarded the terms of the search warrant and conducted an impermissible general search.

The District Court considered the large volume of records on the premises, the "clutter" and the number of records seized, and concluded that the search off-site was justified. The Court stated that "under the circumstances, it would be unreasonable to hold that the law enforcement officials were required to carefully review each document in every file they uncovered. [Citation omitted]. Rather they were only required to have a reasonable belief that a file or collection of papers found in the clutter contained records that were covered by the warrant." Id. at 3.

The District Court further addressed the seizure of nearly 500 computer disks and a personal computer. Defendant argued that the seizure of the information on the disks and in the computer was not authorized by the search warrant. The Court stated:

> In addition to the large number of documents, nearly five hundred computer disks and a personal computer were also taken. Many of the disks contained information whose seizure was not authorized by the search warrant. Law enforcement officers are permitted to search any container found within the premises if there is reason to believe that the evidence sought

> pursuant to a warrant is in it. [Citation omitted.] The police were permitted to examine the computer's internal memory and the disks since there was every reason to believe that they contained records whose seizure was authorized by the warrant. Furthermore, the police were not obligated to give deference to the descriptive labels placed on the disks by [defendant] Baldori. Otherwise, records of illicit activity could be shielded from seizure by simply placing an innocuous label on the computer disk containing them. The police also were not obligated to inspect the computer and disks at the Baldori residence because passwords and other security devices are often used to protect the information stored in them. Obviously, the police was [sic] permitted to remove them from the Baldori residence so that a computer expert could attempt to 'crack' these security measures, a process that takes some time and effort. Like the seizure of documents, the seizure of the computer hardware and software was motivated by considerations of practicality. Therefore, the alleged carte blanche seizure of them was not a 'flagrant disregard' for the limitations of a search warrant. [United States v. Sissler, 1991 WL 239000 at p.3 (emphasis added).]

In yet another case involving the seizure of and off-site search of a computer, United States v. Yung, 786 F. Supp. 1561 (D. Kan. 1992), the defendant contended that an IRS agent went beyond the scope of the search warrant because items not listed in the warrant were seized including video tapes (which tapes were not related to the matter under investigation).

The Yung Court held that seizure of items outside the scope of the search warrant did not invalidate the search. It also noted that video tapes and computer files could not

be individually reviewed prior to the completion of the search. The Court specifically noted that the IRS agent testified that many of the seized items had been returned. Finally, the Court cited Marvin v. United States, 732 F.2d 669 (8th Cir. 1984), and stated that "the extensive seizure of certain types of items was prompted largely by practical considerations and time restraints." Yung, 786 F. Supp. at 1569 (emphasis added).

Based on these cases, it appears courts will sanction the seizure and off-site search of computers, computer peripherals and stored electronic data under the proper facts. The affidavit of probable cause should set forth facts justifying an off-site search and the warrant should authorize it. Reports documenting the execution of search warrants where computers are seized and off-site searches conducted should address all of the facts which establish the impracticality of conducting the computer search on-site.

7. Authorization to Take Computer Peripherals and Documentation

If the State intends to remove the computer from the site for later searching, it should seize all input and output devices, manuals and software and hardware documentation that are reasonably necessary to safely, efficiently and successfully conduct the search.

The input and output devices necessary to operate the computer system, and thus conduct the search, will vary with the computer system. For a simple PC, such devices often will include, in addition to the CPU, the monitor, keyboard, mouse and all external data storage devices.

The justification for seizing such peripherals is that the investigator who will examine the system will need to properly reconfigure the system at the lab in order to read data from it. It will be practically impossible for the specialist to make the system operational if only the CPU or hard-drive is seized. Many pieces of hardware are incompatible with each other. An ever-increasing array of components exist on the market, and hardware and software constantly become obsolete. The most practical way to ensure that the specialist will be able to conduct a search of the computer at the lab is to seize all input and output devices reasonably necessary to make the computer system operational.

Similarly, when investigators will be seizing a computer for off-site searching, they should ask for authority to seize all documentation which explains the hardware and software being seized. Documentation found at the scene may be key to reassembling the computer system, operating it, and using the software on the machine properly.

This discussion does not mean that other computer components which are not necessary to operate the system are exempt from seizure. It only means that some basis for seizing them should be articulated. For example, if the crime consisted of creating fraudulent invoices, then it may be reasonable to seize a printer as evidence to show that the defendant had the ability to create them. If the crime consisted of uttering falsified documents by fax machine or over telephone lines, then a fax machine or external modem could be seized as evidence of the crime.

8. Supplemental Warrant Applications

It will not always be possible to develop detailed factual information about the computer and computer system being utilized prior to executing a search warrant. The probability of encountering a computer or computer system not previously known to exist during the execution of a search warrant is high. Searchers also may encounter computers being utilized to commit crimes different from those detailed in the search warrant. Given that the electronic data stored within any computer or computer system is easily altered or deleted, exigent circumstances may arise requiring law enforcement to obtain additional search warrants on an emergent basis.

Written search warrant applications are preferred, but where exigent circumstances are present, an oral search warrant may be obtained. State v. Valencia, 93 N.J. 126 (1983); State v. Speid, 255 N.J. Super. 398 (Law Div. 1992); State v. Liberti, 161 N.J. Super. 575 (App. Div. 1978), certif. denied, 79 N.J. 502 (1979). Oral search warrants are

sanctioned by R. 3:5-3(b) and the rule has detailed requirements. Since strict compliance with R. 3:5-3(b) is required (see the cases cited above), prosecutors and investigators should be thoroughly familiar with these requirements.

B. WARRANTLESS SEARCHES & SEIZURES

As stated previously, search warrants are always preferred. Nonetheless, because a criminal investigation is a search for the facts, situations will be encountered which could not have been addressed in the warrant. If emergent circumstances exist and a written application is not possible, an oral or telephonic warrant should be considered.

The risks involved in seizing evidence without judicial authorization should be recognized. Unless a court later finds that some exception to the warrant requirement justified a seizure of items outside of the warrant, these items will not be admitted as evidence. If a warrantless seizure is contemplated, prosecutors and investigators must evaluate whether the anticipated search and seizure falls within a specified exception to the warrant requirement. Searches conducted without a warrant are presumed illegal. State v. Jones, 143 N.J. 4 (1995). The state must demonstrate the search falls within one of the specified exceptions to the warrant requirement. State v. Hill, 115 N.J. 169, 173 (1989).

The warrant exceptions that seem most likely applicable to computer searches are discussed below.

1. Plain View

Evidence of a crime may be seized without a warrant under the plain view exception if (1) the officer is legally in a position to view the evidence; (2) the discovery of the evidence is inadvertent; and (3) it is immediately apparent to the officer that the objects in view are associated with criminal activity. State v. Bruzzese, 94 N.J. 210, 213 (1983), cert. denied, 465 U.S. 1030 (1984), citing Coolidge v. New Hampshire, 403 U.S. 443 (1971). The law enforcement official need not be certain that the seized item is evidence of a crime, rather there must be a "practical, nontechnical probability that incriminating evidence is involved." Bruzzese, 94 N.J. at 237, citing Texas v. Brown, 460 U.S 730, 738 (1983). In determining whether the law enforcement official had probable cause to associate the item with criminal activity, the court considered what the officer reasonably knew at the time of the seizure. Bruzzese, 94 N.J. at 237.

In Horton v. California, 496 U.S. 128 (1990), the Court found that even though inadvertence was a characteristic of most legitimate plain view seizures, it was not a necessary condition. Since Horton was decided, New Jersey state courts have not expressly decided that inadvertence was a separate requirement under the state constitution. See State v. Damplias, 282 N.J. Super. 471, 478 (App. Div. 1995) (court did not need to rule on the necessity of the inadvertence requirement because the requirement had been met).

In any event, the inadvertent discovery requirement usually will be met if the other requirements for plain view are present. Discovery of evidence is deemed to be inadvertent for purposes of the plain view doctrine even if the officer knew of the existence of the evidence seized, so long as he had no prior intent to seize it. Id. at 478-79. In other words, the plain view exception will not justify a warrantless seizure if the search was begun on a "pretext" and the officer's "real goal" was to seize the evidence in question without a warrant. Id.

Seizure of computer evidence may be justified under the plain view exception if evidence outside the scope of the warrant is discovered by an officer who viewed the evidence from a lawful vantage point. For example, if some additional evidence is discovered during a search of computer data, its seizure may be justified pursuant to the plain view exception. However, if there was no authority to search the computer, discovery of incriminating information in the computer could not be justified as plain view because the evidence was not discovered from a lawful vantage point. Moreover, care should be taken where the evidence discovered is outside the scope of the warrant. For example, in the case of United States v. Carey, 172 F.3d 1268 (10th Cir. Kan. 1999), the Court suppressed evidence of child pornography where a police officer searching a computer on a warrant looking for evidence of narcotics trafficking, found the images and abandoned his search for narcotics evidence.

2. Exigent Circumstances

A warrantless search or seizure is justified if exigent circumstances exist such that the police do not have time to secure a warrant. Warden v. Hayden, 387 U.S. 294, 298-300 (1967); State v. Lewis, 116 N.J. 477 (1989). For the seizure to be valid, there must be probable cause to believe that the item seized is evidence of a crime and that destruction of evidence is imminent -- so imminent that a warrant could not have first been obtained.[9] In determining whether exigent circumstances justified a warrantless search and seizure, courts have considered the following: the degree of urgency and the time necessary to get a warrant; reasonable belief that evidence is to be removed or destroyed; and the ready destructibility of the evidence. State v. Valencia, 93 N.J. 126, 137 (1983) (citing United States v. Manning, 448 F.2d 992, 998-99 (2d Cir. 1971), cert. denied, 404 U.S. 995 (1971)).

Because this exception is premised on the police's inability to procure a warrant without risking a loss of evidence, the seizure permitted is limited to that which is necessary to prevent the destruction of evidence. See State v. Stupi, 231 N.J. Super. 284 (App. Div. 1989) (exigent circumstances permitted police to enter and secure the premises but did not permit the search of a closed cabinet); State v. Jackson, 268 N.J. Super. 194

[9]In addition to the destruction of evidence, other exigent circumstances also may permit a warrantless search or seizure. These include the pursuit of an armed felon or the need to render assistance to an injured person. The destruction of evidence exception is discussed because it appears to be most applicable to the seizure of computer evidence.

(Law Div. 1993) (exigent circumstances permitted police to enter a dwelling to arrest defendant but did not permit a warrantless search of a locked attic room).

Where computer data is involved, the easy destructibility of evidence, along with other circumstances showing a specific risk that evidence will be destroyed, may allow a limited warrantless seizure. Once the evidence is secured, a further warrantless search of the contents of the computer usually will not be justified under this exception. However, securing a computer may involve more than just guarding it; it could conceivably require taking other steps to disable a computer or otherwise preserve its data, particularly if the circumstances show that the contents of the computer can be accessed from a remote location.

A federal case has permitted a warrantless seizure of a computer based on exigent circumstances. United States v. David, 756 F. Supp. 1385 (D. Nev. 1991). When a witness began deleting information from a computer "memo book" (perhaps akin to a "notebook" computer), the David Court found its immediate warrantless seizure reasonable to prevent the destruction of evidence. However, once the evidence was secured from destruction, a warrant was required to search the computer's contents. Id.

3. Consent

A search of property without a warrant and without probable cause is valid under the Fourth Amendment if proper consent is given. United States v. Matlock, 415 U.S. 164, 165-66 (1974); State v. Douglas, 204 N.J. Super. 265, 276 (App. Div. 1985), certif. denied, 102 N.J. 378 (1985) and 102 N.J. Super. 393 (1986). To be effective, consent must be voluntarily given and, in New Jersey, the state must establish that the consenting person was aware of the right to refuse to consent to the search. State v. Johnson, 68 N.J. 349, 354 (1975); State v. Suazo, 133 N.J. 315 (1993). Consent to search may be expressly given or may be implied from the circumstances. State v. Suazo, 133 N.J. at 322.

a. Scope of Consent

The consenting party may explicitly limit the scope of his consent and also may withdraw his consent. A consent search can go no further than the permission given. For example, if consent to search is expressly limited to the search of a single file or a certain computer, that is all that may be searched pursuant to the consent. Similarly, where consent is withdrawn, the search must stop. If probable cause exists that the computer contains other evidence beyond the scope of the consent and destruction of evidence is possible, the evidence should be secured while a warrant is obtained.

A consent based search is limited to the scope of the consent given. Where a cooperating witness has agreed to provide authorities with information which the witness

himself accessed on his computer through the use of a password, a court held that an officer's later search of the password-protected computer was invalid. United States v. David, 756 F. Supp. 1385 (D. Nev. 1991). The Court found that the later search went beyond the scope of the consent given, particularly since the witness did not provide the password to the agents. Id. at 1391-92.

b. Who May Consent

Consent may be obtained from the owner of the property, from a third party who possesses common authority over the property or a sufficient relationship to the property, or from a person whom the police reasonably believe has the authority to consent to search. State v. Maristany, 133 N.J. 299 (1993); State v. Coyle, 119 N.J. 194, 215 (1990).

Common authority arises not merely from the consenting party's ownership or property interest in the place or thing to be searched but also from his joint access or control. The apparent authority doctrine may allow a search on the consent of a third party who has no actual authority to consent, so long as the police reasonably believe based on the circumstances presented that the third party has the authority to consent. State v. Maristany, 133 N.J. at 305-06.

(1) Family Members and Cohabitants

Under the common authority doctrine, spousal consent to search marital property is usually effective. Moreover, in the absence of objective evidence that the consenting spouse was denied access to the property, investigators reasonably may assume that spouses have authority to consent to a search of anything on the marital property. It seems to follow that a spouse may consent to the search of a computer -- even one he or she does not use -- unless it appears that the spouse was denied access to it. See, e.g., United States v. Duran, 957 F.2d 499, 504-05 (7th Cir. 1992). In the context of a computer search, access may be denied by the use of passwords or other access codes.

Under the common authority doctrine, a parent may consent to a search of common areas of a family home. New Jersey is among the overwhelming majority of courts holding that a parent has the right to consent to the search of the property of a minor child. 3 W. LaFave, § 8.4(b), State v. Douglas, 204 N.J.Super. 265 (App.Div. 1985) certif. denied, 102 N.J. 378 (1985) and 102 N.J. 393 (1986) (holding mother could consent to the search of her minor son's bedroom). Parental consent to search a child's room is based on the parent's authority as head of household or owner of the property, as an exercise of parental authority over the minor, or as a cotenant or common resident. Id. at 279. The court in Douglas discussed In the Interest of Sayler, 44 Ill.App.3d 854 (Ill.App.Ct. 1977), cert. denied, 434 U.S. 925 (1977) wherein a mother's consent to search her minor son's bedroom was upheld even though: the son kept a combination lock

on the outside of the room; the encoded combination was written down over the door; the door had an interior lock; the mother gained entrance only by knocking; the son cleaned his own room delivered his laundry to his mother; and the mother had been in the son's room only three times in the previous three months. The court found that implicit in the rights and duties of a parent is the right to exert parental authority and control over a minor's surroundings, including the minor's room. However, the court noted that there was no showing of any instruction to the mother to let no one else enter the room.

Although it appears that courts may uphold parental consent of the locked room of a minor child, parental consent to search a minor child's computer unit, peripherals and password protected documents has not been tested. When confronted with this issue, the following factors should be considered: (1) who purchased the computer; (2) does the parent have access to the computer; (3) is the computer password protected, and if so, does the parent have access to the password; (4) is the password publicly posted; (5) has the minor child prohibited the parent from using the computer; and (6) does the child contribute to rent and/or utilities for use of the room. In sum, absent a compelling argument against parental common authority over a minor's computer system, parental consent to search a minor child's computer system will probably be valid.

Even in cases where the child has reached adulthood, courts have been reluctant to find that the child had exclusive possession of a room in the parent's home. State v. Crumb, 307 N.J.Super. 204, 704 A.2d 952, (upholding validity of parent's consent to a search of adult son's room), certif. denied, 153 N.J. 215 (1998), citing 3 LaFave, supra, § 8.4(b), at 769. In determining whether an adult child had exclusive possession of a room, the courts have considered: (1) whether the child paid rent and/or utility bills; (2) whether the parent had access to the room; and (4) whether the parent had access to the room to clean it. Crumb, 307 N.J. Super. at 244. The same concerns would apply to roommates, siblings and other cohabitants. However, where there is multiple control over property, any party in possession has the right to consent to a search. State v. Santana, 215 N.J.Super. 63, 69 (App.Div. 1987).

(2) Employers

Employers may be able to permit a search of work-related materials used by an employee since the employer likely has common access or control, if not superior rights, to work-related materials. An employer may consent to a search of an employee's computer and computer data if he has common authority over them. However, not everything that passes through the workplace can be considered part of the workplace. See O'Connor v. Ortega, 480 U.S. 709 (1987). A search of personal property may not be permissible. Whenever practical, investigators should ascertain whether employers have given notice to employees that employee personal information stored on their computers

is subject to review. When executing a search warrant, investigators should also take special care to avoid personal belongings of employees that are not covered by the search warrant.

c. Passwords and Encrypted Documents

Where the subject of the search has taken special steps to secure the property to be searched, evaluation of the effectiveness of the consent to search will depend on the scope of the consent, the status of the consenting party and the nature of the property to be searched. If a party turns over his computer for a full search, it would appear that this would include a search of data which is password protected.

Where a third party offers consent to search a computer, his consent would extend to the documents, files or directories he reasonably appeared to have joint access to or control over. A third party may or may not be able to consent to a search of password-protected materials on the computer. Resolution of this issue will turn on the surrounding circumstances, including whether the consenting party had access to the password or whether the password was commonly known or available.

Encrypted documents pose a slightly different problem. Although encrypted documents are similar to password-protected documents in that they are not immediately readable, there is a difference between them. The encrypted document is not hidden from view. An argument exists that the subject did not choose to segregate or lock the document behind a password. Instead, he left the document open to inspection and

copying and apparently assumed the risk that its meaning could be deciphered by someone who "broke" the code or ran a decryption program. Under this theory, it might be argued that a third party with access to an encrypted document can consent to a seizure of the encrypted document. However, there is no precedent to support this view. A court could find that the subject of the search took steps to keep secret the content of the encrypted document, and hence, the consenting party lacked authority to consent to a violation of this expectation of privacy.

d. Networks

As a practical matter, system administrators of workplace networks can look at the data kept by network users. Applying the principles of the consent doctrine, it can be argued that administrators can consent to a search because they have control over the data and the users assume the risk that others can access their data. No precedent has been located to support this proposition. This situation seems analogous to an employer providing paper files or documents made by the employee in the course of his employment duties but stored in a file cabinet to which the employer had joint access. If computers with e-mail capabilities are involved, the interception of electronic communications in transit requires a wiretap order, and if the electronic communications are in electronic storage, 18 U.S.C.A. § 2701 et seq. and N.J.S.A. 2A:156A-27 et seq., should be consulted to determine whether an order permitting seizure for stored electronic communications is needed. (See section III, infra).

II. SEARCH EXECUTION

From a legal standpoint, the execution of a search warrant is successful if the evidence described in the warrant is seized and the seizure is accomplished in such a manner that the evidence may be used to prove a criminal case. Attorneys and investigators must be thoroughly familiar with what steps are and are not authorized by the warrant and what actions are appropriate if unexpected computer evidence is discovered. Because computer evidence is intrinsically susceptible to alteration and destruction, special care must be taken in seizing computer evidence and in documenting the seizure so that the evidence seized can be used to prove a criminal case.

A. SEIZING COMPUTER EVIDENCE

Because most computer evidence will be seized pursuant to a search warrant, the search and seizure will be guided by the terms of the warrant. Officers may search the places in which the evidence to be seized may be located and may use all investigative methods appropriate in light of the scope of the warrant. State v. Reldan, 100 N.J. 187 (1985). The search may be as extensive as is reasonably necessary to locate the items described in the warrant. See United States v. Sawyer, 799 F. 2d 1494 (11th Cir. 1986), cert. denied, 479 U.S. 1069 (1987).

As emphasized in other parts of this manual, when unexpected evidence is encountered during the execution of a warrant, the best course in most circumstances -- although not necessarily the only legally permissible course -- will be to seek a

supplemental search warrant before executing a search or seizure that is outside of the warrant's authorization even if it appears that an exception to the warrant requirement applies.

The general rule is that seizure of some materials outside of the warrant will not completely invalidate the search. State v. Tunnel Citgo Services Inc., 149 N.J. Super. 427, 434 (App. Div. 1977); Waller v. Georgia, 467 U.S. 39, 43 (1984). However, more drastic steps have been taken by some federal courts where seizures were made in "flagrant disregard" of the warrant's limitations. United States v. Matias, 836 F.2d 744, 747 (2d Cir. 1988); United States v. Henson, 848 F.2d 1374 (6th Cir. 1988), cert. denied, 488 U.S. 1005 (1989); United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982). Where wholesale seizures of evidence have been made in violation of the terms of the warrant, suppression of all evidence (even that sanctioned by the warrant) has been ordered on the theory that the executing officers so severely violated the terms of the warrant that they actually conducted a "general search." Prior to the execution of a search warrant, every effort should be made to thoroughly and accurately instruct the designated searching investigators about the nature and scope of evidence sought in the warrant. The specific evidence sought in the search warrant should be discussed and examples of items beyond the scope of the warrant should be cited. Investigators should be encouraged to search as much as possible while at the premises, and remove to an off-site location only that which cannot reasonably be reviewed on-site in a manner in accordance with the

search warrant. Such instructions should be given immediately prior to the execution of the search warrant and a record should be made of the topics reviewed and persons present.

In determining what action should be taken in regard to computer evidence discovered at the scene but not within the scope of the warrant, it may be appropriate to consider how much data may be stored on the computer, which conceivably could store all of a business's records. If a huge amount of data outside of the scope of the warrant is seized and a court finds that the warrantless seizure was invalid, it potentially could conclude that seizure of the computer and its contents constituted a "general search" and suppress all of the evidence seized.

Although seizure without judicial authorization is strongly discouraged, one proviso is in order. The State has the right and the obligation to secure evidence to the extent necessary to preserve it. Hence, there is no question that where there is probable cause to seize a computer or computer data, such easily destructible evidence may be secured to the extent necessary to preserve it while a supplemental application is made. (See related discussion of the exigent circumstances exception, supra at Section IB2). See also Mincey v. Arizona, 437 U.S. 385, 393 (1978); State v. Stupi, 231 N.J. Super. 284, 289 (App. Div. 1989). Specific situations that may be encountered in regard to computer evidence are discussed below.

B. SEIZING COMPUTER STORAGE DEVICES WHERE THE WARRANT ONLY AUTHORIZES THE SEIZURE OF RECORDS

There is support for the position that computer disks may be seized even if disks or electronically stored records are not specifically described in the warrant, if the warrant permitted the seizure of records. In United States v. Musson, 650 F. Supp. 525, 532 (D. Colo. 1986), the Court relied on case law allowing cassette tapes and micro-cassette recordings to be seized as records to permit seizure of computer disks under a warrant that permitted seizure of documents and records but did not specifically permit seizure of electronically stored data. (See Section IA2c for other authorities supporting this proposition). When possible, the application and search warrant should specifically encompass the seizure of computer disks and electronically stored records. See sample language in Appendix.

C. THE WARRANT SPECIFICALLY PERMITS THE SEIZURE OF COMPUTER RECORDS BUT AN ON-SITE REVIEW IS IMPRACTICAL

If investigators intend to seize computer evidence for later searching off-site, the facts justifying that action should be included in the affidavit and the warrant should authorize it. See Section IA6. Nonetheless, if the warrant authorizes a search of computer evidence but does not authorize the removal of the computers themselves to conduct an off-site search, a supplemental warrant authorizing an off-site search should

be considered, if at the time of execution, investigators determine that an on-site search is not practical.

Courts have upheld searches where for practical reasons property was removed to be searched at another location, even where the warrant did not expressly permit this course of action. Although this technically is a seizure of items outside the warrant, this type of "over seizure" has been permitted when it would be impractical to sort the described items from the other intermingled items at the scene. See 2 W. LaFave, § 4.11(a) at 685-87. In discussing this issue, some courts have suggested that a supplemental application was preferable. For example, in United States v. Shilling, 826 F.2d 1365, 1369 (4th Cir. 1987), cert. denied, 484 U.S. 1043 (1988), agents removed entire file cabinets of documents after realizing that it would be extremely impractical to search through them on the premises. The court denied the motion to suppress but cautioned that a supplemental warrant application would have been the better course. This issue has been specifically addressed in United States v. Upham, 168 F. 3d. 532 (1st Cir. 1999), cert. denied, __ U.S. ___, 119 S.Ct. 2353, 144 L.Ed. 249 (1999). The Court in Upham recognized that, "it is not easy task to search a well-laden hard drive by going through all of the information it contains, let alone to search through it and the disks for information that may have been `deleted.' The record shows that the mechanics of the

search for images later performed off site could not readily have been done on the spot."[10] Id. at 535. See also United States v. Lacy, 119 F.2d 742 (9th Cir. 1997). But see, United States v. Tamura, 694 F. 2d 591(9th Cir. 1982).

If the need for conducting an off-site search of computer evidence becomes apparent in the course of executing a warrant, investigators should make a record of the circumstances which require the off-site search. (This is recommended even where the warrant expressly authorizes the off-site search). The relevant circumstances may include specifics regarding the computer evidence encountered, some estimate of the amount of data that must be reviewed or the memory capacity of the computer devices, as well as general explanations regarding the technical expertise and analysis required to effectively search computer data. See United States v. Lamb, 945 F. Supp. 441, 462-63 (N.D.N.Y. 1996); United States v. Kimbrough, 69 F.3d 723, 727 (5th Cir. 1995), cert. denied, 517 U.S. 1157 (1996).

[10] The storage capacity of hard drives has increased exponentially since the date of the search warrant in Upham. Therefore, the justification and need for an off-site search is even more compelling today.

D. DOCUMENTING THE SEARCH AND SEIZURE OF COMPUTER EVIDENCE

Because the procedures for seizing and securing delicate computer evidence are more involved than those used to seize paper records, a more detailed documentation of the seizure is required. Reports should be kept with the expectation that there will be defense challenges to the use and admissibility of the evidence.

Documentation is necessary because, in order for real evidence (such as data, hardware and software) to be admitted as evidence, a court must find it reasonably probable that the evidence has not been changed in any important respects. Chain of custody or authentication requirements are more stringently applied when the evidence is easily altered. See, e.g., State v. Hoffman, 290 N.J. Super. 588, 595 (App. Div. 1996), mod. on other grounds, 149 N.J. 564 (1997); State v. Binns, 222 N.J. Super. 583, 593-94 (App. Div. 1988), certif. denied, 111 N.J. 624 (1988). See section VC. Precise documentation is also essential because the State may be offering the data as evidence at trial and may have to convince a jury of lay persons to accept the data as reliable evidence.

A report made near to the time of the seizure that details all steps taken in regard to the computer evidence may be critical to the acceptance of this evidence at a future proceeding. It is suggested that the report identify the officers who seized the

evidence, record all actions taken to seize the evidence, identify the evidence seized and explain how the seized evidence was transported and secured.[11]

III. SPECIAL WARRANTS: THE IMPLICATIONS OF THE WIRETAP ACT, AND THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

Since computer searches and seizures can implicate the Wiretapping and Electronic Surveillance Control Act[12], the Electronic Communications Privacy Act[13], and the Privacy

---

[11] R. 3:5-5 requires that a receipt for all property taken pursuant to a search warrant either be given to the person whose property was taken, or be left at the scene ("the receipt" requirement). Similarly, in returning the warrant to the Court, the executing officer must make an inventory of all property taken pursuant to the Court's authority ("the inventory" requirement). To satisfy the receipt and the inventory requirements of R. 3:5-5, the officers must account for "property taken." In some instances, the executing officers may opt to make a "back-up" or a copy of a computer's contents but leave the computer with contents intact with its owner. Although the property copied is not literally taken, both the property copied as well as that physically removed should be listed in the receipt and inventory. In a somewhat analogous situation, federal courts have found that notice must be given under a federal rule nearly equivalent to our R. 3:5-5 when a covert entry warrant is executed and only intangible evidence is seized. United States v. Pangburn, 983 F.2d 449, 454-56 (2d Cir. 1993).

[12] Electronic surveillance orders for contemporaneous interception of wire or electronic communication. N.J.S.A. 2A:156A-1 et seq. and 18 U.S.C.A. § 2510 et seq.

[13] Orders for access to stored electronic communications. N.J.S.A. 2A:156A-27 et seq. and 18 U.S.C.A. § 2701 et seq.

Protection Act[14], prosecutors and investigators should be familiar with these Acts.

A. ELECTRONIC SURVEILLANCE ORDERS

If, during the course of an investigation, it is determined that a computer is actively being used to further a criminal scheme it may be necessary to seek a court order for the interception of the wire[15] or electronic communications as they are being transmitted, otherwise known as a "wiretap." This is governed by the requirements set forth for the interception of wire or electronic communications pursuant to N.J.S.A. 2A:156A-1 et seq., detailed below.

1. Requirements

a. Probable cause to believe that:

(1) the wire or electronic communications will be communicated on the wire or electronic communications facility involved;

---

[14]The Privacy Protection Act and the State Newsperson's Shield Law generally prohibit the use of a warrant to seize certain documentary material. 42 U.S.C.A. § 2000aa et seq. and N.J.S.A. 2A:84A-21.9 et seq.

[15]It should be noted that in the context of the contemporaneous interception of computer transmissions, pursuant to N.J.S.A. 2A:156A-1 et seq., it is possible that the type of communication to be intercepted could be either electronic or wire, or both. Emerging technology allows the use of the Internet for the transmission of the human voice between computers. Those transmissions would be wire communications under the statutory definition.

(2) the person whose communication is to be intercepted is engaging or was engaged over a period of time as part of a continuing criminal activity, or is committing, has or had committed, or is about to commit an offense enumerated in N.J.S.A. 2A:156A-8; and

(3) particular communications concerning such offense may be obtained through such interception.

b. Authorization by the Attorney General or County Prosecutor.

c. Application to specially designated Judges.[16]

2. Type of Communication to be Intercepted

a. Electronic Communications: Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system that affects interstate, intrastate or foreign commerce, excluding wire communications, tone-only pagers or tracking devices. N.J.S.A. 2A:156A-2m.

b. Wire Communications: Any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable or

[16]It is important to make sure that any application for the interception of wire or electronic communications be taken to the appropriate wiretap judge. See Electronic Surveillance and Communications Data Warrant Manual § 4 (Administrative Office of the Courts 1994).

other like connection between the point of origin and the point of reception. "Wire communication" includes any electronic storage of such communication, and the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit. N.J.S.A. 2A:156A-2a.

3. Circumstances Under Which a Wiretap Order Should Be Sought in Connection With a Computer

In the situation in which the crime is currently being committed by the target of the investigation and the investigation reveals that he is utilizing the computer for the transmission of information in the commission of the offense, it may be necessary to consider the use of a wiretap to obtain the evidence. The nature of digital evidence is such that it is transitory and, if not intercepted during its transmission, could be lost forever. Moreover, there are situations in which such a search is the only way that the evidence would be discovered.

B. STORED ELECTRONIC COMMUNICATIONS

New Jersey has addressed the manner in which stored wire and electronic communications may be obtained by law enforcement in N.J.S.A. 2A:156A-27 through 33. The scheme adopted by New Jersey closely parallels the Stored Wire and Electronic Communications and Transactional Records Access Act 18 U.S.C.A. § 2701 et seq.

These sections deal with obtaining various kinds of information from providers of wire or electronic communications services by law enforcement. These sections specifically address two different types of service providers, “electronic communication

services" (ECS) and "remote commuting services" (RCS). In New Jersey, the distinctions are largely academic because the Wiretap Statute deals with both ECS and RCS the same, whereas, under Federal law there are significant differences in the procedures used to obtain information from an ECS and an RCS. See 18 U.S.C.A. § 2703.

An ECS is defined as, "any service which provides to the users thereof the ability to send or receive wire or electronic communications." N.J.S.A. 2A:156A-2 p. An ECS is generally best understood as an Internet Service Provider or telephone company. An RCS is defined as, "the provision to the public of computer storage or processing services by means of an electronic communication system." N.J.S.A. 2A:156A-2 s. Typically, an RCS is a service such as a payroll processing company.

Initially, it should be noted that in New Jersey, "[a] law enforcement agency, but no other governmental entity may require . . . disclosure by a provider." This means that an administrative agency may not require disclosure of information from a provider. Moreover, it is also important to keep in mind that the information which is the subject of N.J.S.A. 2A:156A-27 through 33, is information being held by a third party and not the recipient or the sender. The information is in "electronic storage" which is defined as, "any temporary, intermediate storage of a wire or electronic communication incidental to

the electronic transmission thereof." N.J.S.A. 2A:156A-2 q.[17] As a result, since N.J.S.A. 2A:156A-27 through 33 protects communications while they are in electronic storage, data which is encountered on either the recipient's or the sender's computer it is not "temporary" or "incidental to . . . transmission," and is not covered by this statute. Communications which are not covered by this statute may be obtained by a conventional search warrant or subpoena.[18] For example, in a recent decision, the Appellate Division appropriately dealt with the search of numbers stored on a numeric pager as a conventional search without reference to the Wiretap Statute. State v. Deluca, 325 N.J.Super. 376 (App. Div. 1999). In that case, the court determined that law enforcement could search the numbers stored on a numeric pager, incident to an arrest and due to exigent circumstances.

N.J.S.A. 2A:156A-28 prohibits the disclosure of the contents of a communication while in electronic storage by a person or entity providing an electronic communication service or remote commuting service to the *public*.[19] However, this section provides

---

[17]Due to subtle differences in the manner in which stored wire and electronic communications are dealt with in the statute, access to stored wire communications requires a wiretap order; a warrant is not sufficient. See United States v. Smith, 155 F.3d 1051 (9th Cir. 1998).

[18]This is true unless the target of the search is an ECS or and RCS in which case files being held for subscribers of the service will be covered by these statutory provisions.

[19]In Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill, 1998), the Court found that UOP did not violated the Federal corollary to N.J.S.A. 2A:156A-28, when UOP revealed the contents of e-mail on Andersen's internal e-mail system because the service was not provided to the public. This case indicates that law enforcement may

several important exceptions under which the contents of communications may be "divulged," including; to law enforcement as provided in N.J.S.A. 2A:156A-4, 17,18 and 29; with the consent of the originator or addressee; for the protection of the rights or property of the provider; and where the contents were inadvertently obtained by the provider and appear to pertain to the commission of a crime. If the information is "intercepted" during the course of the transmission, and not accessed in storage, it constitutes a wiretap controlled by N.J.S.A. 2A:156A-1 et seq.

N.J.S.A. 2A:156A-29 controls when and under what conditions, an ECS or RCS must provide information to a law enforcement agency. N.J.S.A. 2A:156A-29 establishes three categories of information, basic subscriber information (N.J.S.A. 2A:156A-29 f.), "record other information pertaining to a customer or subscriber," (N.J.S.A. 2A:156A-29 e.), and the content of communications (N.J.S.A. 2A:156A-29 a.).

Content is defined as "any information concerning the substance, purport or meaning of that communication." N.J.S.A. 2A:156A-2 g.[20] Pursuant to N.J.S.A. 2A:156A-29 a., and under New Jersey Law, it is always necessary to obtain a warrant to

---

obtain information, including content, from a private e-mail service without subpoena or warrant. However, the law is far from settled on this matter.

[20]This definition applies to §§ 28, 29, and 30, but content has a different meaning when used elsewhere in the Wiretap Act.

require either an ECS or an RCS to provide a law enforcement agency with the contents of wire or electronic communications in their possession.[21]

On the other end of the information spectrum, a law enforcement agency may obtain basic subscriber information through either a grand jury or trial subpoena. N.J.S.A. 2A:156A-29 f. The information which can be obtained by a subpoena is limited to, "name, address, telephone number, or other subscriber number or identity, and length of service provided to the customer of such service and the type of services the subscriber or customer utilizes."[22]

There is a vast middle ground of information between the content of a communication and basic subscriber information, which the statute refers to as a "record or other information pertaining to a subscriber or customer." N.J.S.A. 2A:156A-29 e. This type of information includes such items as credit card information and activity logs kept by ECS or RCS. The requirements necessary for a law enforcement agency to obtain this type of information are established in N.J.S.A. 2A:156A-29 e. Subsection e creates a

---

[21]There is a special warrant required to obtain the contents of electronic communications called a Communications Data Warrant (CDW). This warrant may only be issued by a specially designated CDW judge. Refer to the Supreme Court Order designating Wiretap and CDW judges.

[22]The corollary federal provision 18 U.S.C.A. § 2703(c)(1)(C), allows federal agents to obtain "telephone toll billing records" by use of a subpoena. The New Jersey Supreme Court, in State v. Hunt, 95 NJ 338 (1982), required a warrant to obtain telephone toll billing records and that precedent controls in New Jersey. It should be further noted that Federal law permits the use of "administrative" subpoenas. The New Jersey statute requires a "grand jury or trial subpoena."

new type of court order based on "specific and articulable facts showing that there are reasonable grounds to believe that the . . . [record sought] . . . is relevant and material to an ongoing criminal investigation." This order has been designated by the Administrative Office of the Court as a Communication Information Order (CIO) and must be obtained from a Communications Data Warrant Judge. The standard adopted in the statute is derived from the corresponding Federal provisions, 18 U.S.C.A. § 2703 (d), and closely approximates the standard for non-invasive searches first enunciated in Terry v. Ohio, 392 U.S. 1, 64 (1968), i.e., "specific and articulable facts." Moreover, it closely resembles the standard necessary to obtain blood and other evidence in an Investigative Detention Order R. 3:5A-4, "a reasonable and well founded basis from which to believe. . . ."

The following chart provides a simple breakdown of which specific procedure to use depending upon the information sought:

MEANS FOR OBTAINING INFORMATION FROM ELECTRONIC COMMUNICATION SERVICE PROVIDERS AND REMOTE COMPUTING SERVICES N.J.S.A. 2A:156A-29

SUBSCRIBER INFORMATION Name, address, telephone number (or other identifier), length of service & type of service.	Subpoena (N.J.S.A. 2A156A-29(f)) Communication Information Order (CIO) Communications Data Warrant (CDW)
OTHER RECORD OR INFORMATION Including TCP/IP information, transaction logs, credit information, billing method etc.	CIO (specific and articulable facts showing reasonable grounds that record is relevant and material to investigation) CDW (probable cause)
Content (as defined in N.J.S.A. 2A:156A-1g.) & Toll Billing information. Toll Billing records may only be obtained by a CDW	CDW

Pursuant to N.J.S.A. 2A:156A-29 g., a law enforcement agency may request that a provider, "take all necessary steps to preserve, for a period of 90 days, records and other evidence in its possession pending the issuance of a warrant." This provides a valuable resource for law enforcement. In circumstances where there is not sufficient evidence to obtain a warrant this section allows a law enforcement to require a provider to "freeze" the evidence for up to 90 days until law enforcement may obtain a warrant. Many, if not

most, Internet Service Providers routinely recycle the computer memory where the information is stored and if law enforcement does not, or can not, move quickly enough the information is lost forever. There are two potential draw backs to utilizing this section. Once the section has been used it freezes the information as of the date of the request. If it is employed too early in an investigation subsequent information may be lost. Moreover, the section implies that any subsequent request for information must be obtained by a "warrant," thereby eliminating the ability to take advantage of N.J.S.A. 2A:156A-29 e.

The remedies provided for in the Act are civil damages exclusively. However, in recent cases, courts have shown no hesitation in providing for suppression remedy for violation of the Stored Electronic Communications sections of the Wiretap Act. See, McVeigh v. Cohen, 983 F. Supp. 215 (D.C. Dist. 1998).

IV. PRIVACY PROTECTION ACT

There is a relatively obscure federal statute, the Privacy Protection Act, 42 U.S.C.A. 2000aa, which could come into play in the execution of search warrants on computers by state law enforcement officers[23]. Originally enacted in response to the United States Supreme Court opinion in Zurcher v. Stanford Daily, 436 U.S. 547 (1978), the PPA establishes a "subpoena first rule" when seeking information in the hands of the news media. Therefore, unless the circumstances under which the information is held

[23] There is a similar New Jersey statute, N.J.S.A. 2A:84-21.9 et seq., which is much more narrowly drawn than the corresponding federal statute.

comes within one of the statutory exceptions, law enforcement must request information from the media by subpoena and not through a search warrant.

The PPA addresses two categories of information, "work product," the actual items such as an article or book to be published; and "documentary materials," the notes and other material accumulated to produce the work product.

The difficulty arises with the broad scope of what is covered by the statute, which protects "a person reasonably believed to have a purpose to disseminate to the public a newspaper, books broadcast, or other similar form of public communications." In the wake of the explosive growth of the Internet and the unprecedented access to technology, such as web sites and news groups which allow the dissemination of information to the public, it is possible that such activity might be construed by the courts as, "a similar form of public communication." Law enforcement must be cautious when planning and executing warrants on persons who they reasonably believe might have the purpose to disseminate information to the public, such as a corporation which has a newsletter, an individual who is known to be preparing a book of news article or a person who is publishing information to a web site. Keep in mind, however, that this statute is designed to shield the media and does not protect evidence in the possession of the target of a criminal investigation. If the evidence supporting the search warrant indicates that the criminal activity is being committed by the person utilizing the targeted computer, then it

comes with in the target exception in the PPA and a search warrant may be used rather than a subpoena.

The reason that the PPA is of particular interest to state and local law enforcement, is because the act makes state and local law enforcement officers **personally** liable for damages resulting from a violation of the Act. 42 U.S.C.A. § 2000aa-6(a)(2) establishes a civil cause of actions "against an officer or employee of a state who has violated this chapter while acting within the scope or under color of his office or employment, if such state has not waived its sovereign immunity. . ." Thus, an individual prosecutor or police officer is personally liable for damages in a civil suit brought pursuant to the PPA, if the state has not waived its sovereign immunity, which New Jersey has not done.

A. PPA Cases

There have only been a few cases which have dealt with the PPA.[24] Of those cases which have interpreted the PPA the results are inconsistent. The most cited case dealing with the PPA is Steven Jackson Games v. United States, 816 F.Supp. 432 (W.D. Tex. 1993), aff'd on other grounds, 36 F.3d 457 (5th Cir. 1994). In that case the United States Secret Service received information indicating that a person employed as a systems operator at Steven Jackson Games, Inc., ("SJG") was utilizing the electronic bulletin board at SJG to post illegal information. SJG used the bulletin board to disseminate information to the public and in fact had a draft of a book which was to be published.

[24]To date, there are no cases interpreting the New Jersey Newsperson's Shield Law, N.J.S.A. 2A:84A-21.9 et seq.

There was no evidence that SJG was involved in the illegal behavior. The Secret Service obtained a warrant to search the computers at SJG and ultimately seized two of the thirteen computers as well as other materials. SJG immediately requested return of the seized materials, but the Secret Service refused. SJG sued and the court held that the Secret Service did not violate the PPA in its initial seizure, because there was no reason to believe the SJG had the purpose to disseminate to the public, but it did violate the PPA by its failure or refusal to return the protected material when requested. SJG was awarded $300,000 in damages for its violation of the PPA. It is important to note that had the search been conducted by state law enforcement officers, individual officers would have been liable for the damages.

In a more recent case, Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997), the Court ruled that the PPA did not establish a cause of action against municipal police officers, who were municipal and not state employees, and as a result the defendant municipal police officers were not personally liable for violations of the PPA.[25]

[25]This is a hyper-technical reading of the PPA and should not be relied on too heavily by municipal police officers. The better practice is to assume that the law enforcement officers conducting the search will be personally liable for violations of this statute unless and until the State waives its sovereign immunity with respect to the PPA.

B. Conclusion

In sum, the PPA and to a lesser extent the Newsperson's Shield Law create a host of issues concerning the search and seizure of computer systems which may be used to disseminate information to the public. Police and prosecutors are urged to consider the possible applicability of these statutes when planning to apply for a search warrant for computers where there is reason to believe that, a person has a purpose "to disseminate to the public in a newspaper, books, broadcast, or other similar form of public communication."

V. REVIEW AND ANALYSIS OF COMPUTER EVIDENCE

Prosecutors and investigators should expect defendants to claim that the state has -- intentionally or accidentally -- altered some of the electronic evidence used at trial. To meet such arguments, and to ease admissibility of the evidence at trial, See section V, infra, it is recommended that the state retain the original of any data storage medium (disks, drives, tapes, etc.) which contain evidence properly subject to seizure. It is strongly recommended that prosecutors and investigators work only with a copy of the seized data. The procedures outlined below are intended to strengthen the state's proofs that the seized data were not altered by the state. If, in a particular case, the state has decided to return the original data storage medium (DSM) to the owner after copying the

data from it, it is even more important that procedures be followed to establish that data were not altered by the state at any point.[26]

Therefore, it is essential that the state preserve the electronic evidence in exactly the condition it was in at the time of the seizure. Investigators who examine electronic evidence must document exactly what steps they took to examine the electronic data, so that years later, they will be able to testify credibly that they did not alter it.

In order to rebut any claim of deliberate or inadvertent alteration of data, it is advisable to make several copies of the data. The original should be immediately stored as evidence. The original or the "evidence" copy should remain untouched, so it will be available to rebut any charges of data alteration raised at trial.

However, keeping a copy of all data, some of which may be outside the scope of the warrant, raises the question whether the seizure was unreasonably over broad, and therefore illegal. The procedure outlined below should represent a reasonable approach to searching electronic evidence; and a reasonable search is what the Fourth Amendment requires.

A. In conducting a search for records, investigators are permitted to briefly examine every record which may be within the scope of the warrant, in order to determine whether it is in fact within the warrant. Andreson v. Maryland, 427 U.S. 463 (1976); United States v. Santarelli, 778 F.2d 609, 616 (11th Cir. 1985). Thus, making a backup

[26] If it is necessary to return the original storage medium, prosecutors should require defense counsel to stipulate to the authenticity of the copies.

copy of the entire data storage medium, and then examining all of the data for the purpose of determining whether it falls within the scope of the warrant, is permissible. In an excess of caution, any data which has been reviewed at an off-site location and deemed to fall outside the scope of the warrant should be segregated from the remaining evidence and not examined any further. The data should be downloaded and returned to the owner at the earliest opportunity.

B. Some courts have expressed concern that this brief examination must not result in wholesale seizures of items outside the warrant (or not covered by the plain view exception.)

1. United States v. Beusch, 596 F.2d 871 (9th Cir. 1979). The warrant authorized the seizure of records related to all transactions the target had with a named individual. Agents seized a ledger book and a file folder containing telegrams. Some pages in the ledger, and some telegrams in the folder, concerned the named individual, but most did not. Defendant argued that because the records relating to the individual were easily identifiable, and because the pages were easily separable, the agents' seizure of the entire ledger and file folder was impermissible. The court disagreed. "As long as an item appears, at the time of the search, to contain evidence reasonably related to the purposes of the search, there is no reason. . . to suppress it. . . . In so holding, we are careful to point out that we are discussing single files and single ledgers, i.e., single items which although theoretically separable, in fact constitute one volume or one file folder. The

reasons we have given for allowing their seizure may not apply to sets of ledgers or files, but. . . we find it unnecessary to discuss it further." Id. at 877 (citation omitted).

2. United States v. Santarelli, 778 F.2d at 616. Because agents were entitled to examine every document on-site, they could remove all documents and conduct the brief examination off-site, "so long as any items found not to be relevant were promptly returned." See also United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997) (the seizure of computer files without first determining which documents in the files were within scope of warrant did not require blanket suppression, as long as a review procedure promptly after seizure safeguards against the government's retention and use of computer generated documents known to lie beyond a reasonable interpretation of the warrant's scope).

C. If the state retains a backup copy of all data, including that which is outside the scope of the warrant, defendant may argue that the storage medium is akin to a filing cabinet, and not akin to a single file. Defendant would argue that the retention of everything in the storage medium constituted a general search.

1. As the amount of data on the data storage medium increases, this argument becomes more persuasive. Seizure and retention of a 1.44 MB floppy may be like seizure of a ledger book, while seizure of a one gigabyte drive may be more like seizure of an entire filing cabinet.

2. The state would argue under Beusch that the data storage medium constitutes "an item" containing evidence, which was therefore seizable.

3. Accord United States v. Lamb, 945 F. Supp. 441, 458 (N.D.N.Y. 1996). The search warrant authorized seizure from America Online of "[a]ll stored files" in various subscribers' accounts. "There was probable cause to believe that some of those files were image files" containing child pornography. "Although the language does not limit investigators to seizing image files only or image files of child pornography only, the actual content of a computer file usually cannot be determined until it is opened with the appropriate application software on a computer. . . . Because there was probable cause to believe that stored files in the accounts of the suspects contained evidence of the crime. . . the warrant properly authorized the search and seizure of these particular items." Id.

D. A reasonable balance is to retain a copy of all data on any storage medium which contains some relevant evidence, but only work with data within the scope of the warrant (or within the plain view exception). On the other hand, if a particular storage medium, such as an individual drive or disk, does not contain evidence, then that entire medium should be returned, and the state should not retain any copy of the data on it. The following procedure can be used:

1. Make two backup copies of all DSM (three, if the originals are to be returned). Copies should be bit-by-bit[27] or file-by-file as the needs of the case dictate.

2. The original should be placed in the evidence vault. The original should remain untouched unless used at trial.

3. One copy is the discovery copy, which will be provided to the defense in accordance with the discovery rules. This should be sealed in an envelope (dated and signed) and a record should be made documenting that its data was not examined.

4. The second copy is the work copy. The investigator should briefly examine all data on the DSM which might be within scope of warrant, or within the plain view exception.

5. If this examination establishes probable cause to believe that other seizable evidence exists, which is neither within the scope of the warrant nor seizable under an exception to the warrant requirement, a supplemental search warrant should be obtained. This is true whether the other evidence exists within the DSM or at any other place.

6. Once the investigator has identified all data which is properly subject to search and seizure (either within the scope of the warrant, within a recognized

---

[27]A bit-by-bit copy will include "deleted" data which has not been overwritten, and "hidden" files -- those which do not appear on a directory listing of files. A file-by-file copy will only include the files listed in the directory.

exception to the warrant clause, or within the scope of a supplemental warrant), that properly seized evidence should be retained on the work copy. All other data, not properly subject to seizure, should be deleted from the work copy, and all hard copies of it should be destroyed.

7. The investigator should make a record of what steps he took to delete such evidence. This record must document that the retained data was not altered.

8. The investigation should then proceed using the work copy and hard copies of it, which contain only evidence properly subject to seizure.

E. Privileged information: The procedure outlined above should also be used to guard against the examination of privileged material which is outside the scope of the warrant. While examining the data, the investigator should keep in mind that attorney-client documents and doctor-patient records, among others, may be privileged. Nonetheless, these documents may well be stored on a computer, along with seizable evidence.

1. As noted above, the investigator may briefly examine the seized data to determine whether it falls within the scope of the warrant. If the investigator locates arguably privileged data on the work copy, and that data is not within the scope of the warrant, the investigator should delete it from the work copy without examining it more than is necessary to determine it falls outside the warrant.

2. The investigator should document that the data was identified and deleted.

3. In some cases, material which ordinarily would be privileged may be seizable (for example, in a Medicaid fraud investigation, doctor-patient records may be evidence of a crime). In such situations, the prosecutor should provide specific guidance on what records can be retained, and what records cannot be retained. Compare Klitzman, Klitzman & Gallagher v. Krut, 744 F.2d 955 (3d Cir. 1984), with National City Trading Corp. v. United States, 635 F.2d 1020, 1026 (2d Cir. 1980). The investigator should document that records outside the scope of the warrant were not examined any more than absolutely necessary to locate and seize those records which were described in the warrant.

VI. ADMISSIBILITY OF COMPUTER EVIDENCE

Computer evidence must pass a variety of traditional admissibility tests: authenticity, the "best evidence" rule and the rule against hearsay evidence. Traditionally, computer records have been admitted as information generated by businesses, pursuant to the business records exception to the hearsay rule. N.J.R.E. 803(c)(6). See Hahnemann University Hospital v. Dudnick, 292 N.J. Super. 11 (App. Div. 1996). However, "computer evidence" can cover the universe of documentary materials and is not limited to business records. Computer evidence will always need to be authenticated in some way.

A. BEST EVIDENCE RULE

In the computer environment, the original records are actually the electronic impulses stored on a magnetic medium. However, it is not possible to hold up a disk and see what is on it. N.J.R.E. 1002 provides that:

> To prove the content of a writing or photograph, the original writing or photograph is required except as otherwise provided in these rules or by statute.

First, computer data is a "writing." A "writing" is defined in N.J.R.E. 801(e) to include “data compilations. . .recorded by. . .magnetic impulse. . .or by any other means[.]” The 1991 Supreme Court Committee Comment to N.J.R.E. 801(e) states that this rule includes images and data stored in computers, and electronic or other impulses in all forms of preservation that may be perceived by sight, sound or other senses directly or after retrieval.

Second, any accurate printout of the data is an "original" within the meaning of the best evidence rule. N.J.R.E. 1001(c) states: "If data are stored by means of a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'." In United States v. Maxwell, 42 M.J. 568, 581 (U.S.A.F. Ct. App. 1995), rev’d in part on other grounds, 45 M.J. 406 (C.A.A.F. 1996), the court rejected the defense argument that the computer should have been brought into the courtroom and images displayed on the computer screen. Hard copies downloaded from the computer were admitted as originals.

In addition, duplicate electronic documents may be admitted unless authenticity or "unfairness" is an issue. N.J.R.E. 1003 provides that "a duplicate as defined by Rule 1001(d) is admissible to the same extent as an original unless (a) a genuine question is raised as to the authenticity of the original, or (b) in the circumstances it would be unfair to admit the duplicate in lieu of the original." A "'duplicate' is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photograph, including enlargements and reduction, or by mechanical or electronic re-recording, or by chemical reproduction or by other equivalent technique which accurately reproduces the original." N.J.R.E. 1001(d). It is prudent to assume that defense counsel may argue, at least in some cases, that the act of copying the data before it is examined could alter the data. Defense counsel could then insist that the copy is not a "duplicate" because it does not "accurately reproduc[e] the original." N.J.R.E. 1001. The copy then would be inadmissible. Counsel are especially likely to raise this argument if the state has returned the original data storage medium to the defendant. Thus, there is good reason for the state to retain the original data storage medium as described in section V, supra.

Admissibility will not depend entirely on whether the data offered is on hard drive, duplicate floppy disk or a printout of either one. Instead, the court must be satisfied that the data is authentic and that any copies offered are accurate. This raises the issue of authentication of computer records.

B. AUTHENTICATION

N.J.R.E. 901, Requirement of Authentication or Identification, provides:

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

Simply stated, the proponent must demonstrate that the evidence is what it purports to be. Most issues regarding authentication of computer records are likely to arise in the context of disputes over the genuineness of documents retrieved from computers.

According to Fed. R. Evid. 901(b)(9), the proponent of computer generated evidence should produce evidence "describing the process or system used to produce the evidence" and "showing that the process produces an accurate result."

There are three major stages where error can be introduced:

1. Inputting data into the computer;

2. Processing the data by the computer; and

3. Evaluating the data generated by the computer.

The proponent of computer evidence must demonstrate accuracy at all three stages. Seizing, preserving and analyzing evidence stored on a computer implicates stages number 2 and 3.

It is important to follow procedures for the seizure, labeling, transporting and storage of suspect computers. Following proper procedures will assist in establishing the chain of custody and the integrity of the evidence offered in court.

Experts should be used to examine all seized computer evidence and to recover whatever evidence they can. Forensic computer examiners may be able to (1) make the equipment operate properly; (2) retrieve information; (3) retrieve "deleted" or "erased" data; (4) defeat or bypass passwords; (5) decipher encrypted data; and (6) detect viruses.

The most important rule in analyzing computer evidence is DO NOT USE THE SUSPECT'S COMPUTER TO LOOK AT DATA, OR FOR ANY OTHER PURPOSE. USE ANOTHER COMPUTER TO ANALYZE A COPY OF THE DATA INSTEAD. Another important rule to follow in retrieval and/or analysis of computer data is to make sure a clean designated computer is used. Otherwise, one may encounter the argument that data on the computer used for analysis has contaminated the data seized from the suspect.

Prosecutors should think about the witnesses they will offer in court to testify as to what was done with the computer, how it was seized, how data was copied, how it was analyzed (i.e., restoration of deleted files, discovery of hidden files, deciphering of codes).

Prosecutors will want to produce a witness who is trained and experienced in the seizure and analysis of computer evidence.

C. CHAIN OF CUSTODY

Computer evidence requires the same chain of custody procedures as other types of evidence. The state must show the evidence offered is the same thing the investigators seized. Since electronic data is changeable, a hand-to-hand chain of accountability is required. Access should be strictly controlled and accurate records must be kept to show who has examined the evidence; when they did so; and as precisely as practicable, exactly what steps they took to examine it.

VII. CONCLUSION

While the well settled principals of search and seizure law apply to the computer or "cyber world" as much as they do to the physical world, the explosive growth in the use of computers and the Internet has necessitated an examination of the special considerations brought about by the computer revolution. This Manual seeks to examine the unique issues raised by digital evidence and their application to the law of search and seizure. The practitioner should be mindful that this particular area of law is evolving rapidly and the information provided in this Manual is the best information at the time of its publication. The Division will continue to monitor any developments in the law and will update this manual in light of any new developments.

TABLE OF AUTHORITIES

CASES

Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill, 1998) 59

Andreson v. Maryland, 427 U.S. 463 (1976) 9,69

Application of United States for an Order Authorizing the Installation of a Pen Register, Touch Tone Decoder and a Terminating Trap, 458 F. Supp. 1174 (W.D. Pa. 1978) 5

Coolidge v. New Hampshire, 403 U.S. 443 (1971) 36

Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997) 67

Hahnemann University Hospital v. Dudnick, 292 N.J. Super. 11 (App. Div. 1996) . . 75

Horton v. California, 496 U.S. 128 (1990) 36

In the Interest of Sayler, 44 Ill.App.3d 854 (Ill.App.Ct. 1977), cert. denied, 434 U.S. 925 (1977) 42

Klitzman, Klitzman & Gallagher v. Krut, 744 F.2d 955 (3d Cir. 1984) 75

Marvin v. United States, 732 F.2d 669 (8th Cir. 1984) 32

McVeigh v. Cohen, 983 F. Supp. 215 (D.C. Dist. 1998) 64

Michigan Bell Tel. Co. v. United States, 565 F.2d 385, 389 (6 Cir. 1977) 5

Mincey v. Arizona, 437 U.S. 385 (1978) 49

National City Trading Corp. v. United States, 635 F.2d 1020 (2d Cir. 1980) 75

O'Connor v. Ortega, 480 U.S. 709 (1987) 44

State v. Binns, 222 N.J. Super. 583 (App. Div. 1988), certif. denied, 111 N.J. 624 (1988) 53

State v. Bruzzese, 94 N.J. 210 (1983), cert. denied, 465 U.S. 1030 (1984) 38

State v. Coyle, 119 N.J. 194 (1990) 41

State v. Crumb, 307 N.J.Super. 204, 704 A.2d 952 certif. denied, 153 N.J. 215 (1998) 44

State v. Damplias, 282 N.J. Super. 471 (App. Div. 1995) 36

State v. Deluca, 325 N.J.Super. 376 (App. Div. 1999) 59

State v. Demeter, 124 N.J. 374 (1991) 3

State v. Douglas, 204 N.J. Super. 265 (App. Div. 1985), certif. denied, 102 N.J. 378 (1985) and 102 N.J. 393 (1986) 40,42

State v. Fair, 45 N.J. 77, 86 (1965) 22

State v. Hempele, 120 N.J. 182 (1990) 21

State v. Hill, 115 N.J. 169 (1989) 35

State v. Hoffman, 290 N.J. Super. 588 (App. Div. 1996), mod. on other grounds, 149 N.J. 564 (1997) 53

State v. Hunt, 95 N.J. 338 (1982) 61

State v. Jackson, 268 N.J. Super. 194 (Law Div. 1993) 21,39

State v. Johnson, 68 N.J. 349 (1975) 40

State v. Jones, 143 N.J. 4 (1995) 22,35

State v. Lewis, 116 N.J. 477 (1989) 38

State v. Liberti, 161 N.J. Super. 575 (App. Div. 1978), certif. denied, 79 N.J. 502 (1979) 34

State v. Love, 233 N.J. Super. 38, 43 (App. Div. 1989), certif. den., 118 N.J. 188 (1989) 22

State v. Maristany, 133 N.J. 299 (1993) 41

State v. Novembrino, 105 N.J. 95 (1987) 3

State v. Petrone, 161 Wis.2d 530, 544-45, N.W.2d 676, 681 (1991). 19

State v. Reldan, 100 N.J. 187 (1985) 19,47

State v. Santana, 215 N.J.Super. 63 (App.Div. 1987) 44

State v. Schumann, 156 N.J. Super. 563 (App. Div. (1978) 12

State v. Speid, 255 N.J. Super. 398 (Law Div. 1992) 34

State v. Stupi, 231 N.J. Super. 284 (App. Div. 1989) 38,49

State v. Suazo, 133 N.J. 315 (1993) 40

State v. Tunnel Citgo Services Inc., 149 N.J. Super. 427 (App. Div. 1977) 15,16 48

State v. Valencia, 93 N.J. 126 (1983) 34,38

State v. Wright, 61 N.J. 146, 149 (1972) 10,14

Steven Jackson Games v. United States, 816 F.Supp. 432 (W.D. Tex. 1993), aff'd on other grounds, 36 F.3d 457 (5th Cir. 1994) 66

Terry v. Ohio, 392 U.S. 1 (1968) 62

United States v. Beusch, 596 F.2d 871 (9th Cir. 1979) 70,72

United States v. Biasucci, 786 F.2d 504 (2d Cir. 1986), cert. denied, 479 U.S. 827 (1986) 5

United States v. Carey, 172 F.3d 1268 (10th Cir. Kan. 1999) 37

United States v. David, 756 F. Supp. 1385 (D. Nev. 1991) 39,41

United States v. Duran, 957 F.2d 499 (7th Cir. 1992) 42

United States v. Gawrysiak, 972 F. Supp. 853 (D.N.J. 1997) 71

United States v. Henson, 848 F.2d 1374 (6th Cir. 1988), cert. denied, 488 U.S. 1005 (1989) 16,48

United States v. Kimbrough, 69 F.3d 723 (5th Cir. 1995), cert. denied, 517 U.S. 1157 (1996) 24,29 52

United States v. Lacy, 119 F.2d 742 (9th Cir. 1997) 52

United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996) 14,24 26,27 28,52 72

United States v. Matias, 836 F.2d 744 (2d Cir. 1988) 48

United States v. Matlock, 415 U.S. 164 (1974) 40

United States v. Maxwell, 42 M.J. 568 (U.S.A.F. Ct. App. 1995), rev'd in part on other grounds, 45 M.J. 406 (C.A.A.F. 1996) 76

United States v. Musson, 650 F. Supp. 525 (D. Colo. 1986) 16,50

United States v. New York Tel. Co., 434 U.S. 159 (1977) 5

United States v. Pangburn, 983 F.2d 449 (2d Cir. 1993) 54

United States Postal Service v. C.E.C. Services, 869 F.2d 184 (2d Cir. 1989). . . . 23

United States v. Reyes, 798 F.2d 380, 382-83 (10th Cir. 1986). 17

United States v. Rodriguez, 968 F.2d 130 (2d Cir. 1991), cert. den., 506 U.S. 847 (1992) 13

United States v. Ross, 465 U.S. 798, 824 (1982) 20

United States v. Santarelli, 778 F.2d 609 (11th Cir. 1985) 70,71

United States v. Sawyer, 799 F. 2d 1494 (11th Cir. 1986), cert. denied, 479 U.S.

1069 (1987) 47

United States v. Shilling, 826 F.2d 1365 (4th Cir. 1987), cert. denied, 484 U.S. 1043 (1988) 51

United States v. Simpson, 152 F.3d 1241, 1348 (10th Cir. 1998) 19

United States v. Sissler, No. 1:90-CR-12, 1991 WL 239000 (W.D. Mich. Aug. 30, 1991), aff'd, 966 F.2d 1455 (6th Cir. 1992), cert. denied 506 U.S. 1079 (1993) 17,30 31

United States v. Smith, 155 F.3d 1051 (9th Cir. 1998) 59

United States v. Steerwell Leisure Corp., Inc., 598 F. Supp. 171 (W.D.N.Y. 1984) . 7

United States v. Tamura, 694 F.2d 591 (9th Cir. 1982) 48,52

United States v. Upham, 168 F. 3d. 532 (1st Cir. 1999), cert. denied, __ U.S. ___, 119 S.Ct. 2353, 144 L.Ed. 249 (1999) 6,20 24,26 51,52

United States v. Villegas, 899 F.2d 1324 (2d Cir. 1990), cert. denied, 498 U.S. 991 (1990) 5

United States v. Yung, 786 F. Supp. 1561 (D. Kan. 1992) 31,32

Waller v. Georgia, 467 U.S. 39 (1984) 58

Warden v. Hayden, 387 U.S. 294 (1967) 48

Zurcher v. Stanford Daily, 436 U.S. 547 (1978) 64

STATUTES

N.J.S.A. 2A:84A-21.9 51,64,66

N.J.S.A. 2A:156A-1 . . . . . 54,55 60

N.J.S.A. 2A:156A-1g 63

N.J.S.A. 2A:156A-2a 57

N.J.S.A. 2A:156A-2g 60

N.J.S.A. 2A:156A-2m 56

N.J.S.A. 2A:156A-2p 58

N.J.S.A. 2A:156A-2q 59

N.J.S.A. 2A:156A-2s 58

N.J.S.A. 2A:156A-4 60

N.J.S.A. 2A:156A-8 56

N.J.S.A. 2A:156A-27 46,54
57,58
59

N.J.S.A. 2A:156A-28 59

N.J.S.A. 2A:156A-29 60,63

N.J.S.A. 2A:156A-29a 60

N.J.S.A. 2A:156A-29e 60,61
64,66

N.J.S.A. 2A:156A-29f 61,63

N.J.S.A. 2A:156A-29g 63

18 U.S.C.A. § 2510 54

18 U.S.C.A. § 2701 46,54
57

18 U.S.C.A. § 2703 58

18 U.S.C.A. § 2703(c)(1)(C) 61

18 U.S.C.A. § 2703 (d) 62

42 U.S.C.A. §2000aa 55,64

42 U.S.C.A. §2000aa-6(a)(2) 66

RULES

Fed. R. Crim. P. 41 5

Fed. R. Evid. 901(b)(9) 78

N.J.R.E. 801(e) 76

N.J.R.E. 803(c)(6) 75

N.J.R.E. 901 78

N.J.R.E. 1001 76,77

N.J.R.E. 1001(d) 77

N.J.R.E. 1002 76

N.J.R.E. 1003 77

R. 3:1-2 13

R. 3:5A-4 62

R. 3:5-2 5,6
17

R. 3:5-3(b) 35

R. 3:5-5 54

OTHER SOURCES CITED

2 W. LaFave, Search and Seizure: A Treatise on the Fourth Amendment,
§ 3.7(d) at 379 (3d ed. 1996) 9,16
42,51

Electronic Surveillance and Communications Data Warrant Manual § 4 (Administrative Office of the
1994) 58

COMPUTER SEARCH CHECKLIST

I. The fundamental question to be answered before any computer search is what role did the computer play in the offense. To determine the role of a computer, it is essential to have as much information about the target computer or computers as possible. Also, keep in mind that a given computer may have more than one function. For instance a computer may be a hacker's tool but may also be where the hacker's records are stored. In assessing a computer's role, consider the following:

A. Is the computer contraband and therefore subject to seizure? (stolen or obtained by fraud)

B. Is the computer a tool or weapon used in the commission of the offense? (hacker's computer, credit card generator)

C. Is the computer an instrument of the offense? (Internet fraud scheme, child pornographer)

D. Is the computer a storage device?

II After the determination of the role of the computer in an offense, the next determination is where the evidence is likely to be found.

A. Is the evidence on the target's computer?

B. Is the evidence at an Internet Service Provider?

C. Is the evidence on a network?

D. Is the evidence at a remote location?

E. Is the evidence at multiple locations?

F. Is the evidence located out of the jurisdiction?

III. The location of the evidence dictates the procedure which must be used to obtain the evidence.

A. Can the information be obtained by Search Warrant?

B. Can the information be obtained by a Subpoena to a service provider?

C. Does the information sought require a Communications Data Warrant or

Communication Information Order?

D. Does the information sought require a Wiretap?

E. Does the information sought require application for a search warrant or other process in another State or Country?

IV In addition to the seizure of the computer, it is necessary to determine what else must be obtained to facilitate the analysis of the information.

A. Is there special software?

B. Are there passwords or phrases needed to gain access?

C. Is there other documentary evidence related to the crime or identity of the target?

D. Are there operating manuals or invoices?

V. Computer searches may also raise special concerns regarding the safety of the executing officers or the integrity of the evidence. Computer evidence is inherently volatile and easily destroyed. These concerns might require a "no-knock" warrant. Consider the following questions when assessing the danger to the officers or the evidence:

A. Is there evidence of an intent to destroy the evidence?

B. Is there evidence of an intent to injure law enforcement officer?

C. Is there remote access to the computer which would enable persons not present at the site to damage or destroy the evidence?

VI. Because modern computers come in a bewildering number of variations, from simple personal computers and Apple computers to sophisticated corporate networks, and have the ability to store enormous amounts of data, it will likely be necessary to incorporate language that allows the searcher to seize the computer or some of its components for analysis in a controlled environment. The following questions should be answered in assessing the need to seize computer components:

A. Is the computer part of a network?

B. Is there a large volume of evidence to be searched?

C. Is the computer unique in any way?

D. Does the computer setup need to be duplicated in the laboratory exactly in order to operate?

VII. The evidence in a given case may not necessarily be stored only in a desktop computer. The wide spread use of laptop computers, organizers and external storage devices requires a search for all potential sources of evidence including:

A. Floppy disks

B. Removable drives (Jazz, Zip, CD Rom)

C. Multiple hard drives

D. Laptop computers

E. Personal Digital Assistants (palm pilots and organizers)

F. Off site storage (may require an out-of-state or special warrant)

VIII. There are several specialized statutes which may impact a search for computer evidence. Therefore, prior to any search, consideration must be given to whether one of the following statutes will be implicated:

A. Privacy Protection Act

B. Stored Electronic Communications Act

C. Wiretap Act

SAMPLE WARRANT LANGUAGE

As discussed in Section II. A.6. of the Manual, it may be necessary to request authorization to take the computer off of the premises being searched for the purposes of analysis of the contents of the computer. The following language may be useful in justifying that request.

Volume of the Evidence

Computer storage devices like hard disks, diskettes, tapes, and laser disks generally can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

Technical Requirements

Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, coded or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

Training and Experience

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

A) The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many

system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software, operating systems, interfaces, hardware drivers, and any applications software which may have been used to create the data whether stored on hard drives or on external media, as well as all related instruction manuals or other documentation and data security devices.

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

SAMPLE SEARCH WARRANT

The following is a sample search warrant affidavit for computer evidence. The affidavit is structured as a records warrant, the most typical form of warrant used in connection with computer searches. This should be viewed a generic sample which must be modified for the depending on the circumstances associated with a particular warrant.

SUPERIOR COURT OF NEW JERSEY
LAW DIVISION - COUNTY OF

STATE OF NEW JERSEY)
: SS.
COUNTY OF)

CRIMINAL ACTION

APPLICATION FOR SEARCH WARRANTS

, being of full age, duly sworn according to law, upon his/her oath deposes and says:

1. I am presently employed as _____ . I have been so employed since _____ . I am presently assigned to _____. During my tenure, I have been assigned numerous cases involving _____ _____. I have actively assisted in (types of cases and activity, e.g. the monitoring of consensual intercepts, surveillance, undercover investigations as well as the procurement and execution of search warrants and subpoenas.) _____ _____ . In pursuit of these investigations, I have dealt with informants and defendants who have participated in these crimes. Some of the cases have involved _____ .

2. Based on the information which will be detailed in this affidavit, I have probable cause to believe and do believe that in and upon the below-described premises is located certain property which was used in the violation of the penal laws of this State; which was possessed, controlled, designed or intended for such use and which constitutes evidence of or tends to show the commission of the offenses of _____

_____.

The premises to be searched are described as follows:

A) The offices of _____ and more particularly described as:

B) The home of _____ and more particularly described as:

C) (Detail other places to be searched)

I.

ALLEGATIONS RELATING TO (2C Violations)

1. (List probable cause)

2. My review of records on file with _____ revealed that _____.

3. Investigation has revealed that information pertaining to this investigation was entered into the computer. (List detailed information relating to how the computer is used in the commission of the alleged offenses.)

4. Based on the foregoing, I have probable cause to believe and do believe that evidence of the crimes of _____ can be found in the offices of _____ located at _____ and in the home of _____ located at _____.

5. Based on the foregoing, it is respectfully requested that the Court issue a search warrant for the offices of _____ .

6. Based on the foregoing, it is also respectfully requested that the Court issue a search warrant for the home of _____ .

If Statutes require records to be maintained, the following may be applicable:

7. Based on my training and experience I know that _____ maintains large amounts of records. Further, _____ , requires _____ to keep permanent records. Further, _____ requires that these records be maintained for at least _____ years. Based on these requirements, I have probable cause to believe that the records indicated below may be found on the premises to be searched.

****

8. The specific evidence to be searched for and seized at the above-described locations is set forth below. As described below, some of the evidence to be searched for and seized is records. Permission is his/hereby sought to search for and seize these below-described records whether they are kept on paper, in computers or on electronic or magnetic storage media. The evidence to be searched for and seized is as follows:

a) (List types of records) during the period of _____ to the present, including but not limited to:

(1) (Record sought) whether in paper form or electronic media

b) Any and all electronic devices which are capable of analyzing, creating, displaying, converting or transmitting electronic or magnetic computer impulses or data. These

devices include: computer components, computer peripherals, word processing equipment, modems, monitors, printers, plotters, encryption circuit boards, optical scanners, external hard drives, and other computer-related electronic devices;

c) Any and all instructions or programs stored in the form of electronic or magnetic media which are capable of being interpreted by a computer or related components. The items to be seized include operating systems, application software, utility programs, compilers, interpreters and other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio or other means of transmission;

d) Any and all written or printed material which provides instructions, examples, concerning the operation of a computer system, computer software, and/or any related device;

e) Any and all information pertaining to passwords and/or encryption relating to the computer system, computer software, and/or any related device;

f) Any and all of the above described information and/or data stored in the form of magnetic or electronic coding on computer media capable of being read by a computer or with the aid of computer related equipment. This media includes floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, video cassettes, CD ROM and other media which is capable of storing magnetic coding;

9. It is requested that the following be considered regarding computerized evidence:

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

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

b) Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, coded or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

c) Seizure of computer equipment & related devices, software, and documentation. Based upon my knowledge, training and experience, I know that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true for the following reasons:

1) The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software.

2) Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software, operating systems, interfaces, hardware drivers, and any applications software which may have been used to create the data whether stored on hard drives or on external media, as well as all related instruction manuals or other documentation and data security devices.

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

10. It is also specifically requested that the Search Warrant authorize any appropriate Law Enforcement Agency access to the items referred to in _____, the authority to open these items, view their contents and copy and reproduce all images and data contained this/herein.

11. It is also specifically requested that the Search Warrant authorize access to get files that have been “hidden”, erased, compressed, password protected, or encrypted.

_____

Sworn Law Enforcement Officer

Sworn To and Subscribed
Before Me This Day of
, 1999.

_____

COMMUNICATION INFORMATION ORDER

As detailed in section IV B. of the Manual, the Administrative Office of the Courts have designated the Court Order provided for in N.J.S.A. 2A:156A-29(e) as a Communication Information Order (CIO). Applications for CIO's must be taken to the appropriate Communications Data Warrant Judge. The standard to be utilized in evaluating the application is "specific and articulable facts showing reasonable grounds that record is relevant and material to investigation." The types of information which can be obtained from an Electronic Communication Service or Remote Computing Service by means of a CIO include billing information; methods and history of payment; access and Internet protocol (IP) logs; IP addresses; method of connection; connection times and dates. However, the CIO may not request the content of stored electronic communications or toll billing records. For that information it is necessary to obtain a Communications Data Warrant. The form to be utilized should be essentially identical to a CDW but it should request an Order and not a Warrant.

The CIO is designed to permit law enforcement to obtain valuable information in an Internet investigation and to facilitate the development of an investigation where there is insufficient evidence to establish the probable cause necessary to obtain the contents of stored electronic communications.

SAMPLE COMMUNICATIONS DATA WARRANT

SUPERIOR COURT OF NEW JERSEY
COUNTY OF _____

AFFIANT: YOUR NAME AND BADGE
YOUR ORGANIZATION

IN THE MATTER OF THE APPLICATION OF THE STATE OF NEW JERSEY FOR A COMMUNICATIONS DATA WARRANT TO OBTAIN THE CONTENTS OF STORED ELECTRONIC COMMUNICATIONS AND SUBSCRIBER NAME, ADDRESS, CONTACT TELEPHONE NUMBERS, AND FULL ACCOUNT INFORMATION ASSOCIATED WITH SCREEN NAME **List Screen Name/Internet Provider** AND FOR ALL ASSOCIATED INFORMATION, INCLUDING BUT NOT LIMITED TO ACCOUNT BILLING INFORMATION, METHOD AND HISTORY OF PAYMENT, USAGE, ACCESS AND INTERNET PROTOCOL LOGS, CUSTOMER SERVICE RECORDS, AND ANY STATIC OR DYNAMIC INTERNET PROTOCOL ADDRESSES ASSOCIATED WITH THE ACCOUNTS.	)	AFFIDAVIT

STATE OF NEW JERSEY)
ss.
COUNTY OF)

1. I**, Your name and badge number**, of full age, having been duly sworn according to law upon my oath depose and say:

2. I am applying to the Court for the purpose of securing a Communications Data Warrant to obtain the contents of stored electronic communications and subscriber name, address, contact telephone numbers, and full account information associated with screen name **list screen name/Internet Provider** and for all associated information, including but not limited to account billing information, method and history of payment, usage, access and Internet protocol logs, customer service records and any static or dynamic Internet protocol address associated with the accounts. This order is sought to seize and secure evidence of the crime of **cite statute.**

3. I, **Your name and badge number,** have been a sworn member of **your organization. List training and experience**.

4. In my current assignment, I am responsible for conducting and assisting in investigations into **list applicable offenses**.

5. I am familiar with the techniques and methods of operations used by individuals involved in criminal activity to conceal those activities from detection by law enforcement authorities. I have conducted and participated in investigations into the activities and individuals and groups involved in criminal enterprises including **list types of cases worked.**

6. **If applicable, you may list that** I have read publications and documents regarding the methodologies employed by those involved in the commission of high technology crimes.

7. **If applicable, you may list that** As a result of my training and experience, I am familiar with the methods employed by individuals to commit crimes through the use of computer systems. I am familiar with the tools and materials used by individuals carrying out their attacks against computer systems or using computers to facilitate their illegal acts.

8. The facts tending to establish the grounds for this application and the probable cause that such grounds exist are as follows:

9. **List probable cause.**

10. Based on the contents of this affidavit, and my training and experience, I have probable cause to believe that the contents of stored electronic communications and subscriber name, address, contact telephone numbers, and full account information associated with screen name **list screen name/Internet Provider** and for all associated information, including but not limited to account billing information, method and history of payment, usage, access and Internet protocol logs, customer service records and any static or dynamic Internet protocol address associated with the accounts will provide information leading to the identity of the person or persons involved in the violations of the penal laws of the State of New Jersey, or which constitute evidence of, or tends to show violations of **cite statute**.

11. This application for a Communications Data Warrant has not been presented to any other Superior Court Judge in the State of New Jersey. Therefore, it is respectfully requested that based on the foregoing, **List Internet Provider**, be directed to provide the contents of stored electronic communications and subscriber name, address, contact telephone numbers, and full account information associated with screen name **list screen name/Internet Provider** and for all associated information, including, but not limited to account billing information, method and history of payment, usage, access and Internet protocol logs, customer service records and any static or dynamic Internet protocol address associated with the accounts.

12. It is also requested that **List Internet Provider** be ordered not to disclose to subscribers or any other persons, that information is being sought or that **List Internet Provider** has been

ordered to provide any information to **List your name and badge** or other law enforcement officers regarding this matter.

Respectfully submitted,

_____
Your name and badge number
Your unit
Your organization

SWORN AND SUBSCRIBED
BEFORE ME THIS _____ DAY
OF _____

_____
JUDGE OF THE SUPERIOR COURT

SAMPLE SUBPOENA LANGUAGE

N.J.S.A. 2A:156A-29(f) provides that "a provider of electronic communication service or remote computing service shall disclose to a law enforcement agency the name, address, telephone number or other subscriber number or identity, and length of service provided to the subscriber or customer of such service and types of service the subscriber or customer utilized, when the law enforcement entity obtains a grand jury or trial subpoena."

In light of the very specific categories of information which can be obtained by subpoena, it is recommended that any subpoena requesting subscriber information, do so utilizing the statutory language for example:

"The name, address, telephone number or other subscriber number or identity, and length of service provided to the subscriber or customer of such service and types of service the subscriber or customer utilized associated with screen name ABC123."