Computer-Based Investigation and Discovery in Criminal Cases: A Guide for United States Magistrate Judges

National Workshop for Magistrate Judges
San Francisco, California
February 19-21, 2003

Kenneth J. Withers
Federal Judicial Center
Washington, DC

I. Draft PowerPoint slides (*please note: these slides were created on January 13, 2003 and are subject to change before presentation*) 2

II. Annotated Case Law 8

III. Excerpts from *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Second Edition (Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, September 2002)

Appendix B: Sample 18 U.S.C. Sec. 2703(d) Application and Order 11

Appendix D: Three Model Trap and Trace Orders 21

Appendix E: Sample Subpoena Language 38

Appendix F: Sample Language for Search Warrants and Accompanying Affidavits to Search and Seize Computers 40

IV. Susan W. Brenner and Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 Mich. Telecomm. & Tech. L. Rev. 39 (2002) 57

V. Draft Report and Recommendations of the Joint Administrative Office/Department of Justice Working Group on Electronic Technology in the Criminal Justice System *(please note: this is a draft document approved by the AOUSC, but not yet approved by DOJ, and may be subject to revision before final publication is authorized)* 133

Computer-Based Investigation and Discovery in Criminal Cases: A Guide for United States Magistrate Judges

Ken Withers
FJC Research Division
February 19, 2003

Federal Judicial Center

Slide 01

Federal Judicial Center

Differences between conventional and computer-based evidence

- Volume of data
- Co-mingling of information
  - On a single hard drive
  - On a computer network
- Ability to instantly transmit, alter, delete data
  - Need for immediate security
  - Need for special handling procedures

Slide 02

Federal Judicial Center

Differences between conventional and computer-based evidence

- Non-obvious nature of computer data
- Ability to recover deleted data using forensic techniques
- Experts, experts everywhere
  - Danger of technical obfuscation
- Confusion between data and devices
  - Which is being seized?
  - Which is being searched?

Slide 03

Federal Judicial Center

Differences between conventional and computer-based evidence

- Number of possible locations
- Involvement of third parties
- Ever-changing "legitimate and reasonable expectation of privacy"

Slide 04

Federal Judicial Center

Search warrants: probable cause requirement

- Items sought are probably connected to specific criminal activity
  - Probable guilt of suspect not a factor
- Items sought are probably to be found where specified
  - Relationship between IP address and physical location
  - United States v. Grant, 218 F. 3d 72 (1st Cir. 2000)

Slide 05

Federal Judicial Center

Search warrants: probable cause requirement

- Passage of time
  - Will suspect delete data? Is data recoverable?
  - United States v. Hay, 231 F. 3d 630 (9th Cir. 2000)
  - United States v. Zimmerman, 277 F. 3d 426 (3d Cir. 2002)

Slide 06

Federal Judicial Center

Search warrants: particularized description requirement

- Relationship between probable cause and scope of search
- Balancing act between anticipated particularity and unfolding reality
  - United States v. Upham, 168 F. 3d 532 (1st Cir. 1999)

Slide 07

Federal Judicial Center

Search warrants: particularized description requirement

- Warrant to seize information v. warrant to seize hardware ("data or devices")
- Davis v. Gracey, 111 F. 3d 1472 (10th Cir. 1997)
- United States v. Gawrysiak, 972 F. Supp. 853, aff'd. 178 F. 3d 1281 (3d Cir. 1999)

Slide 08

Federal Judicial Center

Search warrants: particularized description requirement

- "All records" search may be overbroad
  - United States v. Hunter, 13 F. Supp. 2d 574 (D. Vt. 1998)
- But some room for law enforcement discretion is needed
  - United States v. Lacy, 119 F. 3d 742 (9th Cir. 1997)

Slide 09

Federal Judicial Center

Search warrants: privileged and irrelevant information

- Law enforcement regulations and practices for searching records of doctors, lawyers, clergy
  - 42 U.S.C. Sec. 2000aa-11(a)
  - 28 C.F.R. Sec. 59.4(b)
  - U.S. Attorneys' Manual, Sec. 9-13.420 (1997)

Slide 10

Federal Judicial Center

Search warrants: privileged and irrelevant information

- *In camera* review
- Appointment of special master
- Use of "taint team"
- See United States v. Sattur, et al., Order dated June 12, 2002 (S.D.N.Y.)

Slide 11

Federal Judicial Center

Search warrants: detailing the search procedure

- Practical extension of "particularized description" requirement
- Anticipates issues and problems
- Gives notice to property owner

Slide 12

Federal Judicial Center

Search warrants: detailing the search procedure

- On-site v. off-site debate
- Distinguish from "data or devices"
- Is off-site inspection more or less reasonable under the circumstances?
  - Limitations of "file cabinet" analogy
  - Limitations of technology currently available to law enforcement
  - Intrusiveness of procedures v. convenience to law enforcement

Slide 13

Federal Judicial Center

Search warrants: detailing the search procedure

- "Key word" v. file-by-file inspection
- Staged inspection procedures with check points and reporting dates

Slide 14

Federal Judicial Center

Search warrants: duration of forensic investigation period

- Related to "reasonableness" of search
- Does Fed. R. Crim. P. 41 requirement that "search" be conducted within 10 days apply?
- Rule 41(e) motions for return of property
- Common orders range from 7 to 30 days
  - Law enforcement usually want "months"
- United States v. Brunette, 76 F. Supp. 2d 30 (D. Me. 1999)

Slide 15

Federal Judicial Center

Searches without warrants: "plain view" doctrine

- Elements
  - Agent must be in lawful position to view incriminating evidence
  - Incriminating character of evidence must be apparent
  - Resolves questions of reasonable expectation of privacy

Slide 16

Federal Judicial Center

Searches without warrants: "plain view" doctrine

- NOT an authorization to open and view computer files without a warrant
  - U.S. v. Turner, 169 F. 3d 84 (1st Cir. 1999)

Slide 17

Federal Judicial Center

Searches without warrants: "closed container" concept

- Closely related to "plain view"
  - United States v. Carey, 172 F. 3d 1268 (10th Cir. 1999)
  - United States v. Runyan, 275 F. 3d 449 (5th Cir. 2001)
  - United States v. Slanina, 283 F. 3d 670 (5th Cir. 2002)

Slide 18

Federal Judicial Center

Searches without warrants: searches "incident to arrest"

- Need to preserve evidence
- Need to avoid harm to officers or public
- Inspections of briefcases, wallets, address books, pagers have been allowed
- Seizure (not inspection) of Zip disk allowed
  - United States v. Tank, 200 F. 3d 627 (9th Cir. 2000)
- Does increased capacity of portable devices increase reasonable expectation of privacy?

Slide 19

Federal Judicial Center

Searches without warrants: "exigent circumstances" exception

- Agent must have reasonable belief that people would immediately be harmed or evidence would immediately be destroyed
- Computer data can be destroyed quickly and unintentionally
- May justify search incident to arrest
  - United States v. Ortiz, 84 F 3d 997 (7th Cir. 1996)
- Does not support subsequent search of seized device

Slide 20

Federal Judicial Center

Searches without warrants: "consent to search"

- Consent may be explicit or implicit, but must be knowing and voluntary
  - Reasonableness of expectation of privacy, especially in public or in workplace
- Consent is limited to reasonable expectation of scope
  - United States v. Runyan, 275 F. 3d 449 (5th Cir. 2001)

Slide 21

Federal Judicial Center

Searches without warrants: searches by third parties

- Workplace searches
  - Questions of consent and apparent authority
  - Role of system administrators
- Home searches
  - Parents, spouses, roommates, landlords
  - Indicia of an "expectation of privacy"

Slide 22

Federal Judicial Center

Computer surveillance: Electronic Communications Privacy Act

- 18 U.S.C. Sec. 2701-2712
- Complicated statute extends 4th Amendment considerations into cyberspace (and limits them, too)
- Generally allows subpoena of information held by network administrators, with certain privacy protections
- Series of classifications:
  - Type of network services provider
  - Type of information sought
  - Method of obtaining disclosure (voluntary or compelled)

Slide 23

Federal Judicial Center

Searches of Internet Service Providers (ISPs)

- Transactional records
- Subscriber information
- Substance of communications
  - Chat room transcripts
  - Email
  - Files

Slide 24

Federal Judicial Center

Computer surveillance: pen registers/trap and trace

- 18 U.S.C. Sec. 3121-3127
- "[I]nformation likely to be obtained is relevant to an ongoing criminal investigation"
- Limited to information *about* communications
- Limited review of applications balanced by strong punishment for violation of orders under 18 U.S.S. Sec. 3121(d)

Slide 25

Federal Judicial Center

Computer surveillance: Wiretap Act (Title III)

- 18 U.S.C. Sec. 2501-2722
- Governs real-time surveillance of *content* of communications
- "Electronic communication" intended to be broad; "intercept" intended to be narrow
- Prohibition and standard of review for wiretap applications high (restricted to Article III judges)

Slide 26

Federal Judicial Center

Computer surveillance: Wiretap Act (Title III)

- Question: when does electronic surveillance become a Title III issue?
- Computer-based surveillance technology blurs distinction between transmission data and content
  - "Carnivore" example

Slide 27

Federal Judicial Center

Computer surveillance: Patriot Act

- Expanded subscriber information that can be obtained under ECPA
- Explicitly extended reach of pen/trap statute to include computer-based technologies
- Removed "stored wire communication" from Title III and moved it to ECPA
  - Voice mail now under ECPA

Slide 28

Federal Judicial Center

Computer-based discovery: what's out there?

- Fed. R. Crim. P. 16(a)(1)(C): Documents and tangible objects
- Fed. R. Crim. P. 16(a)(1)(D): Reports of examinations and tests
- Reciprocal under Rules 16(b)(1)(A) and (B)
- Brady material
- Fed. R. Crim. P. 17(c): Material from third parties

Slide 29

Federal Judicial Center

Computer-based discovery: what's NOT out there?

- Fed. R. Crim. P. 16(a)(2) and 16 (b)(2) exclude all prosecution and defense "work product," broadly defined

Slide 30

Federal Judicial Center

Computer-based disclosures necessary under evidence rules

- Fed. R. Evid. 901(9)
  - Authentication of computer-based evidence by process or system
- Fed. R. Evid. 1006
  - Summaries of voluminous data admitted if source data are available

Slide 31

Federal Judicial Center

Joint AO/DOJ Working Group on Electronic Technology in the Criminal Justice System: Report

- Computer-based information is pervasive and can be harnessed
- Lack of physical resources
- Lack of training
- Disparities between parties
- Unanticipated upfront costs offset anticipated savings

Slide 32

Federal Judicial Center

Joint AO/DOJ Working Group on Electronic Technology in the Criminal Justice System: Recommendations

- Bring investigative agencies into process
- Establish working groups at the local level
- Training for all attorneys
- Avoid blanket rules on form of disclosure or presentation
- "Meet and confer" early on technology in discovery and at trial
- Explore ways to share effort, costs

Slide 33

Computer-Based Investigation and Discovery in Criminal Cases: A Guide for United States Magistrate Judges

Ken Withers
FACT Research Division
February 19, 2003

Federal Judicial Center

Slide 34

Annotated Case Law

Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997). Users of e-mail and electronic bulletin board services challenged action of police officers who executed a warrant calling for search of online service provider's business premises and seizure of virtually all computers, computer-related equipment, including e-mail and software incidentally stored therein, in pursuit of pornographic images and evidence of distribution. The court held that the computer equipment was more than the container of files and records of unlawful activity, it was also the instrumentality of the crime alleged.

U.S. v. Bach, 2002 WL 31545304 (8th Cir. 2002). Search and seizure of defendant's e-mail by employees of the defendant's Internet Service Provider (ISP) were reasonable under the Fourth Amendment, a no person or premises were searched by police, all items seized were located on the ISP's premises, the search was authorized by a judge, and the officers involved complied with all relevant provisions of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701 et seq.

U.S. v. Barth, 26 F. Supp. 2d 929 (W.D. Tex. 1998). A computer hard drive constituted a "closed container," and a warrant was necessary to authorize a search, even when the computer had been delivered to a technician for repairs.

U.S. v. Brunette, 76 F. Supp. 2d 30 (D. Me. 1999). Investigators failed to conduct search of seized computers within 30 days, as required by the terms of the warrant, and subsequently failed to conduct search within 30-day extension granted by magistrate judge, who granted the defendant's motion to suppress based on violation of the warrant.

U.S. v. Campos, 221 F.2d 1143 (10th Cir. 2000). Warrant authorizing agents to seize computer equipment and remove it to a lab for inspection was not overbroad, in that the affidavit accompanying the warrant application explained that the computer equipment itself was a probable instrumentality of the crime and that inspection of the computer equipment in a controlled environment over a period or weeks or months was necessary.

U.S. v. Carey, 172 F.3d 1268 (10th Cir. 1999). Warrant authorized search of computer for "names, telephone numbers, ledger, receipts, addresses, and other documentary evidence pertaining to the sales and distribution of controlled substances." Officer's search for image files (".jpg's") with sexually suggestive file names after opening one such file was beyond the scope of the warrant. Defendant's consent or the plain view doctrine, allowing for continued warrantless search, were not applicable. *Cf*. **U.S. v. Gray,** 78 F. Supp. 2d 524 (E.D. Va. 1999), in which an agent authorized by warrant to search the defendant's computer for files related to computer hacking, opened and viewed several image files containing child pornography to determine that they were outside the scope of the warrant. The image files were subsequently used as evidence in a child pornography prosecution and the defendant's motion to suppress was denied.

U.S. v. Gawrysiak, 972 F. Supp. 853, *aff'd*, 178 F.3d 1281 (3d Cir. 1999). Warrant authorizing search for computer-based information was not violated when agents took possession of computer equipment and subsequently conducted search according to plan described in affidavit accompanying application.

U.S. v. Grant, 218 F.3d 72 (1st Cir. 2000). Evidence linked Internet account activity with defendant's physical presence in home at the same time, giving rise to probable cause that defendant was using Internet account at that time.

U.S. v. Hall, 142 F.3d 988 (7th Cir. 1998). A warrant authorizing the seizure of an entire computer was justified, when the warrant contained language narrowly defining the types of files sought, specifically child pornography. Investigators would not, under the terms of the warrant, be free to rummage through the defendant's property.

U.S. v. Hay, 231 F.3d 630 (9th Cir. 2000). Seizure of computer hardware was a reasonable method for executing a warrant for evidence of digital child pornography, as the hardware was likely to contain the evidence and the accompanying affidavit described the procedure to be used.

U.S. v. Hunter, 13 F. Supp. 2d 574 (D. Vt. 1998). A search warrant calling for the seizure of "all" computers, storage devices, and software systems from the defendant attorney was overbroad and failed to comply with the particularity requirement of the Fourth Amendment. But the detailed search protocol attached to the warrant application assured that the searching agents, monitoring agents, and computer forensics technicians would retrieve relevant files without undue intrusion, and provided adequate basis for applying the good faith exception to the exclusionary rule.

U.S. v. Lacy, 119 F.3d 742 (9th Cir. 1997), *cert. denied*, 523 E.S. 1101 (1998). Although the description of computer equipment to be seized for later searching was in generic terms, the description of files to be seized was specific enough to meet the particularity requirement of the Fourth Amendment.

U.S. v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996). A search of the defendant's e-mail stored on an Internet Service Provider's (ISP's) computer system required a warrant, as the defendant demonstrated a subjective expectation of privacy in e-mail communication in the way he used it and that expectation was objectively reasonable, evidenced by the existence of federal statutes protecting e-mail privacy and the terms of the contract the defendant had with the ISP.

U.S. v. Ortiz, 84 F.3d 997 (7th Cir. 1996). Agents were justified in searching a pager without a warrant but incident to arrest, as information contained in a pager is easily destroyed.

U.S. v. Runyan, 275 F.3d 449 (5th Cir. 2001). Police exceeded the scope of a private search when they searched an entire collection computer disks provided by the defendant's wife. The disks constituted "containers" and scope of private search was limited to those disks which the wife had identified as containing child pornography.

U.S. v. Simons, 206 F.3d 392 (4th Cir. 2000). A warrantless search of the defendant's hard drive using a remote computer did not violate the Fourth Amendment, when the defendant had no reasonable expectation of privacy in files downloaded from the Internet, using a federal agency computer at his workplace, where a clearly articulated "Internet use policy" was in place.

U.S. v. Slanina, 283 F.3d 670 (5th Cir. 2002). Initial warrantless search by government official of government employee's computer was reasonable, as employee had no reasonable expectation of privacy.

U.S. v. Smith, 27 F. Supp. 2d 1111 (C.D. Ill 1998). Defendant's girlfriend validly consented to a warrantless search of the defendant's computer when the girlfriend initiated the call to the police, had free physical access to the computer, the defendant had encouraged her to use it in the past, and the computer was not password protected.

U.S. v. Tank, 200 F.3d 627 (9th Cir. 2000). Agents searching a car incident to a lawful arrest properly seized a Zip disk, which later was found to contain digital child pornography.

U.S. v. Turner, 169 F.3d 84 (1st Cir. 1999). Consent was not given for a warrantless search of computer files, when defendant consented to police search of his home after neighbor had been assaulted. Police, inspecting the upstairs of the home while defendant was downstairs, accidentally knocked computer, activating image of nude female on screen, and prompting police to search the computer for more such images. The court held that a search for computer files was beyond what an objectively reasonable person would have understood as the object of the police search under these circumstances.

U.S. v. Upham, 168 F.3d 1999 (1st Cir. 1999), *cert. denied*, 527 U.S. 1011 (1999). A warrant authorizing the search ands seizure of "any and all computer software and hardware" was not unconstitutionally overbroad, where no narrower method of obtaining digital child pornography files was available to law enforcement. In dicta, the court commented that if the images could have been obtained on-site using a less obtrusive method, there might be no justification for seizing all computer equipment. The court also commented that deletion of 1,400 images from the computer hard drive and diskettes did not in and of itself constitute "abandonment" and surrender of privacy rights in the files, as it might if they were paper files placed in the trash.

U.S. v. Zimmerman, 277 F.3d 426 (3d Cir. 2002). A lapse of six months before a warrant application for digital adult pornography rendered the potential evidence stale and negated probable cause. Adult pornography and child pornography distinguished.

Excerpt from *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Second Edition* (Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, September 2002)

APPENDIX B

Sample 18 U.S.C. § 2703(d) Application and Order

NOTE: Sample information specific to a particular case is enclosed in brackets; this sample information should be replaced on a case-by-case basis. Language required only if the application seeks to obtain the contents of communications (and therefore requires customer notification) is in bold.

UNITED STATES DISTRICT COURT
FOR THE_____ DISTRICT OF_____

	)	
IN RE APPLICATION OF THE	)	
UNITED STATES OF AMERICA FOR	)	MISC. NO. ____
AN ORDER PURSUANT TO	)	
18 U.S.C. § 2703(d)	)	**Filed Under Seal**

APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703 (d)

_____, an Assistant United States Attorney for the _____ District of _____, hereby files under seal this ex parte application for an order pursuant to 18 U.S.C. § 2703(d) to require [name of provider or service], an [description of provider or service, e.g. an educational institution] located in the _____ District of _____ at _____, which functions as [an electronic communications service provider AND/OR a remote computing service] for its [description of users, e.g. students, faculty and others] to provide records and other information [add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **and contents of a wire or electronic communication** pertaining to [subscriber] , one of its customers or subscribers. The records and other information requested are set forth as an Attachment to the Application and to the proposed Order. In support of this Application, the United States asserts:

LEGAL AND FACTUAL BACKGROUND

1. The United States Government, including the Federal Bureau of Investigation and the Department of Justice, are investigating intrusions into a number of computers in the United States and abroad that occurred on [dates of intrusion], and which

may be continuing. The computers that have been attacked include [name(s) of intruded computer systems].

2. These intrusions are being investigated as possible violations of, inter alia, [list possible charges, e.g. 18 U.S.C. § 1030 (fraud and related activities in connection with computers) and 18 U.S.C. § 2511 (interception and disclosure of wire, oral and electronic communications).]

3. Investigation to date of these incidents provides reasonable grounds to believe that [provider or service] has records and other information pertaining to certain of its subscribers that are relevant and material to an ongoing criminal investigation. Because [provider or service] functions as [an electronic communications service provider (provides its subscribers access to electronic communication services, including e-mail and the Internet) AND/OR a remote computing service (provides computer facilities for the storage and processing of electronic communications)], 18 U.S.C. § 2703 sets out particular requirements that the government must meet in order to obtain access to the records and other information it is seeking.

4. Here, the government seeks to obtain three categories of information: (1) basic subscriber information; (2) records and other information pertaining to certain subscribers of [provider or service]; [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **and (3) the contents of electronic communications in [provider or service] (but not in electronic storage).** (fn1)

5. A subpoena allows the government to obtain subscriber name, address, length and type of service, connection and session records, telephone or instrument number including any temporarily assigned network address, and means and source of payment information. 18 U.S.C. § 2703(c)(2). The government may also compel such information through an order issued pursuant to 18 U.S.C. § 2703(d). 18 U.S.C. §§ 2703(c)(1)(B), (c)(2).

6. To obtain records and other information pertaining to subscribers of an electronic communications service or remote computing service, the government must comply with 18 U.S.C. § 2703(c)(1), which provides, in pertinent part:

> A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity- . . .
> (B) obtains a court order for such disclosure under subsection (d) of this section.

7. [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **To obtain the contents of a wire or electronic communication in a remote computing service, or in electronic storage for more than one hundred and eighty days in an electronic communications system, the government must comply with 18 U.S.C. § 2703(b)(1)(B), which provides, in pertinent part:**

> **A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph 2 of this subsection --**
> **. . . .**
>
> > **(B) with prior notice from the government entity to the subscriber or customer if the governmental entity --**
> >
> > **. . . .**
> >
> > > **(ii) obtains a court order for such disclosure under subsection (d) of this section;**
>
> **except that delayed notice may be given pursuant to section 2705 of this title.**

8. [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **18 U.S.C. § 2703(b)(2) states that 2703(b) applies with respect to any wire or electronic communication that is held or maintained on a remote computing service--**

> **(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and**
>
> **(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.**

9. Section 2703(d), in turn, provides in pertinent part:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction (fn2) and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. . . . A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Accordingly, this application sets forth the specific and articulable facts showing that there are reasonable grounds to believe that the materials sought are relevant and material to the ongoing criminal investigation into the attacks on [intruded computer systems].

THE RELEVANT FACTS

10. On [date intrusion was discovered], an unauthorized intrusion was discovered into the [intruded computer system]. Investigation into this incident revealed that the intruder had obtained so-called "root" or system administrator level access into the [intruded computer system], effectively giving him complete control of the system.

11. On [successive date(s) of intrusion] the intruder(s) again connected to the [intruded computer system]. Based on the identification number (IP number [999.999.999.999]) logged by the [investigating party] as the source of the intrusion, investigators were able to determine that the connection had originated from [provider or service].

12. [FURTHER SPECIFIC AND ARTICULABLE FACTS SHOWING REASONABLE GROUNDS TO BELIEVE MATERIALS SOUGHT ARE RELEVANT AND MATERIAL TO THE CRIMINAL INVESTIGATION]

13. The conduct described above provides reasonable grounds to believe that a number of federal statutes may have been violated, [including 18 U.S.C. §§ ,].

14. Records of customer and subscriber information relating to [target of investigation] that are available from [provider or service], [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **AND/OR the contents of electronic communications (not in electronic storage)** that may be found at [provider or service] will help government investigators identify the individual(s) who are responsible for the unauthorized access of the computer systems described above and to determine the nature and scope of the intruder's activities. Accordingly, the government requests that [provider or service] be directed to produce all records described in Attachment A to this Application, which information is divided into several parts. Part A requests the account name, address, telephone number, e-mail address, billing information, and other identifying information for [target of investigation].

15. Part B consists of [target of investigation]'s "User Connection Logs" from [date] through the date of the court's order, for the computer account assigned to [target of investigation], and for the specific terminal he was found to be operating on [dates of intrusion]. Although the first known intrusion occurred on [earliest date of known intrusion], experience has shown that successful computer intrusions are usually preceded by scanning activity that helps would-be intruders identify potential targets and identify their vulnerabilities. In this case, investigators have determined that many [intruded computer systems] systems were scanned in this manner during [time period of intrusion]. As a result, this information is directly relevant to identifying the individuals responsible. The information should include the date and time of connection and disconnection, the method of connection to [provider or service], the data transfer volume, and information related to successive connections to other systems.

16. [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **Part C requests the contents of electronic communications (not in electronic storage) that were placed or stored in [provider or service] computer systems in directories or files owned or controlled by the accounts identified in Part A. Investigators anticipate that these files may contain hacker tools, materials similar to those previously left on the [intruded computer system] computer found by the system administrators, and files containing unlawfully obtained passwords to other compromised systems. These stored files, covered by 18 U.S.C. § 2703(b)(2), will help ascertain the scope and nature of the possible intrusion activity conducted by [target of investigation] from [provider or service]'s computers.**

17. The information requested should be readily accessible to [provider or service] by computer search, and its production should not prove to be burdensome.

18. The United States requests that this Application and Order be sealed by the Court until such time as the court directs otherwise.

19. The United States further requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), that [provider or service] be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this order for such period as the court deems appropriate. The United States submits that such an order is justified because notification of the existence of this order could seriously jeopardize the ongoing investigation. Such a disclosure could give the subscriber an opportunity to destroy evidence, notify confederates, or flee or continue his flight from prosecution. [Optional Buckley Amendment language for cases where provider is an educational institution receiving federal funding: The Government requests that [provider or service]'s compliance with the delayed notification provisions of this Order should also be deemed authorized under 20 U.S.C. § 1232g(b)(1)(j)(ii). See 34 CFR § 99.31(a)(9)(i) (exempting requirement of prior notice for disclosures made to comply with a judicial order or lawfully issued subpoena where the disclosure is made pursuant to "any other subpoena issued for a law enforcement purpose and the court or other issuing agency has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed")].

20. [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **The United States further requests, pursuant to the delayed notice provisions of 18 U.S.C. § 2705(a), an order delaying any notification to the subscriber or customer that may be required by § 2703(b) to obtain the contents of communications, for a period of 90 days. Providing prior notice to the subscriber or customer could seriously jeopardize the ongoing investigation, as such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.**

WHEREFORE, it is respectfully requested that the Court grant the attached Order, (1) directing [provider or service] to provide the United States with the records and information described in Attachment A; (2) directing that the Application and Order be sealed;

(3) directing [provider or service] not to disclose the existence or content of the Order, except to the extent necessary to carry out the Order, and directing that three certified copies of this Order and Application be provided by the Clerk of this Court to the United States Attorney's Office; [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **(4) directing that the notification by the government otherwise required under 18 U.S.C. § 2703(b) be delayed for ninety days.**

Executed on _____.

_____
Assistant United States Attorney

Fn1: "Electronic storage" is a term of art, specifically defined in 18 U.S.C. § 2510(17) as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The government does not seek access to any such materials. Communications not in "electronic storage" include any e-mail communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.

Fn2: 18 U.S.C. § 2711(3) states "the term 'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation."

ATTACHMENT A

You are to provide the following information as printouts and as ASCII data files (or describe media on which you want to receive the information sought), if available:

A. The following customer or subscriber account information for any accounts registered to [subscriber], or associated with [subscriber]. For each such account, the information shall include:
   1. name(s) and e-mail address;
   2. address(es);
   3. local and long distance telephone connection records, or records of session times and durations;
   4. length of service (including start date) and types of service utilized;
   5. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
   6. the means and source of payment for such service (including any credit card or bank account number).

B. User connection logs for:
   (1) all accounts identified in Part A, above,
   (2) the IP address [list IP address, e.g. 999.999.999.999], for the time period beginning [date] through and including the date of this order, for any connections to or from [provider or service].

   User connection logs should contain the following:
   1. Connection time and date;
   2. Disconnect time and date;
   3. Method of connection to system (e.g., SLIP, PPP, Shell);
   4. Data transfer volume (e.g., bytes);
   5. Connection information for other systems to which user connected via [provider or service], including:
      a. Connection destination;
      b. Connection time and date;
      c. Disconnect time and date;
      d. Method of connection to system (e.g., telnet, ftp, http);
      e. Data transfer volume (e.g., bytes);
      f. Any other relevant routing information.

C. [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **The contents of electronic communications (not in electronic storage (fn1)) that were placed or stored in [provider or service]'s computer systems**

in directories or files owned or controlled by the accounts identified in Part A at any time after [date of earliest intrusion] up through and including the date of this Order.

Fn1: "Electronic storage" is a term of art, specifically defined in 18 U.S.C. § 2510(17) as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The government does not seek access to any such materials. Communications not in "electronic storage" include any e-mail communications received by the specified accounts that the owner or user of the account has already accessed, viewed, or downloaded.

UNITED STATES DISTRICT COURT
FOR THE_____ DISTRICT OF _____

	)	
IN RE APPLICATION OF THE	)	
UNITED STATES OF AMERICA FOR	)	MISC. NO. _____
AN ORDER PURSUANT TO	)	
18 U.S.C. § 2703(d)	)	**Filed Under Seal**

ORDER

This matter having come before the court pursuant to an application under Title 18, United States Code, Section 2703(b) and (c), which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing [provider or service] , an electronic communications service provider and a remote computing service, located in the _____ District of _____, to disclose certain records and other information, as set forth in Attachment A to the Application, the court finds that the applicant has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information [Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **and the contents of a wire or electronic communication** sought are relevant and material to an ongoing criminal investigation.

IT APPEARING that the information sought is relevant and material to an ongoing criminal investigation, and that prior notice of this Order to any person of this investigation or this application and order entered in connection therewith would seriously jeopardize the investigation;

IT IS ORDERED pursuant to Title 18, United States Code, Section 2703(d) that [provider or service] will, within three days of the date of this Order, turn over to agents of the Federal Bureau of Investigation the records and other information as set forth in Attachment A to this Order.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three (3) certified copies of this Application and Order.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, and that [provider or service] shall not disclose the existence of the Application or this Order of the Court, or the existence of the investigation, to the listed subscriber or to any other person, unless and until authorized to do so by the Court. [Optional Buckley Amendment language: Accordingly, [provider or service]'s compliance with the non-disclosure provision of this Order shall be deemed authorized under 20 U.S.C. § 1232g(b)(1)(j)(ii).]

[Add only if the application seeks to obtain the contents of communications pursuant to § 2703(b)] **IT IS FURTHER ORDERED that the notification by the government otherwise required under 18 U.S.C. 2703(b)(1)(B) be delayed for a period of [ninety days].**

_____
United States Magistrate Judge

_____
Date

Excerpt from *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Second Edition* (Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, September 2002)

APPENDIX D

This appendix contains three separate model forms for pen register/trap and trace orders on the Internet: an IP trap and trace for a web-based e-mail account; a pen register/trap and trace order to collect addresses on e-mail sent to and from a target account; and an IP pen register/trap and trace order for use in investigating a computer network intrusion.

1) Model form for IP trap and trace on a web-based e-mail account

The sample application and order below are specifically designed for use to locate and/or identify the person using a specified web-based e-mail account on a service such as Yahoo or Hotmail. The order authorizes the collection of the numeric network address(es) -- i.e., the Internet Protocol (IP) address(es) -- from which the user accesses the account. That information, in turn, can be used to trace the user to the other Internet site (such as an ISP, a cybercafe, or a public library terminal) from which he or she accessed the webmail service. It is primarily useful in cases (such as fugitive investigations) where the objective is to identify and locate the user.

Note that this order is not designed to collect the e-mail addresses to which the user sends e-mail messages from the web-based account, nor to collect the addresses from which the account owner receives e-mail. That type of order -- which might be used, for example, to discover the co-conspirators of a criminal known to use e-mail in his/her conspiratorial activities -- would not ask for (or even discuss) IP addresses, and would normally require discussion of the pen register provisions of the statute as well as trap and trace. (For a sample application and order including such language, see the second model form in this appendix. Note that using the latter will likely slow the process of having the provider implement the order, so it should be used only where the additional information - i.e., To: and From: on e-mail traffic sent from/to the target account - is needed.)

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

	)	
IN THE MATTER OF THE APPLICATION	)	
OF THE UNITED STATES OF AMERICA	)	No.
FOR AN ORDER AUTHORIZING THE	)	
INSTALLATION AND USE OF A TRAP	)	
AND TRACE DEVICE	)	
	)	**FILED UNDER SEAL**

APPLICATION

_____, the United States Attorney for the _____ District of _____, by _____, an Assistant United States Attorney for the _____ District of _____, hereby applies to the Court pursuant to 18 U.S.C. § 3122 for an order authorizing the installation and use of a trap and trace device. In support of this application, he/she states the following:

1. Applicant is an "attorney for the Government" as defined in Rule 54(c) of the Federal Rules of Criminal Procedure, and therefore, pursuant to Title 18, United States Code, Section 3122(a), may apply for an order authorizing the installation and use of trap and trace devices.

2. Applicant certifies that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by [investigative agency], in connection with possible violations of Title 18, United States Code, sections _____.

3. [As a result of information obtained through previous orders issued by this Court,] investigators believe that the offense under investigation has been and continues to be accomplished through the user account _____ at _____, an electronic communication service provider located at _____. The listed subscriber for this account is [name], [address], [telephone]. _____, and others yet unknown, are the subjects of the above investigation.

4. A trap and trace device is defined in Title 18, United States Code, Section 3127(4) as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." This definition reflects the significant amendments made by the USA PATRIOT Act of 2001 § 216, Pub. L. No. 107-56, 115 Stat. 272, 288-90 (2001).

5. [webmail provider] is a provider of free electronic mail communication services. [provider's] users access its services by means of the Internet's World Wide Web. Using a standard web browser program (such as Netscape or Internet Explorer), [provider's] users may compose, send, and receive electronic mail through the computers in [provider's] network.

6. Whenever an Internet user visits [provider's] web site (or any other web site on the Internet), that user's computer identifies itself to the web site by means of its Internet Protocol address. An Internet Protocol ("IP") address is a unique numeric identifier assigned to every computer attached to the Internet. An Internet service provider (ISP) normally controls a range of several hundred (or even thousands of) IP addresses, which it assigns to its customers for their use.

7. IP numbers for individual user accounts (such as are sold by ISPs to the general public) are usually assigned "dynamically": each time the user dials into the ISP to connect to the Internet, the customer's machine is assigned one of the available IP addresses controlled by the ISP. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, however, that IP address becomes available to other customers who dial in thereafter. Thus, an individual customer's IP address normally differs each time he dials into the ISP. By contrast, an ISP's business customer will commonly have a permanent, 24-hour Internet connection to which a "static" (i.e., fixed) IP address is assigned.

8. These source IP addresses are, in the computer network context, conceptually identical to the origination phone numbers captured by traditional trap and trace devices installed on telephone lines. Just as traditional telephonic trap and trace devices may be used to determine the source of a telephone call (and thus the identity of the caller), it is feasible to use a combination of hardware and software to ascertain the source addresses of electronic connections to a World Wide Web computer, and thereby to identify and locate the originator of the connection.

9. Accordingly, for the above reasons, the applicant requests that the Court enter an order authorizing the installation and use of a trap and trace device to identify the source IP address (along with the date and time) of all logins to the subscriber account [user account] at [provider]. The applicant is not requesting, and does not seek to obtain, the contents of any communications.

10. The applicant requests that the foregoing installation and use be authorized for a period of 60 days.

11. The applicant further requests that the Order direct that, upon service of the order upon it, [provider] furnish information, facilities, and technical assistance necessary to accomplish the installation of the trap and trace device, including installation and operation of the device unobtrusively and with a minimum of disruption of normal

service. [provider] shall be compensated by [investigating agency] for reasonable expenses incurred in providing such facilities and assistance in furtherance of the Order.

12. The applicant further requests that the Order direct that the information collected and recorded pursuant to the Order shall be furnished to [investigating agency] at reasonable intervals during regular business hours for the duration of the Order.

13. The applicant further requests that the Order direct that the tracing operation shall encompass tracing the communications to their true source, if possible, without geographic limit.

14. The applicant further requests that pursuant to Title 18, United States Code, Section 3123(d)(2) the Court's Order direct [provider], and any other person or entity providing wire or electronic communication service in the United States whose assistance is used to facilitate the execution of this Order (pursuant to 18 U.S.C. § 3123(a)), and their agents and employees not to disclose to the listed subscriber, or any other person, the existence of this Order, the trap and trace device, or this investigation unless or until otherwise ordered by the court and further, pursuant to Title 18, United States Code, Section 3123(d)(1), that this application and Order be SEALED.
The foregoing is based on information provided to me in my official capacity by agents of [investigative agency].

I declare under penalty of perjury that the foregoing is true and correct.

Dated this _____ day of _____, 2002.

_____
Assistant United States Attorney

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION	)	No.
OF THE UNITED STATES OF AMERICA	)	
FOR AN ORDER AUTHORIZING THE	)	
INSTALLATION AND USE OF A TRAP	)	
AND TRACE DEVICE	)	
	)	**FILED UNDER SEAL**

ORDER

This matter has come before the Court pursuant to an application under Title 18, United States Code, Section 3122 by _____, an attorney for the Government, which application requests an Order under Title 18, United States Code Section 3123 authorizing the installation and use of a trap and trace device to determine the source Internet Protocol address (along with date and time) of login connections directed to the user account _____ at [provider name], which is located at [address of provider]. The account is registered to [name/address].

The Court finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violations of Title 18, United States Code, Section _____, by _____ [and others yet unknown].

IT IS THEREFORE ORDERED, pursuant to Title 18, United States Code, Section 3123, that a trap and trace device be installed and used to determine the source Internet Protocol address (along with date and time) of login connections directed to the user account [user account], but not the contents of such communications;

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(c)(1), that the use and installation of the foregoing occur for a period not to exceed 60 days;

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(b)(2) and in accordance with the provisions of section 3124(b), that [provider] , upon service of the order upon it, shall furnish information, facilities, and technical assistance necessary to accomplish the installation of the trap and trace device, including installation and operation of the device unobtrusively and with a minimum of disruption of normal service;

IT IS FURTHER ORDERED, that the results of the trap and trace device shall be furnished to [agency] at reasonable intervals during regular business hours for the duration of the Order;

IT IS FURTHER ORDERED, that the tracing operation shall encompass tracing the communications to their true source, if possible, without geographic limit;

IT IS FURTHER ORDERED that [agency] compensate [provider] for expenses reasonably incurred in complying with this Order; and

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(d), that [provider], and any other person or entity providing wire or electronic communication service in the United States whose assistance is used to facilitate the execution of this Order (pursuant to 18 U.S.C. § 3123(a)), and their agents and employees shall not disclose to the listed subscriber, or any other person, the existence of this Order, the trap and trace device, or this investigation unless or until otherwise ordered by the court and further, pursuant to Title 18, United States Code, Section 3123(d)(1), that this application and Order be SEALED.

Dated this _____ day of _____, 2002.

_____
UNITED STATES MAGISTRATE JUDGE

2) Model form for pen register/trap and trace order to collect addresses on e-mail sent to/from the target account.

The sample application and order below are specifically to collect the e-mail addresses to which the user sends e-mail messages from an account, and to collect the addresses from which the account owner receives e-mail.

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

	)	
IN THE MATTER OF THE APPLICATION	)	
OF THE UNITED STATES OF AMERICA	)	No.
FOR AN ORDER AUTHORIZING THE	)	
INSTALLATION AND USE OF PEN	)	
REGISTER AND TRAP AND TRACE DEVICES	)	
	)	**FILED UNDER SEAL**

APPLICATION

_____, the United States Attorney for the _____ District of _____, by _____, an Assistant United States Attorney for the _____ District of _____, hereby applies to the Court pursuant to 18 U.S.C. § 3122 for an order authorizing the installation and use of pen register and trap and trace devices. In support of this application, he/she states the following:

1. Applicant is an "attorney for the Government" as defined in Rule 54(c) of the Federal Rules of Criminal Procedure, and therefore, pursuant to Title 18, United States Code, Section 3122(a), may apply for an order authorizing the installation and use of pen register and trap and trace devices.

2. Applicant certifies that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by [investigative agency], in connection with possible violations of Title 18, United States Code, sections _____.

3. [As a result of information obtained through previous orders issued by this Court,] investigators believe that the offense under investigation has been and continues to be accomplished through the user account _____ at _____, an electronic communication service provider located at _____. The listed subscriber for this account is [name], [address], [telephone]. _____, and others yet unknown, are the subjects of the above investigation.

4. A pen register, as defined in Title 18, United States Code, Section 3127(3), is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." A trap and trace device is defined in Title 18, United States Code, Section 3127(4) as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." These definitions reflect the significant amendments made by the USA PATRIOT Act of 2001 § 216, Pub. L. No. 107-56, 115 Stat. 272, 288-90 (2001).

5. [provider] is a provider of electronic mail communication services.

6. It is possible to identify the other addresses with which a user of [provider's] service is communicating via e-mail. The "headers" on an electronic mail message contain, among other information, the network addresses of the source and destination(s) of the communication. Internet electronic mail addresses adhere to the standardized format "username@network", where username identifies a specific user mailbox associated with network , the system on which the mailbox is located. Standard headers denoting the source and destination addresses of an electronic mail message are "To:" and "Cc:" (destinations), and "From:" (source). For example, a message containing the headers

From: jane@doe.com
To: richard@roe.com
Cc: pat@address.com

indicates that user "jane" (on the doe.com system) is the sender, and that users "richard" (with a mailbox on roe.com) and "pat" (at address.com) are the intended recipients. Multiple destination addresses may be specified in the To: and Cc: fields.

7. These source and destination addresses, analogous to the origination and destination phone numbers captured by traditional trap and trace devices and pen registers installed on telephone lines, constitute "routing" and "addressing" information within the meaning of the statute, as amended by the USA PATRIOT Act in October 2001. As with traditional telephonic pen registers and trap and trace devices, it is feasible to use a combination of hardware and software to ascertain the source and destination addresses associated with Internet electronic mail.

8. Accordingly, for the above reasons, the applicant requests that the Court:

A. Enter an order authorizing the installation and use of a trap and trace device to identify the source address of electronic mail communications directed to the subscriber account [user account] at [provider].

B. Enter an order authorizing the installation and use of a pen register to determine the destination addresses of electronic mail communications originating from [user account], along with the date and time of such communications.

The applicant is not requesting, and does not seek to obtain, the contents of any communications.

9. The applicant requests that the foregoing installation and use be authorized for a period of 60 days.

10. The applicant further requests that the Order direct that, upon service of the order upon it, [provider] furnish information, facilities, and technical assistance necessary to accomplish the installation of the pen register and trap and trace device, including installation and operation of the device unobtrusively and with a minimum of disruption of normal service. [provider] shall be compensated by [investigating agency] for reasonable expenses incurred in providing such facilities and assistance in furtherance of the Order.

11. The applicant further requests that the Order direct that the information collected and recorded pursuant to the Order shall be furnished to [investigating agency] at reasonable intervals during regular business hours for the duration of the Order.

12. The applicant further requests that the Order direct that the tracing operation shall encompass tracing the communications to their true source, if possible, without geographic limit.

13. The applicant further requests that pursuant to Title 18, United States Code, Section 3123(d)(2) the Court's Order direct [provider], and any other person or entity providing wire or electronic communication service in the United States whose assistance is used to facilitate the execution of this Order, and their agents and employees not to disclose to the listed subscriber, or any other person, the existence of this Order, the pen register and trap and trace devices, or this investigation unless or until otherwise ordered by the court and further, pursuant to Title 18, United States Code, Section 3123(d)(1), that this application and Order be SEALED.

The foregoing is based on information provided to me in my official capacity by agents of [investigative agency].

I declare under penalty of perjury that the foregoing is true and correct.

Dated this _____ day of _____, 2002.

_____
Assistant United States Attorney

UNITED STATES DISTRICT COURT
_____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION	)	No.
OF THE UNITED STATES OF AMERICA	)	
FOR AN ORDER AUTHORIZING THE	)	
INSTALLATION AND USE OF PEN	)	
REGISTER AND TRAP AND TRACE DEVICES	)	
	)	**FILED UNDER SEAL**

ORDER

This matter has come before the Court pursuant to an application under Title 18, United States Code, Section 3122 by _____, an attorney for the Government, which application requests an Order under Title 18, United States Code Section 3123 authorizing the installation and use of pen register and trap and trace devices to collect the source addresses of electronic mail communications directed to, and destination addresses of electronic mail communications originating from, user account _____ at [provider name]. [provider name] is located at [address of provider]. The account is registered to [name/address].

The Court finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violations of Title 18, United States Code, Section _____, by _____ [and others yet unknown].

IT IS THEREFORE ORDERED, pursuant to Title 18, United States Code, Section 3123, that pen register and trap and trace devices be installed and used to identify the source address of electronic mail communications directed to, and the destination addresses of electronic mail communications originating from, [user account], along with the date and time of such communications, but not the contents of such communications;

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(c)(1), that the use and installation of the foregoing occur for a period not to exceed 60 days;

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(b)(2) and in accordance with the provisions of section 3124(b), that [provider] , upon service of the order upon it, shall furnish information, facilities, and technical assistance necessary to accomplish the installation of the pen register and trap and trace devices, including installation and operation of the devices unobtrusively and with a minimum of disruption of normal service;

IT IS FURTHER ORDERED, that the results of the pen register and trap and trace devices shall be furnished to [agency] at reasonable intervals during regular business hours for the duration of the Order;

IT IS FURTHER ORDERED, that the tracing operation shall encompass tracing the communications to their true source, if possible, without geographic limit;

IT IS FURTHER ORDERED that [agency] compensate [provider] for expenses reasonably incurred in complying with this Order; and

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(d), that [provider name], and any other person or entity providing wire or electronic communication service in the United States whose assistance is used to facilitate the execution of this Order, and their agents and employees shall not disclose to the listed subscriber, or any other person, the existence of this Order, the pen register and trap and trace devices, or this investigation unless or until otherwise ordered by the court and further, pursuant to Title 18, United States Code, Section 3123(d)(1), that this application and Order be SEALED.

Dated this day of _____, 2002.

_____
UNITED STATES MAGISTRATE JUDGE

3) Model form for IP pen register/trap and trace on a computer network intruder

The sample application and order below are designed for use in investigating a computer network intrusion. The order authorizes the collection of source and destination information (e.g., source and destination IP addresses and ports) for network transmissions to and from a specified network computer. Because the order does not authorize the collection of communications contents, it is not a substitute for an order issued under Title III, 18 U.S.C. § 2510 et seq. The order is primarily useful in situations where the objective is to identify and locate the intruder, or to map the intruder's patterns of behavior (such as the identities of other network hosts used or victimized by the intruder).

IN THE UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION	)	
OF THE UNITED STATES OF AMERICA	)	
FOR AN ORDER AUTHORIZING THE	)	MISC. NO.
INSTALLATION AND USE OF A PEN	)	
REGISTER AND TRAP & TRACE DEVICE	)	

A P P L I C A T I O N

_____, an Assistant United States Attorney for the ____ District of _____, applies for an order authorizing the installation and use of pen register and trap and trace devices on an Internet-connected computer operated by [victim institution name and address], in the _____ District of _____. In support of said application, the applicant states:

1. The applicant is an "attorney for the government" as defined in Rule 54(c) of the Federal Rules of Criminal Procedure, and therefore, pursuant to Title 18, United States Code, Section 3122, may apply for an order authorizing the installation and use of trap and trace devices and pen registers.

2. The applicant certifies that Federal Bureau of Investigation is conducting a criminal investigation of unknown individuals in connection with possible violations of 18 U.S.C. § 1030 (fraud and related activity involving computers, i.e., "computer hacking") and related statutes; that it is believed that the subjects of the investigation are using a computer system operated by the [victim], in the _____ District of _____ , in furtherance of the described offenses; and that the information likely to be obtained from the pen register and trap and trace devices is relevant to the ongoing criminal investigation.

Specifically, the information derived from such an order would provide evidence of the source of the attacks [and the identity of other systems being used to coordinate the attacks].

3. A pen register, as defined in Title 18, United States Code, Section 3127(3), is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." A trap and trace device is defined in Title 18, United States Code, Section 3127(4) as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." These definitions reflect the significant amendments made by the USA PATRIOT Act of 2001 § 216, Pub. L. No. 107-56, 115 Stat. 272, 288-90 (2001).

4. Data packets transmitted over the Internet -- the mechanism for all Internet communications -- contain addressing information closely analogous to origination phone numbers captured by traditional trap and trace devices installed on telephone lines and destination phone numbers captured by traditional pen registers. Devices to determine the source and destinations of such communications can be implemented through a combination of hardware and software.

5. To date, the investigation has identified a computer at [victim] which is being used to commit or assist in the commission of the offenses under investigation, a machine identified by the Internet Protocol address (fn1) _____. Based upon the configuration of the system, any incoming or outgoing port may be used for communication, including redirected communications, involved in the offenses under investigation. (fn2)

6. The investigation to date indicates that [brief recitation of relevant facts].

[7. It is believed that TCP ports 25, 80, 110, and 143 (relating to e-mail and Worldwide Web traffic (fn3) are not being used in the commission of these crimes and that traffic on these ports can be excluded from the scope of the order.]

8. Accordingly, for the above reasons, the applicant requests that the Court enter an order authorizing the use of pen register and trap and trace devices to trace the source and destination of all electronic communications directed to or originating from any port (except ports 25, 80, 110, and 143) of the [victim] computer identified by the network address _____ and to record the date, time, and duration of the transmissions of these communications for a period of 60 days. The applicant is not requesting, and does not seek to obtain, the contents of such electronic communications (as defined at 18 U.S.C. § 2510(8)).

9. The applicant further requests that the Order direct that [victim] , and any other electronic communications provider whose assistance may (pursuant to 18 U.S.C. § 3123(a)) facilitate the execution of the order, upon service of the order upon them, furnish information, facilities, and technical assistance necessary to accomplish the installation of the trap and trace devices and pen registers including installation and operation of the devices unobtrusively and with a minimum of disruption of normal service. These entities shall be compensated by the Federal Bureau of Investigation for reasonable expenses incurred in providing such facilities and assistance in furtherance of the Order.

10. The applicant further requests that the Order direct that the information collected and recorded pursuant to the Order be furnished to Special Agents of the Federal Bureau of Investigation at reasonable intervals during regular business hours for the duration of the Order.

11. The applicant further requests that the Order direct that the tracing shall encompass tracing the communications to their true source, if possible, without geographic limit.

12. Further, applicant respectfully requests the Court order that, pursuant to 18 U.S.C. § 3123(d)(2), [victim] and any other person or entity providing wire or electronic communication service in the United States whose assistance is used to facilitate the execution of this Order, and their agents and employees, make no disclosure of the existence of this Application and Order, except as necessary to effectuate it, unless and until authorized by this Court and that, pursuant to 18 U.S.C. § 3123(d)(1), the Clerk of Court seal the Order (and this Application) until further order of this Court. Providing prior notice to the subjects of the investigation could seriously jeopardize the ongoing investigation, as such a disclosure would give the subjects of the investigation an opportunity to destroy evidence, change patterns of behavior to evade detection, notify confederates, or flee from prosecution.

The foregoing is based on information provided to me in my official capacity by agents of the Department of Justice, including the Federal Bureau of Investigation.

Executed on ___, 2002.

_____
Assistant United States Attorney

Fn 1: An Internet Protocol (IP) address is a unique numerical address identifying each computer on the Internet. IP addresses are conventionally written in the dot-punctuated form *num1.num2.num3.num4* (*e.g.,* 192.168.3.47).

Fn 2: A "port" in the Transmission Control Protocol used over the Internet is a numeric identifier for a particular type of service being offered by a machine. For example, port

80 is typically reserved for World Wide Web traffic, so that a computer that wishes to retrieve information from a web server would typically connect to port 80. Often, however, hackers run programs which listen at a particular port, but do not provide the typically expected protocol at that port. These are often used as "back doors" into computer systems.

Fn3: TCP port 25 is specifically reserved for the Simple Mail Transfer Protocol (commonly referred to as SMTP), port 80 is reserved for Hypertext Transfer Protocol (HTTP, or web traffic), port 110 is reserved for the Post Office Protocol version 3 (POP3), and port 143 is reserved for the Internet Mail Access Protocol (IMAP). **[Modify list of excluded ports as needed.]**

IN THE UNITED STATES DISTRICT COURT
FOR THE _____ DISTRICT OF _____

IN THE MATTER OF THE APPLICATION	)	
OF THE UNITED STATES OF AMERICA	)	
FOR AN ORDER AUTHORIZING THE	)	MISC. NO.
INSTALLATION AND USE OF A PEN	)	
REGISTER AND TRAP & TRACE DEVICE	)	

O R D E R

This matter comes before the Court pursuant to an application under Title 18, United States Code, Section 3122 by _____ , an attorney for the government, which application requests an order under Title 18, United States Code, Section 3123 authorizing the installation and use of a pen register and trap and trace devices on computers operated by [victim] , which computers are located at_____. The Court finds that the applicant has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation into possible violations of 18 U.S.C. § 1030 by individuals currently unknown.

IT IS ORDERED, pursuant to Title 18, United States Code, Section 3123, that agents of the Federal Bureau of Investigation may install trap and trace devices to trace the source and destination of all electronic communications directed to or originating from any port (except ports 25, 80, 110, or 143) of the computer at [victim] computer network with the network address _____ and record the date, time, and duration (but not the contents) of these communications for a period of 60 days.

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(b)(2), that [victim] and any other electronic communications provider whose assistance may (pursuant to 18 U.S.C. § 3123(a)) facilitate the execution of the order, upon service of this Order upon them, shall furnish information, facilities, and technical assistance necessary to accomplish the installation of the trap and trace devices and pen registers including installation and operation of the devices unobtrusively and with a minimum of disruption of normal service;

IT IS FURTHER ORDERED, that the Federal Bureau of Investigation compensate [victim] and any other person or entity providing wire or electronic communication service in the United States whose assistance is used to facilitate the execution of this Order for expenses reasonably incurred in complying with this Order;

IT IS FURTHER ORDERED, that the results of the trap and trace devices and the pen registers shall be furnished to the Federal Bureau of Investigation at reasonable intervals during regular business hours for the duration of the Order; and

IT IS FURTHER ORDERED, that the tracing operation shall encompass tracing the communications to their true source, if possible, without geographic limit;

IT IS FURTHER ORDERED, pursuant to Title 18, United States Code, Section 3123(b), that this Order and the Application be sealed until otherwise ordered by the Court, and that [victim] and any other person or entity providing wire or electronic communication service in the United States whose assistance is used to facilitate the execution of this Order shall not disclose the existence of the trap and trace devices and pen registers, or the existence of the investigation to any person, except as necessary to effectuate this Order, unless or until otherwise ordered by the Court.

ENTERED: _____, 2002

FOR THE COURT:

_____
United States Magistrate Judge

Excerpt from *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Second Edition* (Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, September 2002)

APPENDIX E

Sample Subpoena Language

Post-PATRIOT Act: The Government is not required to provide notice to a subscriber or customer for the items sought in Part A. below. The information requested below can be obtained with use of an administrative subpoena authorized by Federal or State statute or a Federal or State grand jury or trial subpoena or a § 2703(d) order or a search warrant. See § 2703(c)(2). **If you request the items in Part B (contents), then you must give prior notice or delay notice pursuant to § 2705(a).**

Attachment To Subpoena

You are to provide the following information as [insert specifics on how you want to receive the information, e.g. printouts and as ASCII data files (on 100 megabyte disk for use with a Zip drive, if available, etc.)]:

A. For any accounts registered to [subscriber], or [associated with subscriber], [you should routinely add associated accounts because many ISPs may not provide the associated account information unless specifically requested] the following customer or subscriber account information:

(A) name(s);

(B) address(es);

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number)

B. The contents of wire or electronic communications held or maintained in [ISP's] computer systems on behalf of the accounts identified in Part A at any

time up through and including the date of this Subpoena, EXCEPT THAT you should NOT produce any unopened incoming communications (i.e., communications in "electronic storage") less than 181 days old.

> "Electronic storage" is defined in 18 U.S.C. § 2510(17) as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The government does not seek access to any such materials, unless they have been in "electronic storage" for more than 180 days.

Excerpt from *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Second Edition* (Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice, September 2002)

APPENDIX F

Sample Language for Search Warrants and Accompanying Affidavits to Search and Seize Computers

This appendix provides sample language for agents and prosecutors who wish to obtain a warrant authorizing the search and seizure of computers. The discussion focuses first on the proper way to describe the property to be seized in the warrant itself, which in turn requires consideration of the role of the computer in the offense. The discussion then turns to drafting an accompanying affidavit that establishes probable cause, describes the agent's search strategy, and addresses any additional statutory or constitutional concerns.

I. DESCRIBING THE PROPERTY TO BE SEIZED FOR THE WARRANT

The first step in drafting a warrant to search and seize computers or computer data is to describe the property to be seized for the warrant itself. This requires a particularized description of the evidence, contraband, fruits, or instrumentality of crime that the agents hope to obtain by conducting the search.

Whether the "property to be seized" should contain a description of information (such as computer files) or physical computer hardware depends on the role of the computer in the offense. In some cases, the computer hardware is itself contraband, evidence of crime, or a fruit or instrumentality of crime. In these situations, Fed. R. Crim. P. 41 expressly authorizes the seizure of the hardware, and the warrant will ordinarily request its seizure. In other cases, however, the computer hardware is merely a storage device for electronic files that are themselves contraband, evidence, or instrumentalities of crime. In these cases, the warrant should request authority to search for and seize the information itself, not the storage devices that the agents believe they must seize to recover the information. Although the agents may need to seize the storage devices for practical reasons, such practical considerations are best addressed in the accompanying affidavit. The "property to be seized" described in the warrant should fall within one or more of the categories listed in Rule 41(b):

(1) "property that constitutes evidence of the commission of a criminal offense"

This authorization is a broad one, covering any item that an investigator "reasonably could . . . believe" would reveal information that would aid in a particular apprehension or conviction. *Andresen v. Maryland*, 427 U.S. 463, 483 (1976). *Cf. Warden v. Hayden*, 387 U.S. 294, 307 (1967) (noting that restrictions on what evidence may be seized result mostly from the probable cause requirement). The word "property" in Rule 41(b)(1) includes both tangible and intangible property. *See United States v. New York Tel. Co.,* 434 U.S. 159, 169 (1977) ("Rule 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."); *United States v. Biasucci*, 786 F.2d 504, 509-10 (2d Cir. 1986) (holding that the fruits of video surveillance are "property" that may be seized using a Rule 41 search warrant). Accordingly, data stored in electronic form is "property" that may properly be searched and seized using a Rule 41 warrant. *See United States v. Hall*, 583 F. Supp. 717, 718-19 (E.D. Va. 1984).

(2) "contraband, the fruits of crime, or things otherwise criminally possessed"

Property is contraband "when a valid exercise of the police power renders possession of the property by the accused unlawful and provides that it may be taken." *Hayden*, 387 U.S. at 302 (quoting *Gouled v. United States*, 255 U.S. 298, 309 (1921)). Common examples of items that fall within this definition include child pornography, *see United States v. Kimbrough*, 69 F.3d 723, 731 (5th Cir. 1995), pirated software and other copyrighted materials, *see United States v. Vastola*, 670 F. Supp. 1244, 1273 (D.N.J. 1987), counterfeit money, narcotics, and illegal weapons. The phrase "fruits of crime" refers to property that criminals have acquired as a result of their criminal activities. Common examples include money obtained from illegal transactions, *see United States v. Dornblut*, 261 F.2d 949, 951 (2d Cir. 1958) (cash obtained in drug transaction), and stolen goods. *See United States v. Burkeen*, 350 F.2d 261, 264 (6th Cir. 1965) (currency removed from bank during bank robbery).

(3) "property designed or intended for use or which is or had been used as a means of committing a criminal offense"

Rule 41(b)(3) authorizes the search and seizure of "property designed or intended for use or which is or had been used as a means of committing a criminal offense." This language permits courts to issue warrants to search and seize instrumentalities of crime. *See United States v. Farrell*, 606 F.2d 1341, 1347 (D.C. Cir. 1979). Computers may serve as instrumentalities of crime in many ways. For example, Rule 41 authorizes the seizure of computer equipment as an instrumentality when a suspect uses a computer to view, acquire, and transmit images of child pornography. *See Davis v. Gracey*, 111 F.3d 1472, 1480 (10th Cir. 1997) (stating in an obscenity case that "the computer equipment was more than merely a 'container' for the files; it was an instrumentality of the crime."); *United States v. Lamb*, 945 F. Supp. 441, 462 (N.D.N.Y. 1996). Similarly, a hacker's computer may be used as an instrumentality of crime, and a computer used to run an illegal Internet gambling business would also be an instrumentality of the crime.

Here are examples of how to describe property to be seized when the computer hardware is merely a storage container for electronic evidence:

(A) All records relating to violations of 21 U.S.C. § 841(a) (drug trafficking) and/or 21 U.S.C. § 846 (conspiracy to traffic drugs) involving [the suspect] since January 1, 1996, including lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions; any information related to sources of narcotic

drugs (including names, addresses, phone numbers, or any other identifying information); any information recording [the suspect's] schedule or travel from 1995 to the present; all bank records, checks, credit card bills, account information, and other financial records.

The terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including floppy diskettes, hard disks, ZIP disks, CD-ROMs, optical discs, backup tapes, printer buffers, smart cards, memory calculators, pagers, personal digital assistants such as Palm Pilot computers, as well as printouts or readouts from any magnetic storage device); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

(B) Any copy of the X Company's confidential May 17, 1998 report, in electronic or other form, including any recognizable portion or summary of the contents of that report.

(C) ***[For a warrant to obtain records stored with an ISP pursuant to 18 U.S.C. Section 2703(a)]*** *All stored electronic mail of any kind sent to, from and through the e-mail address [JDoe@isp.com], or associated with the user name "John Doe," account holder [suspect], or IP Address [xxx.xxx.xxx.xxx] / Domain name [x.com] between Date A at Time B and Date X at Time Y. Content and connection log files of all activity from January 1, 2000, through March 31, 2000, by the user associated with the e-mail address [JDoe@isp.com], user name "John Doe," or IP Address [xxx.xxx.xxx.xxx] / Domain name [x.x.com] between Date A at Time B and Date X at Time Y. including dates, times, methods of connecting (e.g., telnet, ftp, http), type of connection (e.g., modem, cable / DSL, T1 / LAN), ports used, telephone dial-up caller identification records, and any other connection information or traffic data. All business records, in any form kept, in the possession of [Internet Service Provider], that pertain to the subscriber(s) and account(s) associated with the e-mail address [JDoe@isp.com], user name "John Doe," or IP Address [xxx.xxx.xxx.xxx] / Domain name [x.x.com] between Date A at Time B and Date X at Time Y, including records showing the subscriber's full name, all screen names associated with that subscriber and account, all account names associated with that subscriber, methods of payment, phone numbers, all residential, business, mailing, and e-mail addresses, detailed billing records, types and lengths of service, and any other identifying information.*

Here are examples of how to describe the property to be seized when the computer hardware itself is evidence, contraband, or an instrumentality of crime:

(A) Any computers (including file servers, desktop computers, laptop computers, mainframe computers, and storage devices such as hard drives, Zip disks, and

floppy disks) that were or may have been used as a means to provide images of child pornography over the Internet in violation of 18 U.S.C. § 2252A that were accessible via the World Wide Website address www.[xxxxxxxx].com.

(B) IBM Thinkpad Model 760ED laptop computer with a black case

II. DRAFTING AFFIDAVITS IN SUPPORT OF WARRANTS TO SEARCH AND SEIZE COMPUTERS

An affidavit to justify the search and seizure of computer hardware and/or files should include, at a minimum, the following sections: (1) definitions of any technical terms used in the affidavit or warrant; (2) a summary of the offense, and, if known, the role that a targeted computer plays in the offense; and (3) an explanation of the agents' search strategy. In addition, warrants that raise special issues (such as sneak-and-peek warrants, or warrants that may implicate the Privacy Protection Act, 42 U.S.C. § 2000aa) require thorough discussion of those issues in the affidavit. Agents and prosecutors with questions about how to tailor an affidavit and warrant for a computer-related search may contact either their local CTC (see Introduction, p. ix) or the Computer Crime & Intellectual Property Section at (202) 514-1026.

A. Background Technical Information

It may be helpful to include a section near the beginning of the affidavit explaining any technical terms that the affiant may use. Although many judges are computer literate, judges generally appreciate a clear, jargon-free explanation of technical terms that may help them understand the merits of the warrant application. At the same time, agents and prosecutors should resist the urge to pad affidavits with long, boilerplate descriptions of well-known technical phrases. As a rule, affidavits should only include the definitions of terms that are likely to be unknown by a generalist judge and are used in the remainder of the affidavit. Here are some sample definitions:

Addresses

Every device on the Internet has an address that allows other devices to locate and communicate with it. An Internet Protocol (IP) address is a unique number that identifies a device on the Internet. Other addresses include Uniform Resource Locator (URL) addresses, such as "http://www.usdoj.gov," which are typically used to access web sites or other services on remote devices. Domain names, host names, and machine addresses are other types of addresses associated with Internet use.

Cookies

A cookie is a file that is generated by a web site when a user on a remote computer accesses it. The cookie is sent to the user's computer and is placed in a directory on that computer, usually labeled "Internet" or "Temporary Internet Files." The cookie includes information such as user preferences, connection information such as time and date of

use, records of user activity including files accessed or services used, or account information. The cookie is then accessed by the web-site on subsequent visits by the user, in order to better serve the user's needs.

Data Compression

A process of reducing the number of bits required to represent some information, usually to reduce the time or cost of storing or transmitting it. Some methods can be reversed to reconstruct the original data exactly; these are used for faxes, programs and most computer data. Other methods do not exactly reproduce the original data, but this may be acceptable (for example, for a video conference).

Denial of Service Attack (DoS Attack)

A hacker attempting a DoS Attack will often use multiple IP or e-mail addresses to send a particular server or web site hundreds or thousands of messages in a short period of time. The server or web-site will devote system resources to each transmission. Due to the limited resources of servers and web-sites, this bombardment will eventually slow the system down or crash it altogether.

Domain

A domain is a group of Internet devices that are owned or operated by a specific individual, group, or organization. Devices within a domain have IP addresses within a certain range of numbers, and are usually administered according to the same set of rules and procedures.

Domain Name

A domain name identifies a computer or group of computers on the Internet, and corresponds to one or more IP addresses within a particular range. Domain names are typically strings of alphanumeric characters, with each "level" of the domain delimited by a period (e.g., Computer.networklevel1.networklevel2.com). A domain name can provide information about the organization, ISP, and physical location of a particular network user.

Encryption

Encryption refers to the practice of mathematically scrambling computer data as a communications security measure. The encrypted information is called "ciphertext." "Decryption" is the process of converting the ciphertext back into the original, readable information (known as "plaintext"). The word, number or other value used to encrypt/decrypt a message is called the "key."

File Transfer Protocol (FTP)

FTP is a method of communication used to send and receive files such a word-processing documents, spreadsheets, pictures, songs, and video files. FTP sites are online "warehouses" of computer files that are available for copying by users on the Internet. Although many sites require users to supply credentials (such as a password or user name) to gain access, the IP Address of the FTP site is often all that is required to access the site, and users are often identified only by their IP addresses.

Firewall

A firewall is a dedicated computer system or piece of software that monitors the connection between one computer or network and another. The firewall is the gatekeeper that certifies communications, blocks unauthorized or suspect transmissions, and filters content coming into a network. Hackers can sidestep the protections offered by firewalls by acquiring system passwords, "hiding" within authorized IP addresses using specialized software and routines, or placing viruses in seemingly innocuous files such as e-mail attachments.

Hacking

Hacking is the deliberate infiltration or sabotaging of a computer or network of computers. Hackers use loopholes in computer security to gain control of a system, steal passwords and sensitive data, and/or incapacitate a computer or group of computers. Hacking is usually done remotely, by sending harmful commands and programs through the Internet to a target system. When they arrive, these commands and programs instruct the target system to operate outside of the parameters specified by the administrator of the system. This often causes general system instability or the loss of data.

Instant Messaging (IM)

IM is a communications service that allows two users to send messages through the Internet to each other in real-time. Users subscribe to a particular messaging service (e.g., AOL Instant Messenger, MSN Messenger) by supplying personal information and choosing a screen-name to use in connection with the service. When logged in to the IM service, users can search for other users based on the information that other users have supplied, and they can send those users messages or initiate a chat session. Most IM services also allow files to be transferred between users, including music, video files, and computer software. Due to the structure of the Internet, a transmission may be routed through different states and/or countries before it arrives at its final destination, even if the communicating parties are in the same state.

Internet

The Internet is a global network of computers and other electronic devices that communicate with each other via standard telephone lines, high-speed telecommunications links

(e.g., fiber optic cable), and wireless transmissions. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

Internet Relay Chat (IRC)

IRC is a popular Internet service that allows users to communicate with each other in real-time. IRC is organized around the "chat-room" or "channel," in which users congregate to communicate with each other about a specific topic. A "chat-room" typically connects users from different states and countries, and IRC messages often travel across state and national borders before reaching other users. Within a "chat-room" or "channel," every user can see the messages typed by other users.

No user identification is required for IRC, allowing users to log in and participate in IRC communication with virtual anonymity, concealing their identities by using fictitious "screen names."

Internet Service Providers ("ISPs")

Many individuals and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.
ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data format and in written record format. ISPs reserve and/or maintain computer disk storage space on their computer system for the use of the Internet service subscriber for both temporary and long-term storage of electronic communications with other parties and other types of electronic data and files. E-mail that has not been opened is stored temporarily by an ISP incident to the transmission of the e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as "electronic storage," and the provider of such a service is an "electronic communications service" provider. A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is providing a "remote computing service."

IP Address

The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to

the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

> ***dynamic IP address*** *When an ISP or other provider uses dynamic IP addresses, the ISP randomly assigns one of the available IP addresses in the range of IP addresses controlled by the ISP each time a user dials into the ISP to connect to the Internet. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, however, that IP address becomes available to other customers who dial in at a later time. Thus, an individual customer's IP address normally differs each time he dials into the ISP.*
>
> ***static IP address*** *A static IP address is an IP address that is assigned permanently to a given user or computer on a network. A customer of an ISP that assigns static IP addresses will have the same IP address every time.*

Joint Photographic Experts Group (JPEG)

JPEG is the name of a standard for compressing digitized images that can be stored on computers. JPEG is often used to compress photographic images, including pornography. Such files are often identified by the ".jpg" extension (such that a JPEG file might have the title "picture.jpg") but can easily be renamed without the ".jpg" extension.

Log file

Log files are computer files that contain records about system events and status, the activities of users, and anomalous or unauthorized computer usage. Names for various log files include, but are not limited to: user logs, access logs, audit logs, transactional logs, and apache logs.

Moving Pictures Expert Group -3 (MP3)

MP3 is the name of a standard for compressing audio recordings (e.g., songs, albums, concert recordings) so that they can be stored on a computer, transmitted through the Internet to other computers, or listened to using a computer. Despite its small size, an MP3 delivers near CD-quality sound. Such files are often identified by the filename extension ".mp3," but can easily be renamed without the ".mp3" extension.

Packet Sniffing

On the Internet, information is usually transmitted through many different locations before it reaches its final destination. While in transit, such information is contained within "packets." Both authorized users, such as system security experts, and unauthorized users, such as hackers, use specialized technology - packet sniffers - to "listen" to the flow of information on a network for interesting packets, such as those containing logins or

passwords, sensitive or classified data, or harmful communications such as viruses. After locating such data, the packet sniffer can read, copy, redirect, or block the communication.

Peer-to-Peer (P2P) Networks

P2P networks differ from conventional networks in that each computer within the network functions as both a client (using the resources and services of other computers) and a server (providing files and services for use by "peer" computers). There is often no centralized server in such a network. Instead, a search program or database tells users where other computers are located and what files and services they have to offer. Often, P2P networks are used to share and disseminate music, movies, and computer software.

Router

A router is a device on the Internet that facilitates communication. Each Internet router maintains a table that states the next step a communication must take on its path to its proper destination. When a router receives a transmission, it checks the transmission's destination IP address with addresses in its table, and directs the communication to another router or the destination computer. The log file and memory of a router often contain important information that can help reveal the source and network path of communications.

Server

A server is a centralized computer that provides services for other computers connected to it via a network. The other computers attached to a server are sometimes called "clients." In a large company, it is common for individual employees to have client computers at their desktops. When the employees access their e-mail, or access files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network. Notably, server computers can be physically stored in any location: it is common for a network's server to be located hundreds (and even thousands) of miles away from the client computers.
In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."

Tracing

Trace programs are used to determine the path that a communication takes to arrive at its destination. A trace program requires the user to specify a source and destination IP address. The program then launches a message from the source address, and at each "hop" on the network (signifying a device such as a router), the IP address of that device is displayed on the source user's screen or copied to a log file.

User name or User ID

Most services offered on the Internet assign users a name or ID, which is a pseudonym that computer systems use to keep track of users. User names and IDs are typically associated with additional user information or resources, such as a user account protected by a password, personal or financial information about the user, a directory of files, or an e-mail address.

Virus

A virus is a malicious computer program designed by a hacker to (1) incapacitate a target computer system, (2) cause a target system to slow down or become unstable, (3) gain unauthorized access to system files, passwords, and other sensitive data such as financial information, and/or (4) gain control of the target system to use its resources in furtherance of the hacker's agenda.

Once inside the target system, a virus may begin making copies of itself, depleting system memory and causing the system to shut down, or it may begin issuing system commands or altering crucial data within the system.

Other malicious programs used by hackers are, but are not limited to: "worms" that spawn copies that travel over a network to other systems, "trojan horses" that are hidden in seemingly innocuous files such as e-mail attachments and are activated by unassuming authorized users, and "bombs" which are programs designed to bombard a target e-mail server or individual user with messages, overloading the target or otherwise preventing the reception of legitimate communications.

B. Background - Staleness Issue

It may be helpful and necessary to include a paragraph explaining how certain computer files can reside indefinitely in free or slack space and thus be subject to recovery with specific forensic tools:

> *Based on your affiant's knowledge, training, and experience, your affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a*

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

C. Describe the Role of the Computer in the Offense

The next step is to describe the role of the computer in the offense, to the extent it is known. For example, is the computer hardware itself evidence of a crime or contraband? Is the computer hardware merely a storage device that may or may not contain electronic files that constitute evidence of a crime? To introduce this topic, it may be helpful to explain at the outset why the role of the computer is important for defining the scope of your warrant request.

Your affiant knows that computer hardware, software, and electronic files may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of crime, contraband, instrumentalities of crime, and/or fruits of crime. In this case, the warrant application requests permission to search and seize [images of child pornography, including those that may be stored on a computer]. These [images] constitute both evidence of crime and contraband. This affidavit also requests permission to seize the computer hardware that may contain [the images of child pornography] if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. Your affiant believes that, in this case, the computer hardware is a container for evidence, a container for contraband, and also itself an instrumentality of the crime under investigation.

1. When the Computer Hardware Is Itself Contraband, Evidence, And/or an Instrumentality or Fruit of Crime

If applicable, the affidavit should explain why probable cause exists to believe that the tangible computer items are themselves contraband, evidence, instrumentalities, or fruits of the crime, independent of the information they may hold.

Computer Used to Obtain Unauthorized Access to a Computer ("Hacking")

Your affiant knows that when an individual uses a computer to obtain unauthorized access to a victim computer over the Internet, the individual's computer will

generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is "used as a means of committing [the] criminal offense" according to Rule 41(b)(3). In particular, the individual's computer is the primary means for accessing the Internet, communicating with the victim computer, and ultimately obtaining the unauthorized access that is prohibited by 18 U.S.C. § 1030. The computer is also likely to be a storage device for evidence of crime because computer hackers generally maintain records and evidence relating to their crimes on their computers. Those records and evidence may include files that recorded the unauthorized access, stolen passwords and other information downloaded from the victim computer, the individual's notes as to how the access was achieved, records of Internet chat discussions about the crime, and other records that indicate the scope of the individual's unauthorized access.

Computers Used to Produce Child Pornography

It is common for child pornographers to use personal computers to produce both still and moving images. For example, a computer can be connected to avideo camera, VCR, or DVD-player, using a device called a video capture board: the device turns the video output into a form that is usable by computer programs. Alternatively, the pornographer can use a digital camera to take photographs or videos and load them directly onto the computer. The output of the camera can be stored, transferred or printed out directly from the computer. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. All of these devices, as well as the computer, constitute instrumentalities of the crime.

2. When the Computer Is Merely a Storage Device for Contraband, Evidence, And/or an Instrumentality or Fruit of Crime

When the computer is merely a storage device for electronic evidence, the affidavit should explain this clearly. The affidavit should explain why there is probable cause to believe that evidence of a crime may be found in the location to be searched. This does not require the affidavit to establish probable cause that the evidence may be stored specifically within a computer. However, the affidavit should explain why the agents believe that the information may in fact be stored as an electronic file stored in a computer.

Child Pornography

Your affiant knows that child pornographers generally prefer to store images of child pornography in electronic form as computer files. The computer's ability to store images in digital form makes a computer an ideal repository for pornography. A small portable disk can contain hundreds or thousands of images of child pornography, and a computer hard drive can contain tens of thousands of such images at very high resolution. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child por-

nography and the disks that contain the files can be mislabeled or hidden to evade detection.

Illegal Business Operations

Based on actual inspection of [spreadsheets, financial records, invoices], your affiant is aware that computer equipment was used to generate, store, and print documents used in [suspect's] [tax evasion, money laundering, drug trafficking, etc.] scheme. There is reason to believe that the computer system currently located on [suspect's] premises is the same system used to produce and store the [spreadsheets, financial records, invoices], and that both the [spreadsheets, financial records, invoices] and other records relating to [suspect's] criminal enterprise will be stored on [suspect's computer].

D. The Search Strategy

The affidavit should also contain a careful explanation of the agents' search strategy, as well as a discussion of any practical or legal concerns that govern how the search will be executed. Such an explanation is particularly important when practical considerations may require that agents seize computer hardware and search it off-site when that hardware is only a storage device for evidence of crime. Similarly, searches for computer evidence in sensitive environments (such as functioning businesses) may require that the agents adopt an incremental approach designed to minimize the intrusiveness of the search. The affidavit should explain the agents' approach in sufficient detail that the explanation provides a useful guide for the search team and any reviewing court. It is a good practice to include a copy of the search strategy as an attachment to the warrant, especially when the affidavit is placed under seal. Here is sample language that can apply recurring situations:

1. Sample Language to Justify Seizing Hardware and Conducting a Subsequent Off-site Search

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

> *(1) The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions 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 and invasive to attempt this kind of data search on-site.*
>
> *(2) Technical Requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is 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 may be necessary to complete an accurate analysis. Further, such searches often require the seizure of 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.*

In light of these concerns, your affiant hereby requests the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.

2. Sample Language to Justify an Incremental Search

Your affiant recognizes that the [Suspect] Corporation is a functioning company with approximately [number] employees, and that a seizure of the [Suspect] Corporation's computer network may have the unintended and undesired effect of limiting the company's ability to provide service to its legitimate customers who are not engaged in [the criminal activity under investigation]. In response to these concerns, the agents who execute the search will take an incremental approach to minimize the inconvenience to [Suspect Corporation]'s legitimate customers and to minimize the need to seize equipment and data. This incremental approach, which will be explained to all of the agents on the search team before the search is executed, will proceed as follows:

> *A. Upon arriving at the [Suspect Corporation's] headquarters on the morning of the search, the agents will attempt to identify a system administrator of the network (or other knowledgeable employee) who will be willing to assist law enforcement by identifying, copying, and printing out*

paper [and electronic] copies of [the computer files described in the warrant.] If the agents succeed at locating such an employee and are able to obtain copies of the [the computer files described in the warrant] in that way, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.

B. If the employees choose not to assist the agents and the agents cannot execute the warrant successfully without themselves examining the [Suspect Corporation's] computers, primary responsibility for the search will transfer from the case agent to a designated computer expert. The computer expert will attempt to locate [the computer files described in the warrant], and will attempt to make electronic copies of those files. This analysis will focus on particular programs, directories, and files that are most likely to contain the evidence and information of the violations under investigation. The computer expert will make every effort to review and copy only those programs, directories, files, and materials that are evidence of the offenses described herein, and provide only those items to the case agent. If the computer expert succeeds at locating [the computer files described in the warrant] in that way, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.

C. If the computer expert is not able to locate the files on-site, or an on-site search proves infeasible for technical reasons, the computer expert will attempt to create an electronic "image" of those parts of the computer that are likely to store [the computer files described in the warrant]. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Imaging a computer permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer hardware. The computer expert or another technical expert will then conduct an off-site search for [the computer files described in the warrant] from the "mirror image" copy at a later date. If the computer expert successfully images the [Suspect Corporation's] computers, the agents will not conduct any additional search or seizure of the [Suspect Corporation's] computers.

D. If "imaging" proves impractical, or even impossible for technical reasons, then the agents will seize those components of the [Suspect Corporation's] computer system that the computer expert believes must be seized to permit the agents to locate [the computer files described in the warrant] at an off-site location. The components will be seized and taken in to the custody of the FBI. If employees of [Suspect Corporation] so request, the computer expert will, to the extent practicable, attempt to provide the employees with copies of any files [not within the scope of the warrant] that may be necessary or important to the continuing function of the [Suspect Corporation's] legitimate business. If, after inspecting the computers, the analyst determines that some or all of this equipment is no longer neces-

sary to retrieve and preserve the evidence, the government will return it within a reasonable time.

3. Sample Language to Justify the Use of Comprehensive Data Analysis Techniques

Searching [the suspect's] computer system for the evidence described in [Attachment A] may require a range of data analysis techniques. In some cases, it is possible for agents to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, agents may be able to execute a "keyword" search that searches through the files stored in a computer for special words that are likely to appear only in the materials covered by a warrant. Similarly, agents may be able to locate the materials covered in the warrant by looking for particular directory or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for information. These steps may require agents to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in [Attachment A].

E. Special Considerations

The affidavit should also contain discussions of any special legal considerations that may factor into the search or how it will be conducted. These considerations are discussed at length in Chapter 2. Agents can use this checklist to determine whether a particular computer-related search raises such issues:

1. Is the search likely to result in the seizure of any drafts of publications (such as books, newsletters, Web site postings, etc.) that are unrelated to the search and are stored on the target computer? If so, the search may implicate the Privacy Protection Act, 42 U.S.C. § 2000aa.

2. Is the target of the search an ISP, or will the search result in the seizure of a mail server? If so, the search may implicate the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-12.

3. Does the target store electronic files or e-mail on a server maintained in a remote location? If so, the agents may need to obtain more than one warrant.

4. Will the search result in the seizure of privileged files, such as attorney-client communications? If so, special precautions may be in order.

5. Are the agents requesting authority to execute a "sneak-and-peek" search? If so, the proposed search must satisfy the standard defined in 18 U.S.C. § 3103a(b).

6. Are the agents requesting authority to dispense with the "knock and announce" rule?

COMPUTER SEARCHES AND SEIZURES: SOME UNRESOLVED ISSUES

*Susan W. Brenner**
*Barbara A. Frederiksen***

Cite as: Susan W. Brenner and Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. TECH. L. REV. 39 (2002)
available at http://www.mttlr.org/voleight/Brenner.pdf

INTRODUCTION 40
I. A HYPOTHETICAL 43
II. OFF-SITE VERSUS ON-SITE COMPUTER SEARCHES.....44
A. *Off-Site Document Searches* 45
B. *Off-Site Computer Searches*.....46
1. Department of Justice Guidelines.....47
2. 1994 Guidelines.....49
3. 2001 Revised Guidelines.....50
C. *When are Off-Site Computer Searches Reasonable?*.....56
D. *Off-Site Document Search*.....56
E. *Off-Site Computer Search* 58
F. *Off-Site Document Search Rationale Inapplicable to Off-Site Computer Searches*.....60
G. *Automated Search Techniques*.....60
H. *Technical Considerations*.....62
I. *Back-Up Copies Made on-Site for Off-Site Search*.....63
J. *Spoliation—Inadvertent*.....65
K. *Spoliation—Advertent*.....67
L. *General Affidavit Language not Sufficient*.....70

* Professor of Law, University of Dayton School of Law. Professor Brenner writes and speaks on cybercrimes. She has spoken at Interpol's Fourth Annual Conference on Cybercrimes in Lyon, France, the National District Attorneys Association's 2001 National Conference and the Hoover Institution's Conference on International Cooperation to Combat Cyber Crime and Terrorism, held at Stanford University. She serves on the American Bar Association's Privacy and Computer Crime Committee, serves on the National District Attorneys Association's Cybercrimes Committee and co-chair of the National Institute of Justice—Electronic Crime Partnership Initiative's Working Group on Policy. She is also the creator of a website dealing with cybercrimes. *See* http://www.cybercrimes.net (last visited Feb. 14, 2002).

** Forensic Software Analyst and Senior Managing Consultant with Johnson-Laird Inc. *See* http://www.jli.com (last visited Mar. 16, 2002). The authors gratefully acknowledge the assistance provided by Josh Muennich, a third-year student at the University of Dayton School of Law. Mr. Muennich, who drafted the sections of the Model Code of Cybercrime Investigative Procedure dealing with off-site searches, reviewed the manuscript and made valuable suggestions and Jef Henninger, University of Dayton School of Law Class of 2004, for reading the manuscript and offering helpful suggestions.

M. *On-Site Search May be Reasonable* 71
N. *On-Site Copy with Off-Site Review* 73
O. *Off-Site Searches: A Proposal* 75
III. THE PLAIN VIEW DOCTRINE AND COMPUTER SEARCHES 89
IV. IS COPYING DATA A SEARCH? A SEIZURE? 106
CONCLUSION 113

INTRODUCTION

> [I]n the application of a constitution, . . . our contemplation cannot be only of what has been but of what may be. . . .
>
> . . . .
>
> . . . Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[1]

Society has come a long way toward realizing the scenario Justice Brandeis hypothesized in the dissent in *Olmstead* , especially with regard to computer-generated "papers." As society moves into the cyberworld,[2] the novel, distinctive characteristics of electronic information are generating a host of questions as to how traditional Fourth Amendment jurisprudence is, and should be, transposed to this new environment.

The rise of the cyberworld has given us cybercrime, a new variety of unlawful behavior in which computers are used in committing crimes.[3] Evidence-gathering by law enforcement officers investigating cybercrime cases can implicate any of several legal standards, including the Fourth Amendment prohibition on unreasonable searches and seizures,[4]

1. Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting).

2. The "cyberworld" is the experience of cyberspace as a distinct reality, a virtual reality. *See* MARGARET WERTHEIM, THE PEARLY GATES OF CYBERSPACE: A HISTORY OF SPACE FROM DANTE TO THE INTERNET 223–252 (1999); John Suler, *Cyberspace as Psychological Space*, at http://www.rider.edu/users/suler/psycyber/psychspace.html (last visited Feb. 11, 2002).

3. *See* Susan W. Brenner, *Is There Such a Thing as "Virtual Crime"?*, 4 CAL. CRIM. L. REV. (2001) at http://www.boalt.org/CCLR/v4/v4brenner.htm (last visited Mar. 16, 2002); Marc D. Goodman, *Why the Police Don't Care About Computer Crime*, 10 HARV. J. L. & TECH. 465 (1997).

4. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, . . .").

the Fifth Amendment privilege against self-incrimination[5] and statutory guarantees such as those created by the Electronic Communications Privacy Act.[6] Statutory guarantees like the Electronic Communications Privacy Act were deliberately crafted to deal with technological issues, but constitutional guarantees evolved in a world in which technology was essentially unknown.[7] It can, therefore, be difficult to translate constitutional guarantees into a technical environment.

The Fourth Amendment is the most troubling provision because applying its guarantees to computer searches and seizures requires extrapolating concepts that were devised to deal with the "real" physical world to the cyberworld.[8] The Fourth Amendment guarantees citizens the right to be free from "unreasonable searches and seizures".[9] A "search" or a "seizure" is reasonable if it meets certain requirements. Officers may conduct a search and/or seizure pursuant to a search warrant that is

5. U.S. CONST. amend. V ("No person . . . shall be compelled in any criminal case to be a witness against himself, . . .").

6. The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 1367, 2521, 2701–2709, 2711, 3117, 3121–3127 (1994).

7. When the Fourth and Fifth Amendments were adopted, 'the form that evil had theretofore taken,' had been necessarily simple. Force and violence were then the only means known to man by which a Government could directly effect self-incrimination. It could compel the individual to testify—a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life—a seizure effected, if need be, by breaking and entry. . . . But 'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting).

8.

> [T]he seizure of a computer raises many issues beyond those that might pertain to mere writings.
>
> For example, seizing a computer may intrude into the privacy interests of individuals other than the intended subjects due to e-mail transmissions to and from a particular computer. Similarly, when a networked computer is subject to a search, it may be possible to examine interactions with computers that are networked to the one being searched. Moreover, the use of a computer to access the internet also raises issues regarding a potential search of that computer, as the hard drive stores information about the internet sites that have been visited by the user. Therefore, the search of a computer could implicate the privacy concerns of many people who did not use a specific computer physically, but in fact used such computer electronically. Furthermore, the seizure of a networked computer may disrupt all or part of a network and interfere with many other users.

People v. Gall, 30 P.3d 145, 162–63 (Colo. 2001) (Martinez, J., dissenting).

9. U.S. CONST. amend. IV.

based on probable cause.[10] The warrant must be issued by a neutral and detached Magistrate Judge and certain other requirements.[11] The officers' conduct will be "reasonable," not in violation of the Fourth Amendment, as long as they stay within the scope of that warrant, or, in other words, as long as their actions are calculated to locate evidence for which the warrant authorizes them to search and seize.[12] There are also a number of exceptions to the warrant requirement; if officers carry out a search and/or seizure pursuant to one of these exceptions, their conduct will be deemed to be reasonable even though they acted without a warrant.[13] If officers carry out a search or seizure that is not authorized by a warrant or by an exception to the warrant requirement, their conduct will be deemed unreasonable, and in violation of the Fourth Amendment.[14]

The parameters used to implement Fourth Amendment guarantees in the context of real world searches and seizures are well-established. The cyberworld lacks the real world's unambiguous physical boundaries, therefore it is often difficult to translate these guarantees into the context of computer searches where simply determining when a "search" or "seizure" occurs can be a complicated endeavor, as can differentiating a "search" from a "seizure."[15]

The areas of Fourth Amendment difficulty are myriad and seem to increase almost every day, so a comprehensive treatment of these issues is outside the scope of this article. The goal of this article is to illustrate the issues that arise in the context of computer search and seizures by examining several areas in which the application of Fourth Amendment concepts to computer searches and/or seizures can be problematic. In order to illustrate this point, the article will build on a hypothetical. The hypothetical situation assumes law enforcement officers have lawfully

10. *See* 2 WAYNE R. LAFAVE, CRIMINAL PROCEDURE § 3.4(d) (2d ed. 1999); *Cf.* State v. Staley, 548 S.E.2d 26 (Ga. App. 2001) (granting motion to suppress evidence because warrant issued to search defendant's computer for evidence of child pornography was not based on probable cause).

11. *See* LaFave, *supra* note 10, at § 3.4.

12. *See* U.S. v. Heldt, 668 F.2d 1239, 1256–60 (D.C. Cir. 1981); LaFave, *supra* note 10, at § 3.4(j).

13. LaFave, *supra* note 10, at §§ 3.2, 3.3.

14. *See* U.S. v. Richards, 638 F.2d 765 (5th Cir. 1981); *See generally* LaFave, *supra* note 10, at § 3.4.

15. *See* MODEL CODE OF CYBERCRIME INVESTIGATIVE PROCEDURE, art. I § 5(a)–(b) (1998) *at* http://www.cybercrimes.net/MCCIP/art1.htm [hereinafter "MCCIP"] (last visited Feb. 11, 2002) (defining the terms search and seizure separately). The MCCIP is a model rule governing what law enforcement officers can and cannot do when they are investigating cybercrimes. The code addresses issues such as the constraints the Fourth Amendment places on officers when they are searching and seizing computers, the legal rules that govern the use of subpoenas to obtain evidence about someone's Internet Service Provider accounts and gaining access to encrypted files.

obtained a warrant to search for and seize evidence concerning the commission of one or more crimes. It will also be assumed that computer technology played some role in the commission of these crimes, so computer equipment and computer data are legitimate objects of the search. This hypothetical is used to explore three issues, each of which concerns the execution of a computer search and seizure warrant:

> Under what circumstances is it reasonable to conduct a search of computers and/or computer files off-site, as opposed to on-site?
>
> What, if any, role should the plain view doctrine play in computer searches and seizures?
>
> Is copying data contained on a hard drive or in some other electronic storage media[16] a search? A seizure?

I. A HYPOTHETICAL[17]

Federal agents spent several years investigating the possible commission of insurance fraud involving the submission of false and/or inflated claims for reimbursement of medical expenses. The agents came to believe that attorneys and employees working for the law firm of Doe & Doe were centrally involved in the commission of the fraud, and concluded that a search of the law firm's files was needed for evidence of that involvement.

To that end, agents obtained a warrant authorizing them to search the office of Doe & Doe and to seize specified "computer hardware, software, and peripherals" at that office. The warrant was based on probable cause, was issued by a "neutral and detached" Magistrate Judge, and in every other way satisfied the requirements of the Fourth Amendment. In addition to authorizing the seizure of computer hardware, software and peripherals, the warrant authorized the investigators to search the seized computer system for data concerning individuals who were targets of the investigation, medical appointment logs, accounting records and other evidence itemized in a schedule

16. Storage and computer media denotes devices used to store computer data, which include floppy disks, hard disks, CD-ROM's, DVD's, ZIP drives, and magnetic tapes. *See* Michael Chappell, Computer Forensics and Litigation Support, *at* http://www.sinch.com.au/articles/2000/computer_forensics.htm (last visited Jan. 31, 2002).

17. Hypothetical is based on the facts found in two related cases. *See* Commonwealth v. Ellis, No. 97-192, 1999 WL 815818 (Mass. Super. Aug. 27, 1999) (ruling on a motion to suppress electronically stored evidence); Commonwealth v. Ellis, No. 97-192, 1999 WL 823741 (Mass. Super. Aug. 18, 1999) (ruling on a motion to suppress evidence).

attached to the warrant application. The warrant required the agents executing the search to make a back-up copy of the information contained in the seized computer hardware, "as soon as reasonably practicable." The judge issuing the warrant ordered that the back-up be sufficient to give Doe & Doe a copy of all the information stored on its seized computer equipment. The warrant also ordered the investigators to make a mirror image[18] of the computer system using the system's own peripherals. The mirror image was to capture all the data on the system to the extent possible, including data purged or deleted from the system. It was also to be used to identify all users who had access to particular data on the system.

The agents charged with executing the warrant entered the Doe & Doe office early one morning, and began by disabling the office's network server. They seized the server and related equipment. The agents then went to each stand-alone computer with independent storage capacity and ran a "key-word" search of its hard drive, using a program called DiskSearch II.[19] If the search produced any key-word "hits," they seized the computer. The agents ultimately seized twenty-two computers, all but four of Doe & Doe's computers. The agents executing the warrant also seized thirteen computer back-up tapes and a printer. The printer was seized to facilitate their off-site searching of the seized computers.

The agents moved the seized computers and computer equipment to an off-site location, where the server and computer were reassembled. Two back-up copies of the data contained on the system were not made until four days after the initial search. One of these copies was then returned to Doe & Doe. The search of the system was not completed for almost two years.

II. OFF-SITE VERSUS ON-SITE COMPUTER SEARCHES

Officers executing an authorized Fourth Amendment intrusion have traditionally searched for and then seized evidence (if, indeed, any was

18. Mirror image backups (also referred to as bit stream backups) involve the backup of all areas of a computer hard disk drive or another type of storage media, e.g., Zip disks, floppy disks, Jazz disks, etc. Such mirror image backups exactly replicate all sectors on a given storage device. Thus, all files and ambient data storage areas are copied. Such backups are sometimes referred to as "evidence grade" backups and they differ substantially from standard file backups and network server backups.

New Technologies, Inc., *Mirror Image Backup—Defined*, *at* http://www.forensics-intl.com/def2.html (last visited Nov. 9, 2001).

19. *See* New Technologies, Inc., *DiskSearch 32*, *at* http://www.forensics-intl.com/dssuite.html (last visited Nov. 27, 2001) (providing the most current version of the software used in the hypothetical).

to be found), rather than the reverse. Indeed, this essential, but generally unarticulated, Fourth Amendment practice is implicitly recognized when referring to search and seizure warrants.[20]

A. *Off-Site Document Searches*

Toward the end of the last century, the practicability of this assumption came into question with regard to certain kinds of Fourth Amendment intrusions. A doctrine was established under which the traditional sequence was reversed, evidence was seized and then searched. This doctrine emerged in the context of "document" searches, cases in which officers executed search warrants requiring them to search through large volumes of paper records and seize specified documents.[21] Instead of searching through the documents on-site and only seizing those documents which fell within the scope of the warrant, officers began seizing all of the documents and removing them to an off-site location where they searched the entire body of documents, seized those that were within the scope of the warrant and then returned the others.[22]

Often, those whose documents were seized challenged the officers' actions, claiming they were not "reasonable" under the Fourth Amendment.[23] Since the officers acted pursuant to a lawfully-issued warrant, the challengers did not claim that the officers' conduct was unreasonable from the outset; instead, they argued that the officers acted unreasonably in the way they executed the warrant.[24] Specifically, the challengers alleged that it was not reasonable for the officers to seize a large volume of documents and take them away for an off-site search. They pointed out, among other things, that in doing so the officers exceeded the scope of the warrant by seizing both relevant and irrelevant documents, e.g., documents which fell within the scope of the search and

20. *See, e.g.*, Wilson v. State, 752 A.2d 1250 (Md. Ct. Spec. App. 2000) (upholding the seizing of defendant's blood followed by a "search" of the blood).

21. *See* United States v. Wuagneux, 683 F.2d 1343, (11th Cir. 1982); United States v. Beusch, 596 F.2d 871 (9th Cir. 1979).

22. *See* United States v. Hargus, 128 F.3d 1358, 1363–1364 (10th Cir. 1997) (holding officers did not "grossly exceed" a search warrant by removing two filing cabinets from defendant's residence because "on-site sorting would be impractical and un-duly time consuming."); *Wuagneux*, 683 F.2d at 1352–1353; *Beusch*, 596 F.2d at 876–877. *See also* FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS § II(C) Step 3 at 47–48 (2001) *available at* http://www.cybercrime.gov/searchmanual.pdf [hereinafter GUIDELINES] (last visited Mar. 16, 2002) (suggesting that when obtaining a warrant the party should alert the court to the possibility of an off-site search).

23. *See Hargus*, 128 F.3d at 1363–1364; *Wuagneux*, 683 F.2d at 1352–1353; *Beusch*, 596 F.2d at 876–877.

24. *See id*.

seizure warrant and those that did not.[25] Courts consistently upheld this practice as "reasonable" under the Fourth Amendment relying, in part, on the premise that having officers search through the entire volume of documents on site is more intrusive than having them do so off-site.[26] One factor often cited in upholding this practice is that clearly incriminating documents are so often intermingled with other non incriminating documents that it simply is not reasonable to require officers to sort the documents on-site.[27]

The application of the off-site document search doctrine is not limited to searches conducted on business property, it also applies to the home. Several decisions apply the doctrine to searches conducted at a person's home, on the premise that it would be even more intrusive to have officers conduct a lengthy sorting and searching process at a home than at a business.[28]

B. *Off-Site Computer Searches*

Warrants that require officers to search for and seize computer generated evidence can also create a large volume of evidence. The various elements of which are often intermingled with each other. For example, a keyword search may identify many files and file fragments which contain the responsive phrase, but depending on the nature of the investigation, not all of these will be relevant or discoverable. The same

---

25. *See id*.

26.

> The search here was limited to Santarelli's upstairs bedroom and an adjoining hallway. . . . Given the fact that the search warrant entitled the agents to search for documents, . . . it is clear that the agents were entitled to examine each document in the bedroom or in the filing cabinet to determine whether it constituted evidence they were entitled to seize under the warrant. . . . It follows that Santarelli would have no cause to object if the agents had entered his home to examine the documents and remained there as long as the search required. The district court estimated that a brief examination of each document would have taken several days. Under these circumstances, we believe that the agents acted reasonably when they removed the documents to another location for subsequent examination. Given that the officers were entitled to examine the documents while they remained in the home, we cannot see how Santarelli's privacy interest was adversely affected by the agents' examination of the documents off the premises, so long as any items found not to be relevant were promptly returned. . . . We find, therefore, that the search of Santarelli's residence was reasonable.

United States v. Santarelli, 778 F.2d 609, 615–616 (11th Cir. 1985) (citations omitted); *See Wuagneux*, 683 F.2d at 1352–1353; *Beusch*, 596 F.2d at 876–877. *See also* GUIDELINES § II(C) Step 3 at 47–48.

27. *See* United States v. Wapnick, No. CR-92-419, 1993 WL 86480 (E.D.N.Y. Mar. 16, 1993); *Wuagneux*, 683 F.2d at 1353. *See also* GUIDELINES § II(C) Step 3 at 47–48.

28. *Santarelli*, 778 F.2d at 615–616; *Wapnick* 1993 WL 86480 at *6–7.

search term may yield results that identify text contained in relevant documents and text in documents which are not relevant to the crime under investigation or contain correspondence between the suspect and their attorney. The search results may also include text that is found in deleted files or e-mails. The terms of the search warrant will dictate whether text located in deleted files can be used as evidence. It is therefore not surprising that officers began to deal with these computer "document" in the same way they had become accustomed to dealing with paper documents. The officers seize the containers in which the computer records are stored and take the records off-site[29], to be searched and sorted.[30]

1. Department of Justice Guidelines

In 1994, the Department of Justice issued the *Federal Guidelines for Searching and Seizing Computers* [hereinafter "*Guidelines*"], the purpose of which was to try to "illustrate some of the ways in which searching a computer is different from searching a desk, a file cabinet, or an automobile."[31] The authors of the *Guidelines* explained that they had attempted to translate traditional search and seizure principles into the context of computer searches, noting that they "often had to extrapolate

29. For the purposes of this article, "off-site" computer searches consist of the "removal and transportation of electronic evidence to a location not on the premises and location where the electronic evidence is found or in the location of the area to be searched described in the warrant." MCCIP art. VII § 4(f)(I)(A)(iii). An "on-site" search is a search conducted "on the premises and location where the electronic evidence is found or in the location of the area to be searched described in the warrant"; in an on-site search, the computers, files or related equipment "may be relocated to a place other than its original location in those premises" for the purpose of conducting the search. MCCIP art. VII § 4(f)(I)(A)(ii). "Electronic evidence" is "any computer hardware, computer software, computer generated or derived data, data storage device, data storage media, or computer peripheral device." MCCIP art. VII § 4(f)(I)(A)(i).

30.

> Rather than attempting to "search" the computers at the scene, the officers merely seized the computers and sought further search warrants to inspect their contents. For various policy reasons, the removal of a sealed container . . . is not only authorized but preferred in limited circumstances, including where "the sorting out of the described items from the intermingled undescribed items would take so long that it is less intrusive merely to take that entire group of items to another location and do the sorting there."

People v. Gall, 30 P.3d 145, 154 (Colo. 2001). *See* United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) ("The record shows that the mechanics of the search for images later performed off site could not readily have been done on the spot."); Commonwealth v. Ellis, No. 97-192, 1999 WL 815818 (Mass. Super. Aug. 27, 1999); United States v. Hunter, 13 F. Supp. 2d 574, 583–584 (D.Vt. 1998); United States v. Gurs, No. 93-30261, 1996 WL 200998, **3 (9th Cir. Apr. 25, 1996).

31. *See* FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 56 Crim. L. Rep. (BNA) Introduction at 2025(1994).

from existing law or policies to try to strike old balances in new areas."[32] As to their authoritativeness, the *Preface* to the *Guidelines* explains that, while the *Guidelines* are drafted by an interagency working group:[33]

> [t]hese *Guidelines* have not been officially adopted by any of the agencies, and are intended only as assistance, not as authority. They have no regulatory effect, and confer no right or remedy on anyone. Moreover, the facts of any particular case may require you to deviate from the methods we generally recommend, or may even demand that you try a completely new approach.[34]

This caveat notwithstanding, the *Guidelines* became an influential, often-cited source of information on how computer searches and seizures should be conducted.[35]

Because of changes in technology, the *Guidelines* were updated by Supplements issued in 1997 and 1999 and a revision was issued early in 2001.[36] The 2001 revision supersedes the 1994 *Guidelines*, as well as the 1997 and 1999 Supplements to the 1994 *Guidelines*.[37] Like the 1994 *Guidelines*, the 2001 revision is not represented as binding authority.[38] But like the 1994 *Guidelines*, the 2001 revision will certainly influence how computer searches and seizures are conducted. It is therefore necessary, when examining any issue involving a search or seizure of

---

32. *Id.*

33. *Id.*, Preface at 2023 (participating agencies included "the Federal Bureau of Investigation; the United States Secret Service; the Internal Revenue Service; the Drug Enforcement Administration; the United States Customs Service; the Bureau of Alcohol, Tobacco, and Firearms; the United States Air Force; the Department of Justice; and United States Attorneys' offices").

34. *Id.*

35. *See* Alex White & Scott Charney, *Search and Seizure of Computers: Key Legal and Practical Issues*, *at* http://www.securitymanagement.com/library/000177.html (last visited Feb. 16, 2002) (stating the 1994 GUIDELINES provided "a comprehensive treatment of the major legal issues likely to be encountered in connection with searches involving computers, and provides policy and practical guidance for Federal law enforcement officials who are involved with such searches").

36. *See* FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS Preface at 1 (2001) *available at* http://www.cybercrime.gov/searchmanual.pdf.

37. *Id.*

38.

> This manual is designed to combine an updated version of the Guidelines' advice on searching and seizing computers with guidance on the statutes that govern obtaining electronic evidence in cases involving computer networks and the Internet. Of course, this manual is intended to offer assistance, not authority. Its analysis and conclusions reflect current thinking on difficult areas of law, and do not represent the official position of the Department of Justice or any other agency. It has no regulatory effect, and confers no rights or remedies.

Id.

computers executed by federal agents, to consider the extent to which the positions articulated in the *Guidelines* correctly extrapolate Fourth Amendment principles of reasonableness into this context.

In terms of off-site computer searches, both versions of the *Guidelines* adopt the rationale used to justify off-site document searches. The respective *Guidelines* authors identify as "document" and "computer document" searches as analogous while specifying the factor unique to computer searches.[39] The sections below compare the treatment of off-site computer searches received in the original 1994 version of the *Guidelines* with the treatment this issue receives in the2001 version. The discussion examines both versions of the *Guidelines* for two reasons: the 1994 *Guidelines* influenced the case law that developed in this area from 1994 until 2000, and, as discussion below illustrates, serve as the foundation of the revised 2001 *Guidelines*.

2. 1994 Guidelines

The 1994 version of the *Guidelines* stated that off-site computer searches are justifiable when the following factors are considered:

(1) A large volume of evidence must be searched, either because the warrant authorized the seizure of a voluminous amount of documents or because the documents that fall within the scope of the warrant are intermingled with an "enormous" number of other documents.

(2) The warrant is executed in a home, rather than in a business.

(3) The evidence consists of intermingled files.

(4) It is necessary to conduct a controlled, off-site search to avoid destroying data.

(5) It is necessary to seize hardware and related documentation to conduct an off-site search on seized evidence.[40]

The 1994 *Guidelines* acknowledged that factors (1), (2) and (3) simply apply the off-site document search doctrine to computer searches.[41] They also suggested that computer searches involve an additional

39. FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 56 Crim. L. Rep. (BNA) § IV(H) at 2038 (1994); FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS § II(C) Step 3 at 49 (2001) *available at* http://www.cybercrime.gov/searchmanual.pdf.

40. *See* FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 56 Crim. L. Rep. (BNA) § IV(H) at 2038 (1994).

41. *Id.* ("This [document search] rationale has been extended to computers.").

element which makes off-site searching even more necessary: the difficulty of locating and identifying the evidence sought.

> [T]he file-cabinet cases . . . implicitly rely on the premise that "documents" are readily accessible and ascertainable items; that any agent can find them and (unless the subject is quite technical) can read, sort, and copy those covered by warrant. The biggest problem in the paper cases is time, the days it takes to do a painstaking job. But computer searches have added a formidable new barrier, because searching and seizing are no longer as simple as opening a file cabinet drawer. When agents seize data from computer storage devices, they will need technical skill just to get the file drawer open. While some agents will be "computer literate," only a few will be expert; and none can be expert on every sort of system.[42]

Continuing this theme, factors (4) and (5) are based on what the 1994 *Guidelines* characterized as unique concerns that can arise when agents are searching for computer-generated evidence. Factor (4) is based on two of these concerns: (a) the possibility that agents unfamiliar with a system's hardware and/or software will damage or destroy evidence while attempting to recover it; and (b) the possibility that a computer system may include a "booby-trap" which, when triggered by an unwary agent, destroys the evidence it contains.[43] Factor (5) does not itself justify a seizure of computer equipment. The factor is a supplemental rule that expands the scope of a seizure when agents have an independent rationale for taking computer hardware to a laboratory for analysis.[44] Factor (5) is based on the premise that if agents are justified in seizing part of a computer system, they should be allowed to seize all of the hardware that makes up that system plus any related documentation; otherwise, it may not be possible to reconstruct the system and operate it at the laboratory.[45]

3. 2001 Revised Guidelines

The 2001 revision of the *Guidelines* takes a slightly different approach to off-site searches. It begins by pointing out that there are basic four possible ways to execute computer searches:

Search the computer and print out a hard copy of particular files at that time;

42. *Id.* at § IV(H)(1)(d).
43. *Id.* at § IV(H)(2)(a).
44. *Id.* at § IV(H)(2)(b).
45. *Id.*

Search the computer and make an electronic copy of particular files at that time;

Create a mirror-image electronic copy of the entire storage device on-site, and then later recreate a working copy of the storage device off-site for review; and

Seize the equipment, remove it from the premises, and review its contents off-site.[46]

As to the third option, the 2001 *Guidelines* note that making a mirror-image copy of

> an entire drive . . . is different from making an electronic copy of individual files. When a computer file is saved to a storage disk, it is saved in randomly scattered sectors on the disk rather than in contiguous, consolidated blocks; when the file is retrieved, the scattered pieces are reassembled from the disk in the computer's memory and presented as a single file. Imaging the disk copies the entire disk exactly as it is, including all the scattered pieces of various files. The image allows a computer technician to recreate (or "mount") the entire storage disk and have an exact copy just like the original. In contrast, an electronic copy (also known as a "logical file copy") merely creates a copy of an individual file by reassembling and then copying the scattered sectors of data associated with the particular file.[47]

Three of the possibilities outlined above involve on-site searches; only the fourth requires that hardware and files be seized and taken off-site to be searched. The 2001 *Guidelines* explain that while many factors will determine which of these options is used for any particular search, the "single most important consideration is the role of the computer hardware in the offense."[48] This consideration gives rise to the default position set out in the 2001 *Guidelines*, namely, that if computer hardware "is itself evidence, an instrumentality, contraband, or a fruit of crime, agents will usually plan to seize the hardware and search its contents off-site," but if computer hardware "is merely a storage device for evidence, agents generally will only seize the hardware if less disruptive alternatives are not feasible."[49] According to the *Guidelines*, this default position arises from Rule 41 of the Federal Rules of Criminal Procedure, which lets agents seize computer hardware when that hardware is *itself*

46. FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS § II(B)(1) at 31 (2001) (footnote omitted) *available at* http://www.cybercrime.gov/searchmanual.pdf.

47. *Id.* at n. 5.

48. *Id.* at § II(B)(1) at 31.

49. *Id.*

contraband, evidence, a fruit of crime or an instrumentality of a crime, but not when it merely *contains* evidence of a crime.[50]

When hardware is contraband, evidence, an instrumentality or a fruit of crime, agents should "obtain a warrant to seize the computer, seize the hardware during the search, and then search through the defendant's computer for the contraband files back at the police station or computer forensics laboratory."[51] This approach is unlikely to pose any practical problems when the object of a search is one or more personal computers, but it can become problematic when the object "is not a stand-alone PC but rather part of a complicated network, the collateral damage and practical headaches that would arise from seizing the entire network generally counsels against a wholesale seizure." [52] In these situations, the agents will "take a more nuanced approach to obtain the evidence they need."[53] Specifically, the *Guidelines* suggest agents confronting this "situation call the Department of Justice's Computer Crime and Intellectual Property Section . . . or the Assistant U.S. Attorney designated as a Computer-Telecommunications Coordinator (CTC) in their district for more specific advice" [54] on how to proceed.

When hardware merely stores evidence of a crime, its seizure is not justified under Rule 41(b).[55] The 2001 *Guidelines* concede that in this situation "Rule 41(b) authorizes agents to obtain a warrant to seize the electronic evidence, but arguably does not authorize the agents to seize the hardware that happens to contain that evidence."[56] Further, Rule 41(b)asserts that "[t]his does not mean that the government cannot seize the equipment: rather, it means that the government generally should only seize the equipment if a less intrusive alternative that permits the

50. *Id.* Rule 41(b) states that a warrant can be issued to search for and seize any "(1) property that constitutes evidence of the commission of a criminal offense; or (2) contraband, the fruits of crime, or things otherwise criminally possessed; or (3) property designed or intended for use or which is or has been used as the means of committing a criminal offense." Fed. R. Crim. P. 41(b).

51. GUIDELINES, § II(B)(1)(a) at 32.

52. *Id.*

53. *Id.* ("For example, if a system administrator of a computer network stores stolen proprietary information somewhere in the network, the network becomes an instrumentality of the system administrator's crime. Technically, agents could obtain a warrant to seize the entire network. However, carting off the entire network might cripple a functioning business and disrupt the lives of hundreds of people, as well as subject the government to civil suits under the Privacy Protection Act, 42 U.S.C. § 2000aa and the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701–11.").

54. *Id.*

55. *See supra* note 49.

56. GUIDELINES, § II(B)(1)(b) at 32. (citing U.S. v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982)).

effective recovery of the evidence is infeasible in the particular circumstances of the case."[57]

The 2001 *Guidelines* explain the circumstances under which a seizure of computer hardware containing evidence is justified:

> As a practical matter, circumstances will often require investigators to seize equipment and search its contents off-site. First, it may take days or weeks to find the specific information described in the warrant because computer storage devices can contain extraordinary amounts of information. Agents cannot reasonably be expected to spend more than a few hours searching for materials on-site, and in some circumstances (such as executing a search at a suspect's home) even a few hours may be unreasonable. Given that personal computers sold in the year 2000 usually can store the equivalent of ten million pages of information and networks can store hundreds of times that (and these capacities double nearly every year), it may be practically impossible for agents to search quickly through a computer for specific data, a particular file, or a broad set of files while on-site. Even if the agents know specific information about the files they seek, the data may be mislabeled, encrypted, stored in hidden directories, or embedded in "slack space" that a simple file listing will ignore. Recovering the evidence may require painstaking analysis by an expert in the controlled environment of a forensics laboratory.
>
> Attempting to search files on-site may even risk damaging the evidence itself in some cases. Agents executing a search may learn on-site that the computer employs an uncommon operating system that the on-site technical specialist does not fully understand. Because an inartful attempt to conduct a search may destroy evidence, the best strategy may be to remove the hardware so that a government expert in that particular operating system can examine the computer later. Off-site searches also may be necessary if agents have reason to believe that the computer has been "booby trapped" by a savvy criminal. Technically adept users may know how to trip-wire their computers with self-destruct programs that could erase vital evidence if the system were examined by anyone other than an expert. For example, a criminal could write a very short program that would cause the computer to demand a password periodically, and if

57. *Id.*

> the correct password is not entered within ten seconds, would trigger the automatic destruction of the computer's files. In these cases, it is best to seize the equipment and permit an off-site expert to disarm the program before any search occurs.[58]

This explanation recycles all five factors the 1994 *Guidelines* cited as justifying an off-site search.[59] The 2001 *Guidelines* do note that agents searching for evidence "stored on the computer network of a functioning business will, in most circumstances, want to make every effort to obtain the information without seizing the business' computers, if possible".[60] They point out that seizing files and hardware for an off-site search will not be necessary if the agents can either make electronic copies of the files targeted by their search warrant or "mirror a segment of the storage drive based on knowledge that the information exists somewhere within that segment of the drive."[61]

Like the 1994 *Guidelines*, the 2001 *Guidelines* encourage agents to have the warrant authorize an off-site search;[62] the 2001 *Guidelines* also emphasize the importance of developing a search strategy before agents ever apply for a warrant to search a computer or computer system.[63] The *Guidelines* also provide sample language to be incorporated in an affidavit seeking authorization of an off-site search.[64] A computer search and seizure manual issued by the New Jersey Attorney General's office takes a slightly different approach:

> 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,

58. *Id.* at 32–33. *See* People v. Gall, 30 P.3d 145, 154 (Colo. 2001) ("In addition to the problems of volume and commingling, the sorting of technological documents may require a search to be performed at another location 'because that action requires a degree of expertise beyond that of the executing officers,' . . .").

59. *See supra* note 39 and accompanying text.

60. GUIDELINES, § II(B)(1)(b) at 33.

61. *Id.*

62. FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 56 Crim. L. Rep. (BNA) § VI(B)(3) at 2049 (1994); GUIDELINES, § II(B) Step 3 at 47–48.

63. GUIDELINES, § II(A)(3) at 30.

64. *Id.*, app. F at 106. *See* United States v. Markey, 131 F. Supp.2d 316, 322 (D. Conn. 2001) ("Agent Nates' affidavit described in detail the procedure that would be followed if an on-site analysis of the data contained in the computer was not practical or feasible"); *see also* NEW JERSEY COMPUTER EVIDENCE SEARCH AND SEIZURE MANUAL, app. B, C (2000) *available at* http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf (last visited Mar. 5, 2002). An example of an application for a search warrant that requests authorization for an off-site search is *available at* http://cryptome.org/usa-v-rtf-swa.htm (last visited Mar. 3, 2002).

> regarding the necessity of examining data in a controlled lab. The warrant should authorize seizure and off-site searching. . . .
>
> 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.[65]

With regard to the justifications for off-site computer searches, there is really no substantive difference between the 1994 *Guidelines* and the 2001 *Guidelines*. Most state and federal courts have upheld off-site computer seizures and searches, citing the off-site document search doctrine and the additional concerns articulated in the Department of Justice's 1994 *Guidelines*.[66] The next section considers whether

---

65. NEW JERSEY COMPUTER EVIDENCE SEARCH AND SEIZURE MANUAL, I(A)(6) at 24 (2000) *available at* http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf (last visited Mar. 5, 2002). The New Jersey manual identifies the following as the factors that will determine whether an off-site search, not authorized by a warrant, will be "reasonable":

> 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.

Id. at 24–25.

66. *See* United States v. Schandl, 947 F.2d 462, 465–466 (11th Cir. 1998); United States v. Gurs, No. 93-30261, 1996 WL 200998 (9th Cir. Apr. 25, 1996) ("[I]t was reasonable for the executing officers to seize the hardware and search the hard drives in a secure location. The only alternative would have been to secure the Gurs's home and search the computers there. This however, could have taken days, and would have unreasonably intrusive in its own right.") United States v. Hunter, 13 F.Supp. 2d 574, 583–84 (D. Vt. 1998). *See also* United States v. Upham, 168 F.3d 532, 535–36 (1st Cir. 1999); Commonwealth v. Gousie, No. BRCR2001-0115-1-6, 2001 WL 1153462 *8 (Mass. Super. Sept. 26, 2001); Commonwealth v. Ellis, No. 97-192, 1999 WL 815818 (Mass. Super. Aug. 27, 1999); United States v. Stewart,

these principles—as carried forward in the 2001 revision of the *Guidelines*—can justify off-site computer searches in any but the most extraordinary circumstances.

C. *When are Off-Site Computer Searches Reasonable?*

An examination of the merits of the justifications that have been put forth for off-site computer searches can be performed utilizing the hypothetical. Since the rationale for off-site computer searches relies heavily on the rationale for off-site document searches, the Doe & Doe hypothetical will be analyzed from two different perspectives: (1) as an off-site document search; and (2) as an off-site computer search.

D. *Off-Site Document Search*

Assume the Doe & Doe search was conducted some years earlier, at a time when law offices did not use computers to generate and store documents. Also assume that all other events occurred as set out in the original hypothetical, e.g., that the agents obtained a warrant to search the Doe & Doe law office, that they executed the warrant, and that they seized approximately 200,000 documents—the equivalent of 2.7 million pages of printed text or 8 gigabytes of storage space on a computer's hard drive—from the office. In addition to seizing these documents, the agents also seized files, i.e., six file cabinets, complete with contents plus ten boxes of files that were in the offices of lawyers and support staff.

The law firm challenged the agents' actions by filing a motion seeking the return of their property.[67] The law firm argued that the agents' seizing of the documents was unreasonable and therefore violated the Fourth Amendment for any or all of several reasons. The first reason was that instead of searching for documents that fell within the scope of the warrant and could therefore legitimately be seized, the agents seized essentially all of the documents they found at the firm, intending to search through them later at another location. Doe & Doe argued this was unreasonable because the agents took documents the warrant did not entitle them to take; since the warrant did not justify seizing these unrelated documents, their seizure clearly violated the Fourth Amendment. Doe & Doe also argued that taking the documents away gave the agents more time to review them, and that they could use this opportunity to exploit

No. Crim. A. 96-583, 1997 WL 189381 (E.D. Pa. Apr. 16, 1997); United States v. Sissler, No. 1:90-CR-12, 1991 WL 239000 *4 (W.D. Mich. Aug. 30, 1991), *aff'd*, 966 F.2d 1455 (6th Cir. 1992).

67. *See* FED. R. CRIM. P. 41(e).

the plain view doctrine,[68] reading irrelevant documents in an attempt to find evidence concerning unlawful activities other than those which were the focus of the warrant.[69] In making this argument, Doe & Doe claimed the agents were using the off-site search to go outside the scope of the warrant and search for evidence of unrelated, as yet undiscovered criminal activity.[70] Doe & Doe noted that such a search would be unreasonable because it would not be authorized by the warrant nor by a valid exception to the warrant; that is, Doe & Doe argued that this would violate the requirement that a warrant specify the items to be searched for and seized because it gave the agents essentially unfettered discretion to review the documents in an effort to identify evidence of crimes other than those which gave rise to the search warrant.[71] Finally, Doe & Doe argued that the seizure was unnecessary because the agents could simply have sorted through the law firm's documents *in situ*, taking documents that fell within the scope of the warrant and leaving those that did not.

In response, the government argued that it was reasonable for the agents to seize all the documents and take them off-site where they were reviewed and sorted into those that fell within the scope of the warrant. Those documents that fell within the scope of the warrant were seized, those that did not fall within the scope were returned to Doe & Doe. Noting that it took the agents many days to sort and review the documents, the government claimed it would have been unreasonably intrusive to have this process conducted at the law firm's office. The government argued that the presence and activities of the agents would have disrupted all activity at the firm for a similar period of time, and that it was, therefore, more reasonable to have them remove the documents

68. *See infra* Part IV.

69. In dealing with paper records, officers are allowed to conduct a fairly brief review of a record in order to determine if it falls within the scope of the warrant, but this review must cease as soon as it becomes clear that the document does not fall within the scope of the warrant. *See* United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1981); United States v. Ochs, 595 F.2d 1247, 1258 (2nd Cir. 1979). *See also* Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("[R]esponsible officials . . . must take care to assure that [document searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy.").

70. Doe & Doe pointed out that by taking the documents off-site, the agents were able to review them without any representative of Doe & Doe's being present to ensure that the agents did not exceed the scope of the warrant by thoroughly reviewing clearly irrelevant documents.

71. *See* Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 325–26 (1979) (holding a search violated the Fourth Amendment's requirement that a warrant particularly describe the place to be searched and the items to be seized because the warrant essentially gave the parties conducting the search unlimited discretion to expand their search as they went through items on the scene). Doe & Doe would make an argument based on holding in *Lo-Ji Sales* by claiming the officers have taken advantage of the opportunity to seize a large quantity of information which allows the officers to rummage through the information at their leisure in an attempt to identify items that are within and outside the scope of the warrant.

and review them off-site. As to the scope of the seizure, the government explained that the agents were forced to seize a large volume of documents because they believed each of the seized files contained at least some documents encompassed by warrant. The government pointed out that, under the off-site search doctrine, officers are allowed to seize large volumes of records when it appears that relevant and irrelevant documents are so closely intermingled that it is not possible to sort them out quickly,[72] as long as they return any irrelevant documents within a reasonable period of time.[73] With regard to Doe & Doe's claim that the agents impermissibly used the off-site search to exploit the plain view doctrine, the government pointed out that this is an issue which could easily be resolved by a motion to suppress evidence. If Doe & Doe felt the officers unconstitutionally used the plain view doctrine to find evidence of unrelated crimes, Doe & Doe can move to suppress any such evidence, and it will be up to the government to show that the evidence was discovered lawfully.[74] Finally, as to Doe & Doe's claim that the off-site search was unreasonable because it was conducted without the presence of any representative of the law firm, the government argued that the firm had no constitutional right to be present during the search, and that allowing the firm to have a representative present while the search was conducted would undoubtedly have only lengthened the process.[75]

To resolve the hypothetical, it will be assumed that the court will apply the off-site document search doctrine. The court will therefore reject Doe & Doe's arguments and uphold the constitutionality of the off-site search. It will be assumed that the off-site document search doctrine is a valid Fourth Amendment principle and that the doctrine was correctly applied in this instance. The purpose of this scenario is to illustrate how the doctrine can be applied to paper document searches.

E. *Off-Site Computer Search*

The Doe & Doe scenario illustrates that the off-site document search doctrine is grounded in some characteristics peculiar to paper documents. In order to search the contents of paper documents, an officer has to leaf through each page of a document, reading or at least scanning the text of the document to determine whether the document falls within the

72. *See* United States v. Hargus, 128 F.3d 1358, 1363–64 (10th Cir. 1997).

73. *See* United States v. Tamura, 694 F.2d 591, 596 (9th Cir. 1982).

74. *See* Commonwealth v. Ellis, No. 97-192,, 1999 WL 823741 at *34 (Mass. Super. Aug. 18, 1999) (suppressing documents seized during law firm search, the documents did not fall within the scope of the warrant and could not have legitimately been discovered under the plain view doctrine).

75. *See id*. at *24.

scope of the warrant that authorized this intrusion. This is necessarily a tedious, time-consuming process. In the Doe & Doe scenario, if the documents stored as computer files had been in paper form, searching through them would require officers to review 200,000 documents constituting roughly 2.7 million pages of text, and to determine which of those pages contained information that would permit the documents to be seized under the authority of the warrant. Since the alleged criminal activity that justified the warrant was complex in nature, an officer might, on occasion, have to seek a prosecutor's assistance in making this determination. This consultation will only increase the time required to review the documents and select those that could legitimately be seized. If all this were done on-site, the officers (and any prosecutors assisting them) would be encamped at the Doe & Doe offices for many days.

Another characteristic of a paper document search is the time and effort involved in copying the documents. Assume that instead of either reviewing the Doe & Doe documents on-site or taking them off-site and reviewing them elsewhere, the officers had decided to copy all the documents, take the originals and leave the copies with Doe & Doe. This would not simply entail copying the aggregate 2.7 million pages of text represented by the seized 200,000 documents. The officers would have to copy every document, collate the copied pages of that document and assemble the pages into a duplicate of the document or file. This would be a tedious, time-consuming process. If the officers copied the documents at Doe & Doe, the process could shut down the law firm for many days. If the documents were taken off-site to be copied, there would still be the problem of document seizure.

Finally, paper documents are relatively sturdy. When officers seize paper documents and take them off-site to sort and search, there is very little likelihood that any of the documents will be destroyed, and essentially no chance that the information the documents contain will be altered. Therefore, taking paper documents off-site to sort and process them creates a very minimal risk that evidence will be damaged or lost.

The off-site document search doctrine accurately reflects the practical difficulties involved in conducting a search of a large quantity of documents, especially when the search is intended to locate evidence of complex criminal activity.[76] However, the analysis must be applied to the off-site computer search doctrine to determine if it accurately reflects the processes involved in searching for computer-generated evidence.

76. The scenario we are using involves business premises instead of a home. The considerations discussed above would apply with equal force when a large quantity of documents are discovered at a home.

F. *Off-Site Document Search Rationale Inapplicable to Off-Site Computer Searches*

While the officers, in the original hypothetical, undoubtedly seized a quantity of paper documents, the primary focus of their efforts was the Doe & Doe computers. As the hypothetical in § I explains, the officers seized Doe & Doe's network server, twenty-two stand-alone computers, thirteen computer back-up tapes and a printer. The seized computers and computer equipment were taken to an off-site location, where the officers reassembled the server. When the officers had reassembled the system, they made back-up copies of the data it contained and then began searching the computer system and storage media.

In the previous section, it was assumed the off-site search would have been reasonable under the Fourth Amendment if the officers had seized only paper documents. This assumption must be reconsidered when officers seize computer-generated evidence.

The primary justification given for off-site searching of paper documents is the time and effort involved in reviewing large quantities of documents to determine which, if any, contain evidence that falls within the scope of the warrant.[77] As the previous section notes, this process necessarily requires that each document be reviewed by one or more officers; there is no way to automate the review.

G. *Automated Search Techniques*

With computer-generated evidence it is possible to perform certain limited searches using automation. The officers in the original hypothetical used a program to run a key-word search on all of Doe & Doe's stand-alone computers. The officers used the key-word search to determine which of the stand-alone computers to seize and search more thoroughly off-site. The fact that a search was conducted demonstrates one basic difference between paper documents and computer-generated evidence. Officers using search software could search for specific words or phrases in the Doe & Doe computer files in a small fraction of the time it would take their hypothesized counterparts to review the same information contained in paper documents.

From the technical viewpoint, automated search techniques have inherent strengths and weaknesses that distinguish the search from conventional document review. Automated keyword searches have the advantage of being both fast and accurate. The usefulness is limited to situations where there is some precise textual identifier that can be used

77. *See supra* Part II(A).

as the search argument. Keyword searches are context insensitive, and cannot employ the discrimination used by a human investigator. If either the data encoding or the alleged criminal activity is complex in nature, human judgment will be required to determine the evidentiary value of specific electronic documents and whether the documents fall within the scope of the warrant.

The benefits of electronic search techniques are that they are fast, accurate, and within the narrow scope of their capabilities. If the officers are searching for very specific information and know one or two exact phrases or words to search for, a comprehensive electronic search can be conducted in a matter of hours. For example, if the officers were searching for a copy of specific insurance claims or accounting records, and the officers knew with certainty that these records would contain specific phrases, numbers, or names, these records could be located very quickly. Once the appropriate electronic records were located, they could be copied on a file-by-file basis, in effect allowing seizure of only the files that fall within the scope of the warrant.

By contrast, if the officers conducting the search do not have specific information (names, numbers, phrases) sufficient to allow an accurate identification of *all* relevant documents, electronic searches are far less useful. The use of common words or phrases as keywords may still help locate relevant evidence, but such searches yield a high number of false hits. False hits are documents that contain the searched—for term, but have no evidentiary value and are beyond the scope of the warrant.

The usefulness of keyword searches is further diminished by the fact that such searches are context insensitive. Computer data is encoded. Many computerized documents require specialized software to read or render their contents comprehensible. Such software provides the *context* required to interpret electronic data. For example, the medical records, accounting data, and medical appointment logs in our hypothetical would most probably contain many abbreviations or coded values representing various medical procedures and associated charges. A record containing a patient's name, a numeric value of 1, a procedure code of 346 and a charge of 740000 might not seem suspicious. But if the numeric value 1 is a code that indicates that the patient is a male, and the medical procedure code of 346 identifies the operation as a hysterectomy, then the legitimacy of the $7400.00 charge is suspect. Without knowing the context of the numbers 1, 346, and 740000, the data represented cannot be evaluated for relevance.

The manner in which computer data is represented also limits the effective scope of automated search techniques. Many automated search tools are based on the detection of textual character strings embedded in

documents. These techniques can only be applied to textual data, and not for pictures, diagrams, or scanned images. For example, a search for the word "submarine" would locate text that contained those characters, but it would fail to locate the scanned image of a submarine, a digital photo of the control tower, or even a scanned image or photo of the original document. The textual search would also fail to locate the desired document if it had been compressed, encrypted, or password protected. Depending on the software used for the search, it might or might not detect the word "submarine" in files that had been deleted.

Other types of searches depend on properly identifying documents by either document type or by file name. Searches by file *name* are unreliable because a user is free to name (or rename) files without regard to their content. Searches by file *type*, can be accomplished using specialized tools that identify files based on the "signature" associated with the program used to create the file. This technique can be used to identify or group files based on how data is represented. These tools can identify file *format*, but are not able to search *content*. Searches based on file type are not normally effective against files which have been encrypted, compressed, or password protected.

H. *Technical Considerations*

The feasibility of conducting an on-site search should be influenced by three primary technical considerations: the configuration of the software and hardware, the overall size and complexity of the computer system, and the technical demands of the search.

The configuration of the software and hardware is an issue because specialized knowledge is required to avoid damaging the evidence while performing even simple tasks such as starting up the computer, examining a directory listing, or opening a file to inspect the contents. On most computer systems all of these acts will result in damage to the evidence. The specific remedy to avoid damage will depend on the technology of both the computer system and the tools to be used.

Software and hardware configuration will also determine the skills (and tools) that the examining officer must possess in order to conduct a successful search. Different tools and techniques are required for different operating systems, and also for different software products. For example, some common e-mail systems save messages in a simple textual format that can be readily searched using keyword searches. Other common e-mail products save messages in a compressed format, in order to save disk space. E-mail systems that use compression cannot be searched with the normal tools used for keyword searches. The examin-

ing officer must use the e-mail system itself, or specialized utilities, to examine the contents of messages.

The size and complexity of the computer system is also a factor in the feasibility of conducting an on-site search. On large-scale computer systems the feasibility of off-site searches breaks down under the sheer weight of system size, but even without the size consideration, an off-site search is often infeasible due to the system complexity.

The core of the problem is that these "big-iron" systems possess a far more complex hardware and software profile than a personal computer. The problem of seizure is similar to the task of disassembling and assembling an analog watch. There are a vast number of interconnected pieces, which are related to each other in very specific ways, and the interactions between the pieces is both precise and delicate. A large support staff, each with specialized skills and knowledge, maintains most mainframe systems. The costs to care for and maintain a mainframe are high. It is common that the annual budget for mainframe hardware, maintenance, support, and software exceeds several million dollars. An additional problem is presented by the amount of time that would be required to seize a copy of a mainframe system due to the amount of storage involved. In a typical large system, there might be thousands of gigabytes of active disk storage to back up. Such a system might also have tens of thousands of backup tapes.

The technical demands of the search may determine whether an on-site search is feasible. Some of the factors to consider include whether or not appropriate search tools exist for the specific configuration, whether the tools are already installed on the computer to be searched, whether the tools available on-site can be used without destroying evidence, whether the searching officer has sufficient information about the format and encoding of the electronic evidence to conduct a meaningful search, whether deleted files are to be searched, and whether the computer system is protected by passwords, encryption, or other security that might thwart attempts to conduct an on-site search in a timely fashion.

The number of terms to be searched for is also a factor. As the list of search terms grows, so does the time required to accomplish the search. A ten-gigabyte hard disk can be searched, using a single search term, in less than an hour. If the list of search terms is increased to 50, the search will take 15–20 hours to complete.

I. *Back-Up Copies Made on-Site for Off-Site Search*

Even if we assume that an automated search of the Doe & Doe computer files would consume enough time that the officers' presence at the law firm would be sufficiently intrusive to justify letting them conduct

their search off-site, there is another alternative. As the previous section explained, copying paper documents is not a realistic alternative to searching off-site because the process of making the copies is time-consuming, costly, and intrusive. This is not true in regards to computer-generated evidence. Officers can generate back-up copies on-site and then search the back-ups off-site.[78] The time required to make the back-up copies would be only a small fraction of the time that would be required to copy a corresponding volume of paper documents. Therefore, generating the back-up copy would not rise to the level of intrusiveness of copying paper documents.

The act of making back-up copies normally will require that the agents or technicians generating the copies be given unfettered access to the computer system, a requirement which may disrupt a law firm's (or a business') ability to continue its operations. In some cases, making the necessary back-up copies may require days of dedicated access to the computer system, but, even so, the process of making such copies is less disruptive than seizing the system hardware.

Another virtue of the officers creating back-up copies is that the law firm is not deprived of the information it needs to conduct business. When the officers seize Doe & Doe's computers (or Doe & Doe's paper documents, in the variant hypothetical), they completely deprive Doe & Doe of the information stored on those computers (or contained in the paper documents). This makes it difficult, if not impossible, for Doe & Doe to conduct its professional activities. A generally unacknowledged side effect of seizing information for an off-site search is that the seizure can effectively prevent the owner of the seized information from continuing to conduct regular business or professional activities.[79] (This effect is, of course, only compounded if the officers also seize the computer equipment belonging to the person or business that is the object of the scenario; this issue is discussed below). The disruption of business does not occur if the officers copy the information stored on the owner's computer systems. The officers can conduct their searches and the owner of the information can proceed with business.[80]

78. *See infra* Part III(D), IV (discussing the scope of the off-site search). *See also* DIBS Computer Forensics: Portable Evidence Recovery Unit *at* http://www.computer-forensics.com/products/peru.html. (last visited Oct. 2, 2001).

79. *See* Steve Jackson Games, Inc. vs. United States Secret Service, 816 F.Supp 432, 437–39 (W.D. Tex. 1993), *aff'd* 36 F.3d 457 (5th Cir. 1994) http://www.sjgames.com/SS/; *infra* Part II(K).

80. *See id*. (determining the agents who executed the warrant had experts available who could have copied the information contained on the stored hardware within hours and therefore awarded damages against the agency responsible for seizure of business' computers and data).

From the technical perspective, the preferred course of action is *always* to preserve a forensic copy[81] of the evidence first, before any search is performed, to provide insurance against any possible contamination or damage to evidence by either the search process or any subsequent seizure. In many cases, production of a forensic copy will obviate the need for seizure. Preserving a forensic copy of the evidence should be the first step regardless of whether the computer system is to be searched on-site or off-site. Special backup software provides the capability of creating accurate backups that contain all of the evidence from the original media, including information contained in deleted files and space on the hard disk that is not allocated to any file.

J. *Spoliation—Inadvertent*

Having the officers make back-up copies of the information stored on computers, like the Doe & Doe computers, reduces the possibility that evidence will be altered or destroyed. As the previous section noted, paper documents are relatively impervious to inadvertent alteration and are sufficiently sturdy so that they are unlikely to be destroyed, absent some unanticipated accident or cataclysm. That is not true of computer-generated evidence. Computer-generated evidence can be very vulnerable. Even without deliberate spoliation attempts, normal use of a computer system will result in the inadvertent obliteration of large quantities of evidence.[82]

During the normal use of a computer, the computer's operating system and programs record information that can be used to reconstruct the actions of the human operator. This information, which is invisible to the average computer user, can reveal when the system was used, when files were created, modified, or accessed, what Internet sites were visited, what searches were performed, what files were downloaded, what

81. Forensic copy, for the purposes of this article, is defined as a copy of the computer system or media which contains an accurate copy of all of the active files, deleted files and unallocated space on the computer media. The copy must have sufficient information to identify the system from which the back-up copy was made, along with the date, time and technology used in making the back-up copy. A forensic back-up should, if possible, be accompanied by a checksum for both the original media and any back-up copy. This checksum can be used both to authenticate the copy and to determine whether the evidence contained in the copy has been the subject of any tampering or contamination.

82. Many forms of forensic examination run the risk of contamination. Biological samples from a subject can be inter-mingled with those of the examiner. But the problems with some computer-derived material are intense—the very act of opening an application or file, even if there is no intention to alter anything, often in fact creates changes although they may not be immediately visible. *See* Peter Sommer, *Downloads, Logs and Captures: Evidence From Cyberspace*, 5 J. FIN. CRIME 138, 142 (2000).

documents were edited, and what e-mails were sent and received. The information may also reveal what files were deleted, when they were deleted, and even the contents of e-mail, documents, and images that the user has attempted to destroy.

The information is automatically generated by the operating system and programs and is revised constantly as the computer system is used. During normal computer use, many temporary files are created and deleted by the operating system. Additional files are created, deleted, or modified by the specific actions of the user. If the computer system is in continual use, older information will be overwritten with newer information. The more the system is used, the more evidence will be lost. The simple act of starting a Microsoft Windows system will destroy more than 4,000,000 characters of evidence, and the spoliation will be far greater if the system is used to run any programs.

The spoliation that results from casual use takes several forms. Normal use destroys evidence in the form of system data, which records information about recently used files and user actions such as Internet access. This destruction of evidence occurs as information recording system activity is overlaid by new user activity. File use, both deliberate and incidental to the system operation, will result in contamination of the date information that records when files were created, accessed, or modified.

When a computer is used, the system and programs used create and, subsequently, discard many temporary files. Human users create, modify, or delete additional files. Creation of new files results in the overlay and obliteration of information that remains in deleted files, rendering the contents of deleted files unrecoverable.

In addition to the spoliation that occurs as a result of casual use, there are additional threats to the electronic evidence. These include automated housekeeping tasks, virus corruption, hardware failure, software failures, mishandling, and deliberate actions taken to alter or destroy evidence.

The computer performs various housekeeping tasks that are required to allow the system to function optimally. These tasks include activities such as flushing the Internet cache file and overlaying the information recorded about Internet activity, deleting temporary files to free up disk space, defragmenting disk space (which overlays the contents of deleted files), and compressing mail boxes (which overlays the contents of deleted e-mail messages).

When a computer system is used, the electronic evidence it contains is vulnerable to damage by a computer virus. After infecting a computer system, many destructive viruses will remain dormant and undetected

until some specific event triggers their activation. Triggering events can include innocent actions such as use of a program to open or save a file, reading an e-mail message,[83] visiting an unfriendly web site, or simply having the computer turned on when a certain calendar date occurs.

Hardware and software failures occur unpredictably and can damage or completely destroy electronic evidence. Software failures can result in corrupted documents, accidental overlays of information, malformed data, or accidental deletion of files. Hardware or media failures can result in partial or complete obliteration of electronic and optically recorded information. There is not a form of computer readable media or hardware that can be used to read and write to a medium that is not subject to the possibility of failure. Over time, all computer media degrades, even if handled carefully. Attempts to read good media in faulty or dirty drives can also result in data destruction.

Accidental mishandling or trauma can also destroy electronic evidence. Media can be damaged by electrical spikes that occur while the system is used, shocks from falling, electro-magnetic fields, or physical extremes in heat, moisture, or cold. Computers and media can be easily damaged if they are improperly handled when transported.

K. *Spoliation—Advertent*

Electronic evidence may also be altered or destroyed in any number of deliberate ways. There are utility programs available to shred electronic e-mail and documents, alter the invisible system dates, and overwrite deleted files or entire disks. Even without any special tools, most of the deleted files on a computer system can be rendered effectively irrecoverable by overwriting them with benign files.

The discussion so far has focused on whether it is reasonable to extrapolate the justifications for conducting off-site searches of documents to off-site searches of computer-generated evidence. This does not exhaust the rationales given for off-site computer searches. Both versions of the *Guidelines*[84] also justify off-site searches on the basis of two factors that are unique to computer searches: (a) the need to conduct a controlled search to prevent the destruction of evidence, and (b) the need to seize computer hardware and use it to search seized files.[85]

83. Until recently, the act of merely reading an e-mail message could not, by itself, launch a virus attack. Many new e-mail systems are both more sophisticated and more vulnerable than their predecessors. The vulnerability stems from the automatic execution of invisible commands embedded in the messages.

84. *See infra* Part II(B).

85. FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 56 Crim. L. Rep. (BNA) § IV(H)(2) at 2040 (1994); FEDERAL GUIDELINES FOR SEARCHING AND SEIZING

This standard makes no mention of the specialized software that may be needed to render data comprehensible—even though such software may present a greater technical challenge than the hardware. This standard also omits any clear guidelines for situations that involve specialized hardware or software residing on a separate computer system—i.e. software that runs on a client, which is required to access data on a separate server.

The Department of Justice bases its contention that off-site searches are necessary to prevent the destruction of evidence on two different premises, the first of which is a variation on a traditional exception to the warrant requirement. The exceptions is for actions which would otherwise be unreasonable under the Fourth Amendment but the actions can be justified by the need to prevent the destruction of essential evidence.[86] This is certainly a valid point, as long as there is probable cause to believe that the destruction of evidence is, in fact, imminent.[87] For an off-site search to be justifiable under this theory, the government should have to show, at a minimum, that there is reasonable suspicion to believe evidence will be destroyed if officers attempt to conduct an on-site search.[88] Reasonable suspicion for such a belief might be established, for example, if the government adduced evidence showing the search was to be conducted of equipment owned or used by a "hacker" or computer terrorist, and if the government could show there was specific reason to believe this person might have "booby-trapped" his or her computer so that evidence could easily be destroyed by someone unfamiliar with the system.[89] On the surface, it would seem highly improbable that this rationale could be used to justify an off-site search of business computers such as those owned and operated by Doe & Doe.[90] Aside from anything

COMPUTERS § II(B)(1)(b) at 32–33 (2001) *available at* http://www.cybercrime.gov/searchmanual.pdf.

86. *See* WAYNE R. LAFAVE, 3 SEARCH AND SEIZURE § 6.5(b) (3d ed. 1996).

87. *Id.*

88. This is analogous to the showing officers have to make to justify a no-knock entry when executing a search warrant. No-knock entries are an exception to the Fourth Amendment's requirement that officers knock and announce their presence before entering to make an arrest or execute a search warrant. *See* Richards v. Wisconsin, 520 U.S. 385, 394–95 (1997).

89. *See* Mahlberg v. Mentzer, 968 F.2d 772, 775–76 (8th Cir. 1992) (holding it was reasonable for officer executing computer search warrant to seize disks when he had been warned by suspect's former employer, from whom suspect had stolen software, that the suspect might booby-trap his computer so it would erase files when agents tried to search it on site). *See also* FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 56 Crim. L. Rep. (BNA) § IV(H)(2)(a) at 2040 (1994).

90. *See* Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), *aff'd* 36 F.3d 457 (5th Cir. 1994) (finding failure in an agent who obtained and executed business search warrant for not taking time to determine that the business was a legitimate operation that would have cooperated with the agent's investigation).

else, it stretches credibility to the breaking point to imagine that a law office would "booby-trap" its computer system, so that its files, billing records and other documents might be destroyed by the inadvertent actions of a clerk. In reality, no such deliberate "booby-trap" would be required for evidence to be destroyed. As explained above, the normal use of a computer system will result in the destruction and contamination of evidence. Even the act of inspecting file contents will alter the evidence unless the inspection is performed using specialized tools, or against a copy of the original.

The second premise the Department of Justice relies on as supporting its contention that off-site searches are necessary to prevent the destruction of evidence is the need to have searches conducted by persons with the requisite computer expertise.[91] As the *Guidelines* explain,

> [t]he computer expert who searches a target's computer system for information may need to know about specialized hardware, operating systems, or applications software just to get to the information. For example, an agent who has never used Lotus 1-2-3 (a spreadsheet program) will not be able to safely retrieve and print Lotus 1-2-3 files. If the agent entered the wrong computer command, he could unwittingly alter or destroy the data on the system.[92]

Computer searches should be conducted by qualified personnel, but it is difficult to see why the need for off-site searches becomes part of this proposition. Would it not be far more reasonable to bring the qualified personnel to the scene and have them conduct the search on-site, instead of disassembling the computer equipment, seizing it, taking it to an off-site location, reassembling it and then having the experts run their analyses?

From the technical viewpoint, this question cannot be answered with a simple yes or no. In order to avoid contaminating the evidence, the tools used to perform searches and analyze electronic evidence can not be installed on the target computer until after a complete forensic backup has been secured. Installing such tools on the target computer would overwrite deleted files, create new files, and reduce the possibility that tampering will be detected. Installing search and analysis tools also causes changes to certain of the system files and dates that would be examined in the normal course of an investigation, thereby damaging the

91. *See* FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 56 Crim. L. Rep. (BNA) § IV(H)(2)(a) at 2040 (1994); GUIDELINES, app. F at 106.

92. FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 56 Crim. L. Rep. (BNA) § IV(H)(2)(a) at 2040 (1994).

evidence further. In practice, these limitations can be overcome by searching the computer systems media from a separate computer system that is specially configured for this purpose. Depending on the nature of the hardware involved on both the search and target computers it may not be practical, or in some cases even possible, to conduct such searches on-site.

L. *General Affidavit Language not Sufficient*

Another, less convincing argument is illustrated by this excerpt from an agent's affidavit, submitted to obtain a warrant to seize and search computer equipment as part of a child pornography investigation:

> Computer storage devices . . . can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. 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; and searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The wide variety 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 should analyze the system and its data. . . .[93]

There are several problems with allowing computer equipment to be seized and searched off-site based on assertions such as these. Some of the problems are technical; one is not. As to the latter, the language above is an example of form language that is often included in computer search warrants. There is nothing in the above paragraph that provides any idiosyncratic information about the specific individual/suspect whose computer equipment is to be seized or why it is not feasible to search that particular equipment on—site. Just because searching "can take weeks or months" does not mean it will take weeks or months to search this particular suspect's computers on-site.

The technical objections also present problems of specificity. The above language fails to articulate a specific technical basis for seizure. The language does not identify whether the scope of the search is limited to images, e-mail, documents, or if other computer records are also to be

93. United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000).

searched. Assuming for a moment that the scope of the search is to locate only graphic images, the language above does not state why any of the techniques to be used for the search would require the search activity to be conducted against all files, or why it must be conducted off-site. This affidavit implies that file names are relevant to the search, but does not state why. Since file names are not constrained, a search based on file names would be a poor way to proceed. Better tools exist which would allow the officers to search for (and copy) files belonging to specific categories of information (text, graphic images, movies, etc.) The above language fails to specify which types of file are within the scope of the search warrant, and why appropriate techniques will not be used to isolate relevant materials from those outside the scope of the warrant. The above language also fails to specify any situation specific hurdles that would render an on-site search unfeasible. By way of example, if the system to be searched was expected to be so large that an on-site search was impractical, the officers should provide an estimate of the system size and the amount of time the search was expected to take, in order to allow the court the opportunity to decide the feasibility on those case-specific merits. The above language fails to consider on-site backup/off-site search of the copy, which would be a less intrusive alternative to most seizures.

Taking these technical issues into account, an affidavit submitted to secure a warrant should include identification of what specific systems or portions of systems are to be preserved, how many copies will be produced, how such copies will be made and verified, and who should receive copies of the media contents and checksum information. Once these issues are addressed, the affidavit should proceed to determination of the scope of any subsequent search, whether any allowed search should be conducted on-site or off-site, what will happen to any backup copies after the search is complete and, finally, to determine whether there is any legal or technical basis for seizing the actual hardware and software.

M. *On-Site Search May be Reasonable*

On-site searches are not inherently impossible or impracticable. In certain situations an on-site search is the most reasonable course of action. Situations in which an on-site search should be considered include those where the computer system is sufficiently small to allow a forensically accurate copy of the system to be preserved *in situ* and where the scope of the search is sufficiently narrow that automated tools could effectively be deployed to locate the relevant evidence in a reasonable period of time. Examples where this might be true include situations

where the scope of the search is limited to one or few computers with finite domains of electronic evidence such as e-mail or graphic images, and where appropriate tools exist to conduct the search without requiring manual access to individual documents. In those cases, files that fall within the scope of the warrant can be copied and searched on-site, or copied and the copy seized for off-site search.

Other situations in which an on-site search might reasonably be required include systems of sufficient size or complexity that it is impractical to search them off-site. For instance, as the *Guidelines* note, searching is necessarily done on-site whenever a mainframe computer system is involved.[94] In the case of mainframe computers, both the volume of evidence and the complexity of the computer system may render creating a copy or seizing the entire computer system impractical.

Consideration must also be given to the potential harm that might be caused by seizure of a computer system that is used for legitimate business purposes or which are used by third parties who are not subject to the warrant. Creating a complete forensic backup of a computer system requires unfettered access to the system, and prohibits the use of the system by other users for the entire period of time required to secure the copy. This could mean that users of very large computer systems could be denied access to the computer for a number of days, or possibly even weeks.

The final factor cited in the *Guidelines* as justifying off-site searches is the need to seize computer equipment (and documentation)[95] so experts can use the suspect's equipment to analyze his or her data at the law enforcement laboratory.[96]

> With an ever-increasing array of computer components on the market—and with existing hardware and software becoming obsolete—it may be impossible to seize parts of a computer system . . . and operate them at the laboratory. In fact, there may be times when agents will need to seize every component in the computer system. . . . Many hardware incompatibilities exist . . .

94. *See* FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 56 Crim. L. Rep. (BNA) § IV(H)(2)(a) at 2040 (1994). As a point of technical accuracy, it is possible to search a mainframe off-site, but the costs and technical hurdles that must be overcome are both formidable.

95. This does not appear to provide for seizing computer software that is needed to conduct the search, which may be a more problematic element from the technical viewpoint.

96. FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 56 Crim. L. Rep. (BNA) § IV(H)(2)(b) at 2040 (1994).

> and the laboratory experts may need to properly re-configure the system back at the lab in order to read data from it.[97]

This rationale is valid only if there is an independent justification for conducting an off-site search. If law enforcement experts can conduct their searches on-site, there is no need to seize all or part of a suspect's computer system and take it off-site.

If officers seize a business or professional suspect's computer system and data files, they have effectively shut down the suspect's operations. (If they give the suspect a back-up copy of the data, a back-up is of little use with no computers.) This happened to Steve Jackson Games, a company that publishes role-playing games, along with books and magazines about games.[98] On March 1, 1990, the Secret Service executed a search warrant at the company's offices; the warrant was issued as part of an investigation of data piracy, and authorized the seizure of computers and computer data.[99] The agents seized three computers, over 300 computer disks, a book and other documents intended for publication, a bulletin board system, and other materials.[100]

The seizure of this equipment and information caused great business and financial hardship for Steve Jackson Games.[101] No charges were ever brought against Steve Jackson Games or any of its employees and, indeed, the company recovered damages in a civil suit it brought against the Secret Service.[102]

All of these issues should be considered in determining whether an on-site search is feasible. If the warrant requests seizure and an off-site search, it should provide specific reasons why an on-site search cannot be performed.

N. *On-Site Copy with Off-Site Review*

From the technical viewpoint, there are many situations where on-site searches are either impractical or impossible. In these cases on-site preservation, followed by off-site analysis, is a more reasonable course of action. Having experts preserve the evidence first minimizes the possibility that evidence would be altered or destroyed by either subsequent use of the computer system, deliberate tampering, or the search itself.

97. *Id.*

98. *See* Welcome to Steve Jackson Games!, *at* http://www.sjgames.com/general/about-sjg.html (last visited Feb. 8, 2002).

99. *See* Steve Jackson Games, Inc. v. United States Secret Service, 816 F.Supp 432, 436–37 (W.D. Tex. 1993), *aff'd* 36 F.3d 457 (5th Cir. 1994).

100. *Id*. at 434–37.

101. *See Steve Jackson*, 816 F. Supp at 438–39 .

102. *See id*. at 435, 438–39.

Creating backups of the system before any extensive examination takes place also minimizes the possibility that evidence will be contaminated or destroyed in the event of any mishap when computer equipment is moved off-site, physically examined, re-assembled, or restarted.

Once a proper forensic backup is secured, having the expert conduct the actual search off-site is the best technical alternative. Off-site search allows the expert to employ techniques that minimize the possibility that the search process will contaminate the evidence. Due to the availability of both additional tools and additional time a more thorough search can be conducted off-site, ensuring that relevant evidence will not be overlooked. Off-site search of a forensic copy minimizes the intrusion of the search process and reduces the potential for mistakes induced by the pressure of attempting complex and delicate analysis on an expedited timeline in a hostile environment.

In situations that involve on-site preparation of a forensic copy, and subsequent off-site search, the application for the warrant should state specifically what search techniques will be used, and what specific precautions will be taken to ensure that the scope of the search is consistent with the scope of the warrant. If keyword searches are to be used, the warrant should describe the specific topics that will be searched for in as much detail as possible. By way of example, an affidavit for a warrant to search e-mail for evidence of drug trafficking activity might expressly state that e-mail files would be identified based on file signature and inclusion of to/from headers, and that a subsequent key-word search would be used to identify e-mail in these files which was to or from the suspect and which also contained any reference to drugs or drug-related activity.[103] Any e-mail identified by the keyword search would be reviewed to see if it contained reference specifically to drug trafficking activities, and if so a copy of the e-mail would be seized as evidence.

Based on the specific technical and legal fact pattern, off-site search of a forensic copy is probably the most practical scenario for most cases. Even so, there are situations where there may be no alternative to seizing the entire computer system for off-site search. In such cases, the application for a warrant to seize should explicitly state both the legal basis for the seizure and the specific technical reasons why on-site search or off-site search of a forensic copy is impractical.[104]

103. FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS app. F(C) at 111 (2001) *available at* http://www.cybercrime.gov/searchmanual.pdf (providing sample language for warrant application including use of key-word search).

104. *See* MODEL CODE OF CYBERCRIME INVESTIGATIVE PROCEDURE, art. VII § 7(f)(i) (1998) *at* http://www.cybercrimes.net/MCCIP/art7.html (last visited Feb. 16, 2002).

O. *Off-Site Searches: A Proposal*

There should not be a blanket prohibition against off-site computer searches under the Fourth Amendment. However, because of the direct and consequent intrusiveness which can result from seizing someone's computer data and equipment,[105] off-site searches must be specifically authorized by a Magistrate Judge in a warrant.[106] Also, no warrant should be issued authorizing the seizure of computer hardware, instead of making a forensic back-up copy of the data, unless the warrant affidavit provides a specific explanation of the technical reasons why the search cannot be conducted on-site or conducted off-site using forensic back-up copies of data.

The authorization can be contained in an original warrant or in a supplemental warrant. Warrant officers obtain supplemental warrant after they have begun to execute an original warrant and discover that an on-site search is simply not feasible.[107] It must not be based on generic, conclusory assertions about the time needed to copy and analyze the data on the computer system and/or about the need to seize data and equipment to prevent its destruction by "booby-traps" that could be installed on the system.[108] Conclusory allegations offered to obtain an authorization for an off-site search are analogous to conclusory allegations included in an application for a search warrant; in neither instance can the Magistrate

105. *See* People v. Gall, 30 P.3d 145, 160 (Colo. 2001) ("[T]he nature of the property seized under this warrant is particularly important, since computers, by their unique nature, raise special privacy concerns. Because computers process personal information and effects, they require heightened protection under the Fourth Amendment against unreasonable searches or seizures.").

106. *See infra* Part IV; Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 107 (1994). *See also* United States v. Tamura, 694 F.2d 591, 595–596 (9th Cir. 1982) ("In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the Government and law enforcement officials generally can avoid violating Fourth amendment rights by sealing and holding the documents pending approval by a Magistrate Judge of a further search, in accordance with the procedures set forth in the American Law Institute's Model Code of Pre-Arraignment Procedure. If the need for transporting the documents is known to the officers prior to the search, they may apply for specific authorization for large-scale removal of material, which should be granted by the Magistrate Judge issuing the warrant only where on-site sorting is infeasible and no other practical alternative exists . . . The essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached Magistrate. In the absence of an exercise of such judgment prior to the seizure in the present case, it appears to us that the seizure, even though convenient under the circumstances, was unreasonable."); A MODEL CODE OF PRE-ARRAIGNMENT PROCEDURE § 220.5 (1975) (requiring a special procedure where documents that are to be searched contain additional material not specified in the warrant).

107. *See infra* Part IV.

108. *See supra* Part II(C); Gall, 30 P.3d at 154 (officers seized computers and sought further warrants to authorize searching their contents).

Judge rely on general allegations without abrogating his or her duty to find facts and draw inferences independently.[109] The Magistrate Judge, not the officer, must make the determination that a seizure of computers and computer storage media is necessary, and, to do that, the Magistrate Judge must have specific facts from which he or she can make that determination.[110]

The officer applying for an off-site search authorization must, therefore, provide the Magistrate Judge with specific, detailed information about the suspect and the computer system at issue; information sufficient to allow the Magistrate Judge to make his or her own independent assessment as to whether an off-site search is reasonable under the circumstances.[111] An off-site computer search should be treated as an unusual measure, just as (but not for the same reasons) no-knock entries are treated as extraordinary measures.[112] Any requirement to seize computer hardware, software, or documentation must be addressed

---

109. *See* Aguilar v. Texas, 378 U.S. 108, 111 (1964); Nathanson v. United States, 290 U.S. 41, 47 (1933).

110. *See Aguilar*, 378 U.S. at 112.

111.

> [I]f agents expect that they may need to seize a personal computer and search it off-site to recover the relevant evidence, the affidavit should explain this expectation and its basis to the magistrate judge. The affidavit should inform the court of the practical limitations of conducting an on-site search, and should articulate the plan to remove the entire computer from the site if it becomes necessary. The affidavit should also explain what techniques the agents expect to use to search the computer for the specific files that represent evidence of crime and may be intermingled with entirely innocuous documents. . . .
>
> . . . .
>
> . . . [T]he affidavit should explain the techniques that the agents plan to use to distinguish incriminating documents from commingled documents.

FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS § II(C)(3) at 47–50 (2001) *available at* http://www.cybercrime.gov/searchmanual.pdf.

> The *Guidelines* do not require enough. The affidavit should be required to (a) specify the information they are searching for and the techniques they intend to use in an effort to find the evidence in as much detail as possible; and (b) return to the Magistrate Judge to obtain a supplemental warrant if their original search strategy proves unsuccessful. The requirement that the agents obtain a supplemental warrant is the best way of implementing Fourth Amendment policies in this context, since it ensures that the decision to broaden the scope of a search is made by the Magistrate Judge, not by the agents alone.

See MODEL CODE OF CYBERCRIMES INVESTIGATIVE PROCEDURE, art. VII § 4(f)(I) (1998) *at* http://www.cybercrimes.net/MCCIP/art7.htm.

112. *See* Richards v. Wisconsin, 520 U.S. 385, 394–95 (1997) (officers must have reasonable suspicion of danger or destruction of evidence to make no-knock entry); United States v. Tavarez, 995 F. Supp. 443, 446–47 (S.D.N.Y. 1998) (affidavit for warrant provided specific facts justifying no-knock entry).

separately in the application. Any such requirement for seizure must clearly describe both the basis for the seizure and the reason(s) the search and subsequent analysis cannot be conducted against a forensic copy of the computer system.[113] The decision to seize and to search off-site must be made by the Magistrate Judge issuing the warrant, and this requires that the Magistrate Judge be given specific information about what evidence the officers will be searching for.[114] The affidavit should

113. The United Kingdom recently adopted legislation that lets an officer seize an item if he has "reasonable grounds" to believe it may contain something for which he is authorized to search pursuant to a warrant. Criminal Justice and Police Act, 2001, c. 16 § 50 (Eng.), *at* http://www.hmso.gov.uk/acts/acts2001/20010016.htm (last visited Jan. 31, 2002). The act of copying property, including computer disks or files, constitutes a seizure. *Id*. at c. 63(1)(a). The officer can only seize the item if "in all the circumstances, it is not reasonably practicable for it to be determined" on the premises where the property was found, "whether what he has found is something that he is entitled to seize," or "the extent to which what he has found contains something that he is entitled to seize". *Id.* at c. § 50(1)(c). If the officer decides it is not reasonably practicable to make either determination on the premises where the property was found, the officer is allowed to "seize so much of what he has found as it is necessary to remove from the premises to enable that to be determined." *Id.* The officer is limited to the following factors to make the determination if it is reasonably practicable to seize the property:

> (a) how long it would take to carry out the determination or separation on those premises;
>
> (b) the number of persons that would be required to carry out that determination or separation on those premises within a reasonable period;
>
> (c) whether the determination or separation would (or would if carried out on those premises) involve damage to property;
>
> (d) the apparatus or equipment that it would be necessary or appropriate to use for the carrying out of the determination or separation; and
>
> (e) in the case of separation, whether the separation-would be likely, or if carried out by the only means that are reasonably practicable on those premises, would be likely, to prejudice the use of some or all of the separated seizable property for a purpose for which something seized under the power in question is capable of being used.

Id. at c. § 50(3).

114. The *Guidelines* suggest that agents seeking a warrant to search for and seize computer-generated evidence ask that the Magistrate Judge authorize the decision whether the search should be conducted off-site after the search has begun:

> Based upon your affiant's knowledge, training and experience, your affiant knows that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:
>
> (1) The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks) can store the equivalent of millions 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 par-

describe the computer systems that will be searched, the types of files that fall within the scope of the warrant (e.g., text files, data files, deleted files, images and video files), the methods (software and hardware) that will be used to search for this evidence,[115] the number of computers and

---

> ticular 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 and invasive to attempt this kind of data search on-site.
>
> (2) Technical Requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is 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 may be necessary to complete an accurate analysis. Further, such searches often require the seizure of 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.
>
> In light of these concerns, your affiant hereby requests the Court's permission to seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, *if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.*

GUIDELINES, app. F at 112 (emphasis added). This decision should not be left to the discretion of the agents executing the search but should be made by the Magistrate Judge because it is an essential part of describing the place to be searched and the items to be seized. *See* U.S. CONST. amend. Iv; *See also* FED. R. CRIM. P. 41(c)(1).

This requirement does not impose an onerous obligation on the agents. The agents can seek a supplemental warrant authorizing an off-site search (and defining the scope of that search) if they find searching on-site to be impracticable. However, the agents have probable cause to believe that circumstances at the search site make it dangerous to delay the search while seeking such a warrant, they can proceed with the search under the authority of an exception. *See* LAFAVE, *supra* note 86, § 6.5(b).

115.

> Paragraph 42 of the affidavit and application for the second warrant contained the following:
>
> The search procedure of the electronic data contained in computer operating software, hardware or memory devices will be performed in a controlled environment and may include the following techniques:
>
> (a) Surveying various file 'directories' and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

storage media the officers expect to search, the time they expect the search to consume, and any other facts unique to the execution of this warrant that support the issuance of an off-site authorization.[116] As to the standard for issuing such an authorization, reasonable suspicion to believe an off-site search is necessary is a logical choice, both because reasonable suspicion is the standard used to justify no-knock entries[117] and because one could analogize an off-site search to a stop authorized by *Terry v. Ohio*[118], in that the equipment is being detained for a limited period of time to let officers locate evidence of a crime.

When a court issues a seizure and an off-site search authorization, it should require that the officers create at least one back-up copy of the information on the seized equipment and give this back-up copy to the owner of that equipment. If the contents of the disk are such that the materials can not reasonably be left in possession of the owner, for example, agents seize child pornography, then a second sealed backup copy should be produced, and retained for use by defendant's counsel and experts. The sealed copy can be used to demonstrate whether the evidence was contaminated or tampered with after leaving the suspect's possession.

(b) "Opening" or reading the first few "pages of such files in order to determine their precise contents;

(c) "Scanning" storage areas to discover and possibly recover deleted data;

(d) "Scanning" storage areas for deliberately hidden files; and/or

(e) Performing keyword searches through all electronic storage areas to determine whether recurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

State v. Fink, No. 0005008005, 2001 WL 660105, at *4 (Del. Super. Mar. 30, 2001). *See* People v. Gall, 30 P.3d 145, 160 (Colo. 2001) (Martinez, J., dissenting) ("[A] warrant must include measures to direct the subsequent search of a computer's data.").

116. As the note above illustrates, one of the primary justifications for conducting searches off-site is the time required to analyze large amounts of data. *See supra* Part II(B). This is an issue that will only become more problematic, given the ever-increasing storage capacities of computer systems, so it is imperative that the legal system develop standards for determining when an off-site search is reasonable simply because of the amount of data that has to be processed. From the technical perspective, the least intrusive option is to prepare backups of the system on-site, and to perform the search and analysis off-site. In such instances it is vitally important that the warrant authorizing search of the computer(s) be specific as to the scope of the files to be searched, and the nature of the searches to be performed.

117. *See* Richards v. Wisconsin, 520 U.S. 385, 394 (1997) ("In order to justify a 'no-knock' entry, the police must have a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, . . . would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence."). There is no equivalent constitutional guarantee for on-site computer searches, the reasonable suspicion standard would be adequate protection.

118. 392 U.S. 1, 30 (1968) (allowing a limited search of a person if the officer has a reasonable and articulate suspicion of danger).

The court should also require that the suspect be given a detailed inventory of the hardware that is seized and of the data and files that are seized. These inventories should be supplied in addition to the back-up copies of any seized data. The inventories are not substitutes for back-up copies. For hardware, the inventory should include the quantity, description, and serial number(s) for any devices seized. For computer media or seized files the inventory should describe the type of media, capacity (if known), number seized, and a listing of the files contained on the media. This listing of files should detail, at a minimum, the file name, creation date, access date, file size, and the location of the file on the disk (either the full path of the file, or its absolute address on the disk). For any copy of media produced on-site, the defendant should be left with a CRC or MD5 hash value for the media so copied.[119]

The combination of the hash count and specific file information will serve to provide a detailed record of the property seized, and also to allow detection of any tampering or evidence contamination. The production of such file listings should not be burdensome, since these listings can easily be produced using the same tools that are used to preserve and examine computer based evidence. The CRC or MD5 hash sums can be produced using readily available software tools, and these checksums are built in to most backup software used by law-enforcement.

Regardless of whether the officers take the suspect's equipment with the "original" stored data contained thereon or satisfy themselves with a copy of that information, the court must set some parameters for what they can, and cannot, do in searching these data files. In the Doe & Doe hypothetical, for example, the officers searched for evidence that employees of the law firm were involved in perpetrating a complex insurance fraud scheme. The evidence, if any, of their involvement in these activities would consist of text files, alpha-numeric files, not graphics files. Therefore, the warrant should explicitly limit the scope of the officers' search of the Doe & Doe computer system and computer data files to text files. This should be done regardless of whether the search is conducted on-site, off-site using a back-up copy of data from the Doe & Doe computer files or is done off-site using seized Doe & Doe computer equipment.

119. Cyclic Redundancy Check (CRC) and Message Digest 5 (MD5) are techniques that use an algorithm to generate a unique digital signature called a hash value based on the contents of a computer file. The act of changing a single character in a file would result in the generation of a different hash value. Therefore, comparing CRC or MD5 hash values of the original file and a purported copy of that file is a quick and reliable way to detect whether the copy has been altered or tampered.

To ensure that the search does not go beyond permissible bounds, the warrant should specify that the officers are allowed to search for text files. The affidavit should include a description of exactly what text files means in this particular instance, and specify the software programs and analytical techniques the officers can employ in conducting this search.[120] If generalized tools are to be used, the warrant should describe what specific actions will be taken to limit the search to those files within the scope of the warrant. One way this can be accomplished is to stipulate that only files of the types specified within the warrant will be examined. This can be accomplished by using appropriate computer forensic tools to identify and isolate files based on the file type, and to exclude files that are outside the scope of the warrant from manual examination. These tools determine file types based on invisible character strings that are embedded in the file header, so they are not in any way dependent on the name of the file. Section IV discusses this issue in more detail, because it is really a matter of ensuring that officers do not impermissibly use the plain view doctrine to expand the scope of their search beyond reasonable limits.[121]

If the officers conducting an off-site search pursuant to a validly-issued warrant unexpectedly discover that they are confronted with intermingled files, some of which may be within the scope of the warrant and others of which may fall outside the scope of the warrant, they should not continue with their search.[122] Instead, the officers should return to the Magistrate Judge to seek a second, more specific warrant that specifies the scope and the methods the officers are to use in conducting a search of the intermingled files.[123]

---

120. *See* State v. Fink, No. 0005008005, 2001 WL 660105 at *4 (Del. Super. Mar. 30,2001); People v. Gall, 30 P.3d 145, 160 (Colo. 2001) (Martinez, J., dissenting).

121. *See infra* Part IV.

122. *See* United States v. Campos, 221 F.3d 1143, 1147–1148 (10th Cir. 2000); United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999); United States v. Barbuto, No. 2:00CR197K, 2001 WL 670930 *5 (C.D. Utah Apr. 12, 2001).

123.

> Because the agents who testified at the evidentiary hearing on Defendant's motion to suppress had no knowledge of the search methods or criteria used by the agents who searched the computers, the United States has offered to provide additional testimony regarding such methods. However, this court concludes such methods or criteria should have been presented to the magistrate before the issuance of the warrants or to support the issuance of a second, more specific warrant once intermingled documents were discovered.

Barbuto, 2001 WL 670930 at *5. The *Barbuto* court suppressed documents seized from the defendant's computers, including his personal journal, because it found that when the agents were faced with intermingled documents, such as Defendant's personal journal, the agents did not return for further instructions or a more specific warrant from the magistrate. The

The warrant should also specify a time frame for conducting the search. Magistrate Judges have imposed time limits on computer searches.[124] This is the correct approach as the Supreme Court has held that the length of time in which property is seized for the purposes of being searched is a factor that bears directly on the reasonableness of that seizure.[125] The Department of Justice, on the other hand, takes issue with this approach, arguing that "[t]he law does not expressly authorize magistrate judges to issue warrants that impose time limits on law enforcement's examination of seized evidence."[126]

This argument erroneously equates off-site computer searches to conventional searches and seizures. In conventional searches and seizures, the execution of a warrant typically involves two stages: a "search" for evidence that is followed by the "seizure" of evidence once it has been found. Absent a court's granting a motion for the return of property lawfully seized pursuant to this process, law enforcement will be allowed to retain and analyze that property as long as is necessary. This may last until after a trial and conviction, until after a plea of guilty, until after a plea or conviction has been upheld on appeal or for an indeterminate period. If the property is contraband, it will never be returned. If the seized property is mere evidence, then the property can be retained, absent a successful motion for its return, for as long as the legitimate needs of law enforcement require. But this is property that has been lawfully seized pursuant to the authority of a warrant that was completely executed. A Magistrate Judge's authority ends once the execution of a warrant is complete.

In off-site computer searches, the execution of a warrant involves four stages, not two: a *search* designed to locate computer equipment; the *seizure* of that equipment and its removal to another location; a thorough *search* of the contents of the equipment which is conducted at that location; and a *seizure* of relevant evidence located in the course of that search. Here, the initial *seizure* of the equipment is simply a preliminary

document displayed on the computer screen at Defendant's home that led the agents to seek warrants to search the computers was an intermingled "To Do" list of Defendant's daily activities. The agents should have known that the warrant needed to specify what types of files were sought in searching the two computers so that personal files would not be searched.

124. United States v. Brunette, 76 F. Supp. 2d 30, 42 (D. Me. 1999) (suppressing evidence not reviewed within the time period set forth in the warrant and extension granted). *See* FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS S II(D)(2) at 52 (2001) *available at* http://www.cybercrime.gov/searchmanual.pdf.

125. *See* United States v. Place, 462 U.S. 696, 709–10 (1983).

126. *See* GUIDELINES, § II(D)(2) at 52http://www.cybercrime.gov/searchmanual.htmIId2. *See also* United States v. Hernandez, ___ F. Supp. 2d ___, 2002 WL 32702, No. CRIM. 01-635 (SEC), at * 10 (D.P.R. Jan. 4, 2002) ("Neither Fed. R. Crim. P. 41 nor the Fourth Amendment provides for a specific time limit in which a computer may undergo a government forensic examination after it has been seized pursuant to a search warrant.").

stage in the execution of the warrant; the execution of the warrant is not completed until the equipment has been *searched* off-site and identified evidence seized from the property. The Magistrate Judge who issued the warrant has the authority to set conditions governing the execution of the warrant—including the *search* which will be conducted off-site. The Magistrate Judge can, therefore, impose time limits and other constraints on the conduct of the off-site search. The Magistrate Judge's authority to do so derives from Rule 41 of the Federal Rules of Criminal Procedure[127] and from the court's inherent power to issue a warrant whenever the requirements of the Fourth Amendment are met.[128] The imposition of time limits is required because "[i]f the police were allowed to execute the warrant at leisure, the safeguard of judicial control over the search which the fourth amendment is intended to accomplish would be eviscerated."[129]

In addition to specifying a time frame for conducting an off-site computer search, the warrant should require that officers examine the seized equipment as soon as possible to determine if all or part of the equipment can be returned to its rightful owner.[130] This is especially

127. Fed. R. Crim. P. 41(c)(1) (Warrant "shall command the officer to search, within a specified period of time not to exceed 10 days . . . ."). *But see* United States v. Koelling, 992 F.2d 817, 823 (8th Cir. 1993) (upholding the practice of issuing an anticipatory warrant which ties the execution of the warrant to a specific event); United States v. Garcia, 882 F.2d 699, 702–703 (2nd Cir. 1989) (upholding anticipatory warrants). Therefore, a Magistrate Judge can also exercise this authority to set time limits governing the off-site search of seized computer equipment.

128. *See* United States v. Villegas, 899 F.2d 1324, 1334 (2nd Cir. 1990) ("Obviously the Fourth Amendment long antedated the Federal Rules of Criminal Procedure . . . . Given the Fourth Amendment's warrant requirements, and assuming no statutory prohibition, the courts must be deemed to have inherent power to issue warrant when the requirements of that Amendment are met."); Therefore, even if one assumed that Rule 41 does not authorize a Magistrate Judge to set time limits for the process of conducting an off-site search of seized computer equipment, the reservoir of inherent power identified by the *Villegas* court does confer such authority.

129. United States v. Bedford, 519 F.2d 650, 655 (3rd Cir. 1975). *See* United States v. Shegog, 787 F.2d 420, 422 (8th Cir. 1986). *See also* United States v. Rowland, 145 F.3d 1194, 1201–1202 (10th Cir. 1998) (holding that a condition precedent is necessary for an anticipatory warrant because it "not only insures against premature execution of the warrant, but also maintains judicial control over the probable cause determination and over the circumstances of the warrant's execution."(citations omitted)); United States v. Ricciardelli, 998 F.2d 8, 12 (1st Cir. 1993) (noting the need to place limits on anticipatory warrants to prevent possible abuse); United States v. Garcia, 882 F.2d 699, 703–704 (2nd Cir. 1989) (stating a warrant needs to be explicit, clear, and narrowly drawn to avoid potential abuse); State v. Womack, 967 P.2d 536, 543–544 (Utah App. 1998).

130.

> It shall be the duty of the person for the time being in possession of the seized property in consequence of the exercise of that power to secure that there are arrangements in force which . . . ensure—

appropriate when the justification for the seizure is that the equipment contains commingled evidence and, therefore, it is not possible to determine, on-site, which files fall within the scope of the warrant and which do not. It is also appropriate when the possibility exists that the seized equipment contains evidence that is encompassed by a valid privilege; absent countervailing considerations, the privileged material should be returned to the rightful owner as soon as possible.[131] The Magistrate Judge may want to give the owner of the seized property the opportunity to be present at, or have a representative present at, this examination.[132]

Finally, when executing computer searches officers may give the owner of the equipment/data the option of (a) having the officers search on-site or (b) letting the officers make back-up copies of the information contained on the system which will then be searched off-site. The option is offered in the interest of expediting the searching and seizing of evidence as authorized by the search warrant. The second option comes with a condition, namely, that the owner[133] of the equipment/data must execute a stipulation in which he or she (a) concedes that the back-up copies are complete and accurate copies of the file contents of the systems searched as of the date in question and (b) agrees not to challenge the accuracy or reliability of the back-ups or of any evidence retrieved

---

> (a) that an initial examination of the property is carried out as soon as reasonably practicable after the seizure;
>
> (b) that that examination is confined to whatever is necessary for determining how much of the property falls within subsection (3);
>
> (c) that anything which is found, on that examination, not to fall within subsection (3) is separated from the rest of the seized property and is returned as soon as reasonably practicable after the examination of all the seized property has been completed; and
>
> (d) that, until the initial examination of all the seized property has been completed and anything which does not fall within subsection (3) has been returned, the seized property is kept separate from anything seized under any other power.

Criminal Justice and Police Act, 2001, c. 16 § 53(2) (Eng.), *at* http://www.hmso.gov.uk/acts/acts2001/20010016.htm (last visited Jan. 31, 2002) (Clause (3) provides for the retention of property that was properly seized as falling within the scope of the original warrant or that property that is not reasonably practicable to separate from property falling within the scope of the warrant).

131. *See id*. at c. 16 § 54(1) (establishing a duty to return items subject to legal privilege to the owner as soon as reasonably practicable after the seizure).

132. *See id.* at c. 16 § 53(4) ("due regard shall be had to the desirability of allowing the person from whom [the equipment] was seized, or a person with an interest in that property, an opportunity of being present or (if he chooses) of being represented at the examination"). *See also infra* Part IV *See generally* United States v. Abbell, 914 F. Supp. 519 (S.D. Fla. 1995).

133. For businesses, the stipulation can be executed by an authorized agent.

from them.[134] The use of these stipulations needs to be analyzed very carefully, since someone executing such a stipulation waives any and all rights to challenge the admissibility of evidence obtained from the back-ups. Such waivers can be problematic for various reasons, some technical, some legal.

Technically speaking, a stipulation such as this is inadvisable because it is necessarily made on incomplete information. The person executing the stipulation probably has no idea what techniques the officers will use to create the back-ups; this person certainly has no way of knowing what techniques will be used to retrieve and analyze the data once it arrives at the police laboratory and no way of monitoring that process. There is no easy way that the person executing the stipulation can ascertain that the backup is either complete or accurate. Allowing the suspect to observe the copy operation and examine any resultant reports is only helpful if they are familiar with the software used to create the backup. Depending on how files or media are copied, the resultant copy might not include all files from the original media, or might misrepresent the original organization of the files. Media read errors, which might prevent the backup copy from being complete, would not be readily evident until the media is actually read during subsequent copy or search activity. Even assuming the backup copy was complete, the copy might still be inaccurate. Depending on how files are copied important forensic evidence may be lost. At a minimum, improper copying may fail to preserve deleted files and file creation and access dates.

The suspect is generally not in a position to verify that the copy is an accurate, and even if the copy is accurate at the time it is created, it may not reflect the contents of the computer at the point in time when the search began. This is especially true when the investigating officers have made any attempt to access individual files before the computer system was backed up. By way of example, if the officers conducting the search have opened files to review their contents, the officers will have altered the record of when those files were last accessed and may even have altered the contents of the file. If one of the files opened was infected with a destructive virus, the act of opening the file might also result in the deletion of files or destruction of data. Subsequent examination of the computer system might lead one to erroneously conclude that the system had been deliberately "booby-trapped" or sanitized by the suspect, even though no such suspicious activity actually occurred.

134. *Cf.* United States v. Orefice, No. 98 CR. 1295(DLC) 1999 WL 349701 (S.D.N.Y. May 27, 1999).

Other situations may also cause the contents of a computer to change while a search is in progress. Changes may be caused by activity on the part of other users who have access to the computer via a network or modem connection, changes that are induced by programs running on the computer, and changes caused by automated tasks (such as housekeeping tasks) that are triggered by time-of-day or system events. Given these technical considerations, such stipulations to accept the accuracy or reliability of the copy are inadvisable.

A stipulation to search also has serious legal ramifications. These stipulations resemble a consent to search. When someone consents to a search, they agree to let officers enter an identified area and search for evidence, until the suspect withdraws his or her consent.[135] The off-site search stipulations superficially resemble consents to search because an owner of computer equipment who executes a stipulation enters into an agreement with officers that facilitates the officers carrying out a search. But these stipulations differ from consents to search in two ways. First, rather than authorizing a search from the outset, the suspect simply approves a change in the way the search is carried out (off-site as opposed to on-site). Second, someone who consents to search still retains the ability to challenge the validity or accuracy of evidence discovered during that search, but when someone executes one of these stipulations, he or she is waiving any right to object to having evidence retrieved from the back-ups used against him or her.

Therefore, these computer search stipulations can be analogized to a consent to search or to a stipulation allowing incriminating evidence to be admitted. To be valid, a consent to search must be made voluntarily.[136] An individual's execution of a stipulation allowing the use of incriminating evidence must be made voluntarily and knowingly.[137]

Either alternative would therefore require that an off-site computer search stipulation be executed voluntarily for the stipulation to be enforceable. Both alternatives use the same test for determining voluntariness, borrowing a test developed to decide whether confessions can be used without violating due process.[138] Due process requires that a confession cannot be used if it was given involuntarily. A confession will

135. *See* LAFAVE, *supra* note 86, § 8.1.

136. *See* Ohio v. Robinette, 519 U.S. 33, 40 (1996); Schneckloth v. Bustamonte, 412 U.S. 218, 222–27 (1973). *See* also MODEL CODE OF CYBERCRIME INVESTIGATIVE PROCEDURE, art. VII § 6(b)(I) (1998) *at* http://www.cybercrimes.net/MCCIP/art7.htm.

137. *See* Bonilla-Romero v. United States, 933 F.2d 86, 88 (1st Cir. 1991); United States v. Cozine, 21 M.J. 581, 584 (A.C.M.R. 1985).

138. *See Schneckloth*, 412 U.S. at 227; *Cozine*, 21 M.J. at 584; LAFAVE, *supra* note 86, § 8.2.

be deemed to have been given voluntarily if it was the product of the suspect's free will, uncoerced by the actions of law enforcement officers.[139] A confession will, on the other hand, be deemed to have been given involuntarily if the officers offered the suspect a *quid pro quo*, such as the opportunity to avoid physical harm or a promise of leniency, in exchange for confessing.[140]

Consent searches arise in varied contexts, but the most precise analogy to the off-site computer search stipulation is to the situation in which officers give a suspect a choice. The suspect can choose to consent to the officers' search without a warrant or to wait until the officers obtain a warrant. Courts have held that consents given in this situation are voluntary, absent the presence of some other coercive factor(s).[141] The stipulation used in computer searches presents an analogous situation. In stipulating to an off-site computer search the owner of the property to be searched chooses between having the search conducted on-site or having it conducted off-site (incrementally surrendering the chance to challenge the admissibility of the evidence recovered). This argument implicitly assumes that in both instances the owner of the property surrenders some legal protection in exchange for convenience. In the pure consent scenario, the person surrenders his or her right to have the search conducted pursuant to a warrant in exchange for not waiting while the officers obtain the warrant. While in the computer search scenario, the person surrenders his or her rights (a) to have the search conducted on-site[142] and (b) to challenge the use of the evidence in exchange for not having the officers conduct their search on-site.

The problem is that while the situations are superficially similar, they are not precise analogues. In the pure consent search scenario, the person consenting is choosing between two equivalents (a search conducted under the aegis of consent or a search conducted under the aegis of a warrant). In the computer search scenario, however, the person executing the stipulation is not choosing between equivalents. The choice is between two different kinds of Fourth Amendment intrusions while striking a different, less advantageous bargain. For the two situations to be precise analogues, in the computer search context, the owner of the property would have to be given the alternatives of consenting to have the officers conduct the search off-site or waiting until they obtain a

139. *See* Colorado v. Connelly, 479 U.S. 157, 167 (1986); LAFAVE, *supra* note 86, § 8.2.

140. *See* Dickerson v. United States, 530 U.S. 428, 433–35 (2000); United States v. Dillon, 150 F.3d 754, 757–758 (7th Cir. 1998).

141. *See* LAFAVE, *supra* note 86, § 8.2.

142. Assuming the officers need the owner's consent to search off-site because the officers' warrant does not authorized an off-site search.

warrant authorizing an off-site search. This is not the bargain someone executing one of these stipulations confronts. The bargain the stipulations offer is to either have the officers conduct the search on-site or consent to an off-site search surrendering one's right to challenge the admissibility of any evidence discovered during the off-site search.

Due to the lack of equivalence, the latter situation is problematic. It is a voluntariness problem. Instead of exchanging equivalents, the owner of the property is engaging in a one-sided bargain with the officers, from which it might be inferred that the officers (may) exploit the intrusiveness and inconvenience of searching on-site to coerce the property owner into executing the stipulation. The permissibility of this inference is significantly enhanced if the officers obtain such a stipulation when the warrant already authorizes an off-site search. If it does authorize an off-site search, the owners are trading something for nothing. The owner is trading the right not to object to the admissibility of recovered evidence for something the officers already have permission to do. It is, to a lesser extent, enhanced if the warrant does not authorize an off-site search. For the reasons explained in the previous section the officers may very well find it easy to obtain a supplemental warrant authorizing an off-site search but may not want to go to the trouble of obtaining a supplemental warrant, and may exploit this opportunity to persuade the owner to waive the right to challenge the admissibility of any evidence the officers recover.

The stipulations raise another issue, one which implicates the consequences of the choice, rather than the voluntariness of the choice. It is likely that the person who executes a stipulations does not fully understand what he or she surrenders when agreeing not to challenge the admissibility of evidence discovered during the off-site search. Therefore, the stipulation raises the issue of whether or not the decision to execute the stipulation was made knowingly. As noted above, courts have held that an individual's execution of a stipulation allowing the use of incriminating evidence must be made voluntarily and knowingly.[143] The person executing the stipulation acts knowingly in that he or she realizes there is a choice. The choice is between the execution of the stipulation or having to endure an on-site search. But the owner may not act knowingly in terms of realizing the consequences of his or her actions.

The owner's failure to realize the consequence of his or her actions has two elements. First, there is a failure to realize the consequences surrendering evidentiary objections can have at a trial based on evidence discovered during the search. Second, there is a failure to realize that the

143. *See supra* note 136.

methods used to conduct the off-site search could provide the factual predicate for objections to the admissibility of the evidence. While the consequences of a stipulation of this type may not be sufficiently weighty to require an inquiry analogous to that conducted under Fed. R. Crim. P. Rule 11(c)(3),[144] the stipulations do raise potential due process concerns about fairness and overreaching.[145]

These stipulations are sufficiently problematic for the technical and legal reasons set out above that they should not be used. Only a Magistrate Judge should be allowed to authorize an off-site search, such authorization to be contained either in the original search warrant or in a supplemental warrant. Until this alternative is implemented, courts dealing with a challenge to one of these stipulations should inquire closely into the circumstances under which the off-site search was executed.

III. THE PLAIN VIEW DOCTRINE AND COMPUTER SEARCHES

The plain view doctrine is an exception to the general rule that a warrant is required to make a seizure reasonable under the Fourth Amendment.[146] The doctrine allows evidence to be used even though it was seized by an officer who acted without the authorization of a search warrant.[147] Under the plain view doctrine, an officer can lawfully seize evidence of a crime without a warrant if three conditions are met:

> The officer was lawfully in a position from which to view the object seized. The officer did not violate the Fourth Amendment interest in privacy by observing the object.
>
> The object's incriminating character was immediately apparent. By simply viewing the object the officer had probable cause to believe it was evidence of a crime; and
>
> The officer had a lawful right of access to the object. The officer could approach the object and seize it without violating a Fourth Amendment interest in privacy or possession.[148]

144. *See* Fed. R. Crim. P. Rule 11(c)(3) (requiring that the person executing a stipulation acted voluntarily and knowingly). *See also* United States v. Lyons, 898 F.2d 210, 214–215 (1st Cir. 1990).

145. *See* Brookhart v. Janis, 384 U.S. 1, 8–9 (1966) (separate opinion of Harlan, J.).

146. *See* WAYNE R. LAFAVE, 1 SEARCH AND SEIZURE § 2.2 (3d ed. 1996).

147. *Id.*

148. *See* Horton v. California, 496 U.S. 128, 134 (1990); Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971). *See also* LAFAVE, *supra* note 146, § 2.2.

> The plain view doctrine only justifies the seizure of an object. The doctrine does not justify a search, however minimal.[149]

The plain view doctrine, predicated on aspects of physical reality,[150] has been invoked to justify searches involving the cyberworld. The plain view doctrine has been used as a justification for officers searching a computer hard drive or other computer media for specific evidence and seizing evidence that was not encompassed by the warrant.[151]

In *United States v. Carey*,[152] officers were searching the hard drives of two computers pursuant to a warrant that authorized a search for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances."[153] While conducting a key-word search of text files that was designed to locate the information identified in the warrant, one officer—Detective Lewis—discovered JPEG or image files.[154] He copied the JPEG files and used different software to view the images and found child pornography.[155] Carey challenged the search, arguing that it exceeded the scope of the warrant.[156]

---

149. *See* Arizona v. Hicks, 480 U.S. 321 (1987).

150. *See generally* LAFAVE, *supra* note 146, § 2.2.

151. *See* United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (finding subdirectories in suspect's computer which contained child pornography were within plain view of agent who was executing warrant authorizing search for evidence of hacking and who opened subdirectories in the course of searching for such evidence); State v. Fink, No. 0005008005, 2001 WL 660105 (Del. Super. Mar. 30, 2001) (denying a motion to suppress in finding that the officer's opening of computer files was done to search for evidence described in the warrant, therefore the discovery of child pornography was inadvertent and lawful under the plain view doctrine); State v. Schroeder, 613 N.W.2d 911 (Wis. App. 2000) (finding that images of child pornography found while searching defendant's computer that was seized pursuant to warrant for evidence of online harassment were in plain view). *But see* United States v. Turner, 169 F.3d 84, 88–89 (1st Cir. 1999) (rejecting the government's attempt to use the plain view doctrine to justify a search for JPEG file conducted after the suspect consented to a search of his apartment for evidence of an intruder and/or a sexual assault); United States v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996) (plain view doctrine did not apply to search of computer files under a screen-name not listed in warrant).

152. 172 F.3d 1268 (10th Cir. 1999).

153. *Id*. at 1270.

154. *Id*. at 1271 ("[The officer's]method was to enter key words such as, 'money, accounts, people, so forth' into the computer's explorer to find 'text-based' files containing those words. This search produced no files 'related to drugs.' ").

155. *Id.* at 1270–1271.

156.

> Mr. Carey moved to suppress the computer files containing child pornography. During the hearing on the motion, Detective Lewis stated although the discovery of the JPG [sic] files was completely inadvertent, when he saw the first picture containing child pornography, he developed probable cause to believe the same kind of material was present on the other image files. . . .

Detective Lewis admitted at the suppression hearing that he had no idea what the JPEG files contained until he opened the files.[157] The government claimed the detective's actions were authorized by the plain view doctrine.[158] The government maintained that a computer search such as the one undertaken in this case is tantamount to looking for documents in a file cabinet pursuant to a valid search warrant. The seizure of the pornographic computer images was permissible because officers had a valid warrant, the pornographic images were in plain view, and the incriminating nature was readily apparent as the photographs depicted children under the age of twelve engaged in sexual acts. The warrant authorized the officer to search any file because " 'any file might well have contained information relating to drug crimes and the fact that some files might have appeared to have been graphics files would not necessarily preclude them from containing such information.' "[159]

The Tenth Circuit disagreed, explaining that:

> [t]he government's argument the files were in plain view is unavailing because it is the contents of the files and not the files themselves which were seized. Detective Lewis could not at first distinguish between the text files and the JPG files upon which he did an unsuccessful word search. Indeed, he had to open the first JPG file and examine its contents to determine what the file contained. Thus, until he opened the first JPG file, he stated he did not suspect he would find child pornography. At best, he says he suspected the files might contain pictures of some activity relating to drug dealing.

> Upon further questioning by the government, Detective Lewis retrenched and stated until he opened each file, he really did not know its contents. Thus, he said, he did not believe he was restricted by the search warrant from opening each JPG [sic] file. Yet, after viewing a copy of the hard disk directory, the detective admitted there was a 'phalanx' of JPG [sic] files listed on the directory of the hard drive. He downloaded and viewed these files knowing each of them contained pictures. He claimed, however, 'I wasn't conducting a search for child pornography, that happened to be what these turned out to be.'

Id. at 1271.

157.

> Detective Lewis later testified at the time he discovered the first JPG [sic] or image file, he did not know what it was nor had he ever experienced an occasion in which the label 'JPG' [sic] was used by drug dealers to disguise text files. He stated, however, image files could contain evidence pertinent to a drug investigation such as pictures of 'a hydroponic growth system and how it's set up to operate.'

Id. at 1270 n.2.

158. *Id.* at 1272.

159. *Id.* at 1272 (quoting Erickson v. Commissioner of Internal Revenue, 937 F.2d 1548, 1554 (10th Cir. 1991)).

> In his own words, however, his suspicions changed immediately upon opening the first JPG file. After viewing the contents of the first file, he then had "probable cause" to believe the remaining JPG files contained similar erotic material. Thus, because of the officer's own admission, it is plainly evident each time he opened a subsequent JPG file, he expected to find child pornography and not material related to drugs. Armed with this knowledge, he still continued to open every JPG file to confirm his expectations. Under these circumstances, we cannot say the contents of each of those files were inadvertently discovered. Moreover, Detective Lewis made clear as he opened each of the JPG files he was not looking for evidence of drug trafficking. He had temporarily abandoned that search to look for more child pornography, and only "went back" to searching for drug-related documents after conducting a five-hour search of the child pornography files.
>
> We infer from his testimony Detective Lewis knew he was expanding the scope of his search when he sought to open the JPG files. Moreover, at that point, he was in the same position as the officers had been when they first wanted to search the contents of the computers for drug related evidence. They were aware they had to obtain a search warrant and did so. These circumstances suggest Detective Lewis knew clearly he was acting without judicial authority when he abandoned his search for evidence of drug dealing.[160]

Other courts have reached the opposite conclusion in cases with almost identical facts.[161] In *State v. Schroeder*,[162] officers were investigating a case on online harassment and obtained a warrant to seize Schroeder's computer and search it for evidence that he had posted the harassing messages.[163] While searching for evidence showing Schroeder was the harasser, the officer conducting the search, Marty Koch, found pornographic pictures of children.[164] These pictures, and other pornographic

160. *Id.* at 1273. *But see* United States v. Wolfe, No. 00-5045, 2000 WL 1862667 at *1 n.2 (10th Cir. Dec. 20, 2000) ("*Carey* does not foreclose an argument that agents searching pursuant to a warrant for counterfeit currency templates, some of which could conceivably have computer graphics-type file extensions such as .GIF or .JPG, would inevitably have uncovered computer graphics files of the type at issue in this case during the course of the search.").

161. *See supra* note 150.

162. 613 N.W.2d 911 (Wis. App. 2000).

163. *Id.* at 913.

164. *Id.* at 913–14.

pictures discovered in Schroeder's computer, were used to charge him with possessing child pornography. Schroder moved to suppress the pornographic images, arguing that Koch's search exceeded the scope of the original warrant.[165] The Wisconsin court rejected his argument, finding that Koch's activities fell within the plain view doctrine.

> Koch testified that when he searches a computer he systematically goes through and opens user-created files, regardless of their names. This makes sense, as the user is free to name a file anything. Were Koch to limit his search to files whose names suggested the type of evidence he seeks, it would be all too easy for defendants to hide computer evidence: name your porn file '1986.taxreturn' and no one can open it. While systematically opening all user-created files, Koch opened one that contained images that he considered child pornography. At that point, he stopped his search. . . . He did not resume his search and find the rest of the nude images of children until after a second search warrant had been issued. Thus, his initial discovery of child pornography was when he opened a file and saw a nude picture of a child pop up on the screen. It was in plain view. This was no different than an investigator opening a drawer while searching for drugs and seeing a nude picture of a child on top of a pile of socks. The first element of the plain view test is satisfied. Regarding the second and third prongs, it is undisputed that Koch had a warrant to search the computer for evidence of harassment and that the first image Koch found could reasonably be viewed, on its face, as child pornography. The plain view doctrine applies.[166]

As these two cases illustrate, trying to apply the plain view doctrine to computer searches is not a simple matter. In rejecting the government's attempt to rely on the plain view doctrine, the *Carey* court noted that "the question of what constitutes 'plain view' in the context of computer files is intriguing and appears to be an issue of first impression for this court, and many others . . . ."[167] Because the applicability of the plain

165. *Id.* at 915–16.

166. *Id.* at 916. *See supra* note 150. *See also* State v. Fink, No. 0005008005, 2001 WL 660105, at *3 (Del. Super. Mar. 30, 2001) (denying a motion to suppress evidence of child pornography, the incriminating nature of which was immediately apparent, an officer inadvertently discovered while conducting search of computer files authorized by warrant).

167. *Carey*, 172 F.3d at 1273. The court also stated that analogizing the information contained on computers and computer storage media to "closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.' " *Id.* at 1275 (citations omitted).

view doctrine to computer searches presents a variety of complex and generally unexplored issues, courts need to consider whether the doctrine can reasonably be transposed to the cyberworld, and there used to expand the scope of a search conducted pursuant to a search warrant or pursuant to an exception to the warrant requirement.[168]

The plain view doctrine is predicated on the empirical concept of visual observation, of sight, as it functions in the physical world. In the physical world, sight is essentially a zero sum phenomenon. When an officer steps into a room for the purpose of executing a search warrant, the items in that room are either in sight or out of sight. Sight in the physical world is an unambiguous phenomenon, one that neither requires nor lends itself to the development of guidelines stating how it is to be employed. It would be absurd and impossible for a warrant to specify what officers can and cannot observe when they enter premises to execute the warrant. Items that are sitting on a table, for example, are in the officer's sight. It would be neither reasonable nor practicable to require the officer to pretend he or she did not see those items. In this context, the plain view doctrine is both eminently reasonable, given the concerns underlying the Fourth Amendment's prohibitions, and easily implemented.

In the cyberworld, on the other hand, there is no analogue of real world sight. As the facts in *Carey* illustrate, searches of computer-files are method-specific.[169] As long as the officer is using a text-based search program, the contents of non-textual files, such as JPEG files, will be opaque to him, clearly not in plain view. To use the example given in the previous paragraph, it is as if the officer had entered a room containing a series of computer files. As the officer uses the software program to search text files, the contents of all text files on the computer's hard drive are in the officer's sight, but the contents of the non-textual files, the JPEG files, are not. The JPEG files are of course visible to the officer, but they are analogous to a closed and locked box. In order to view the contents of the locked box, an officer would have to obtain the implements to unlock and then open the box. Unlocking and opening the box would, for the reasons noted earlier, be a search, and so, outside the scope of the plain view doctrine.[170]

Due to the encoded nature of computer data, textual and visual information stored in computer files can only be viewed through the

168. *See supra* note 150.

169. *See* New Technologies, Inc., *TextSearch Plus*, *at* http://www.secure-data.com/txtsrchp.html (last visited Oct. 3, 2001) (detailing a program used for such searches).

170. *See* Arizona v. Hicks, 480 U.S. 321 (1987).

intermediary of computer software. When the officer enters a computer to be searched, the only information that is truly visible is displayed on the computer screen when the search begins. To examine the other contents of the computer, the officer must first look in file directories and sub-directories, commonly represented as a series of nested folders (analogous to a series of store-rooms) to locate specific files of interest. The officer must then open the individual files (analogous to opening individual boxes contained within the store-rooms) to inspect the contents of the files.

The contents of a typical desktop computer are poorly organized. A single computer may contain thousands of files, which are stored in a hierarchy within hundreds of nested directories. A single directory can contain hundreds of individual files, with textual and graphic images intermingled. File names, and even file-type suffixes, are not a reliable indicator of file contents, so the officer entering the computer is faced with the choice of examining thousands of individual files, or using some form of search technique to locate the specific files most likely to contain evidence.[171]

In common practice, some form of systematic approach, such as the use of software that allows an officer to search for specific textual words or names, or to identify specific file types, helps the officer to identify files of interest. In the field of computer forensics, the systematic identification of files of interest based on some particular content or characteristic is commonly termed a *search*.

Keyword searches differ from their physical counterpart in one very important way, the officer using a keyword search does not inspect the contents of a file himself. The officers merely use a software program to identify files that might be relevant to inspect. From the technical view point, the closest physical-world analogy to these computer searches are the searches officers conduct using the assistance of a trained dog. Just as a trained dog may identify boxes that *potentially* contain contraband, the software searches identify files that *potentially* contain textual evidence of a particular crime. In order to determine the actual contents of a box (or file), it must be opened, and the contents examined. In the field of computer forensics, this examination is commonly termed a *review* or *assessment*.

In the case of computer files, the box must be opened with a program that can render its contents comprehensible. The review of textual files requires that they must be opened with programs that can format

171. *See* State v. Fink, No. 005008005, 2001 WL 660105 at *3 (Del. Super. Mar. 30, 2001).

and display text. Files containing visual images must be opened with software that can render the image visible on the user's screen. Some content, such as web pages or PowerPoint presentations, require special software that can properly represent data containing both text and images.

Even assuming files buried in nested sub-directories are in plain view, it is difficult to apply the plain view doctrine to files that must receive special treatment before the files can be searched. Files stored on a computer may be compressed, encrypted, or password protected. Such files do not lend themselves to simple automated searches. Special steps or tools may be required to render their contents visible to the search tool. Files containing images, video, or sound also present special problems. There is no search software to search for specific visual or audio data content. (It is possible to identify files that contain visual or audio data, but not to do content specific searches. Files containing child pornography cannot be distinguished from photos of a family pet unless the files are opened and viewed.)

Deleted files also present an additional layer of technical complexity. The normal use of a computer results in a wealth of deleted files and e-mails, many of which are created without the knowledge of the computer user. Some of these files can be observed by simply opening the appropriate recycle or trash directory. Others may only be observed after special software or processes are used to recover them. It is unclear what the status of such files should have, with respect to the plain view doctrine.

One way of preserving the concept of the plain view doctrine for computer searches while maintaining the integrity of the Fourth Amendment's right to privacy implication, is to tie "cyberplain view" to specific search methods which are set out in warrants authorizing computer searches.[172] This principle can be applied to the facts in *Carey.* The warrant in *Carey* authorized the officer to search files on Carey's computer that could contain evidence of his involvement in drug-dealing. Evidence such as "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances."[173] Files containing this type of evidence would be textual files, so the method the officer could use for the search would be limited to software that lets him search and review the contents of text files, and only text files. This would prevent the officer from doing what

172. *See* United States v. Abbell, 914 F. Supp. 519, 521 (S.D. Fla. 1995) (ordering a specified method to be used in searching computer files seized from law office).

173. 172 F.3d at 1270.

Detective Lewis did in *Carey*, namely, broadening the scope of his search by using different software. Software designed to open non-text files are clearly not encompassed by the scope of the officer's warrant.

Using the analogy developed above, the text-search software program would define the scope of the officer's sight when he was inside the computer's hard drive. Those files in plain view of that circumscribed variety of sight would be encompassed by the plain view doctrine, and the officer could seize those files without a warrant. Assume that while the officer was using the software program to search Carey's textual files for evidence of drug-dealing he discovered a text file containing Carey's detailed plan to rob a local bank. Depending on how immediately apparent the incriminating nature of the plan was, the information contained in that file could be encompassed by the plain view doctrine, since the officer was occupying a lawful Fourth Amendment vantage point when he/she observed the information. The information would not be in plain view if the officer had to scroll through the file, reading most of it to ascertain its incriminating nature, but would be in plain view if its incriminating nature was immediately apparent, or apparent as soon as the officer viewed an initial portion of the file.

The practice of limited reviews is not circumscribed to text files. Other techniques could be used to limit the scope of review to files of certain types (based on the invisible file signature), files created or modified within certain date ranges, (based on dates maintained by the operating system), or files controlled by a certain individual or department (based on access privileges defined by the computer's security system.) For instance, if the intent of the warrant was to permit only a review of graphics images, then file type could be used to block textual files from review.

What happens if an officer, while executing a warrant authorizing a search of text-based files, discovers evidence that gives her probable cause to believe other files, files that do not fall within the scope of her warrant, contain evidence of criminal activity? The plain view doctrine will not let her proceed because she cannot confirm or deny that belief without opening the files to search them, and the plain view doctrine only justifies seizures, not searches.[174]

174. *See* Hicks, 480 U.S. at 325–29. *See also* FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS § I(C)(3) at 18 (2001) *available at* http://www.cybercrime.gov/searchmanual.pdf ("[T]he plain view exception cannot justify violations of an individual's reasonable expectation of privacy. The exception merely permits the seizure of evidence that has already been viewed in accordance with the Fourth Amendment. In computer cases, this means that the government cannot rely on the plain view doctrine to justify opening a closed computer file."(footnote omitted)). *Accord* NEW JERSEY COMPUTER EVIDENCE SEARCH AND

Must the officer simply ignore those files? If she has probable cause to believe the files at issue contain evidence of criminal activity, she should use that probable cause to apply for a second, supplemental warrant, which authorizes a search of those files.[175]

The officer should do exactly the same thing if she discovers that the method(s) her warrant authorizes to be used in executing the search is insufficient for the stated purpose. Assume that the officer has a valid warrant to search for textual data using a special program that searches for specific words and phrases. While conducting the initial examination, the officer discovers that the computer to be searched has many compressed files, and evidence that suggests that the computer might also contain images of scanned documents. Since neither compressed files nor scanned documents can be searched with text-based tools, the officer should seek a separate supplemental warrant to review these files using the appropriate software.

The scenarios above are based on *Carey* and, therefore, address the more limited issues that arise when officers search only one or two computers. The application of the plain view doctrine is not, of course, limited to small computers. The doctrine has also been invoked when officers search a large number of computers and a large volume of files on computer storage media.[176]

Such systems can introduce distinct challenges for the law, since officers must deal with specifying the computers, storage media, or directories in a shared environment that will be searched. For example, Network Technologies, World Wide Web Hosts, and Internet-based storage providers such as Xdrive, allow users to store data on remote computers. Such data may be stored on a computer and hard drive that is owned by a third party and shared by many unrelated users. A search for one particular user's data should not become a carte blanche to allow searches that would violate the privacy of others.

SEIZURE MANUAL, I(B)(1) at 36 (2000) *available at* http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf (last visited Mar. 5, 2002). *Cf.* United States v. Lemmons, ___ F.3d ___, 2002 WL 272742, No. 00-3809, at *4, n.5 (7th Cir. Feb. 27, 2002) (stating, in dicta, that plain view doctrine did not apply to computer files because searching officer "had to access them by opening a program and looking on the hard drive for pornographic images").

175. *See* United States v. Gray, 78 F. Supp. 2d 524, 530–31 (E.D. Va. 1999); State v. Schroeder, 613 N.W.2d 911 916 (Wis. App. 2000). *See also* GUIDELINES, § II(D)(1) at 51 ("If investigators seize computer equipment for the evidence it contains and later decide to search the equipment for different evidence, . . . they should obtain a second warrant.").

176. *Cf.* Commonwealth v. Ellis, No. 97-192, 1999 WL 823741 *34 (Mass. Super. Aug. 18, 1999) (suppressing large volume of documents seized during law firm search because court found the documents did not fall within the scope of the warrant and could not have legitimately been discovered under the plain view doctrine).

As the Doe & Doe hypothetical illustrates, these large-scale searches can occur either on-site, at the suspect's home or place of business, or off-site, at a police computer laboratory.[177] One issue that arises in large-scale computer searches, and one of the justifications for conducting them off-site, is the problem of intermingled files.[178] As Part II explains, the premise is that officers are confronted with such a large number of incriminating and non-incriminating files, that it is simply not reasonable to expect them to sort and review the files on-site.

Part II deals with the issue of where such a review should be conducted. If the review is conducted on-site, the officers will probably use back-up copies of the files to preserve the originals; the same is true if the review is conducted off-site.[179] The back-ups will not consist of a subset of the files owned by the person or entity on whom the warrant is served; the back-ups will be mirror images of all the data on that system. Therefore, it is likely that the back-ups will contain files with information irrelevant to the scope of the search authorized by the warrant. In some instances, such as the Doe & Doe hypothetical, the back-ups may contain files which include privileged information. The presence of non-incriminating and/or privileged files requires the implementation of some technique to focus the officers' file review on files that are at least likely to fall within the scope of the warrant. This will prevent the officers from using the plain view doctrine impermissibly to conduct a general search of all the files on the back-up copy of that computer system.

Large-file searches tend to involve only text files.[180] The technique set out above for minimizing the scope of the plain view doctrine when officers are confronted with text files and non-text files cannot provide the solution for this problem. There is no simple technology that can be used to minimize the scope of a search of text files, other than a prudent selection of search terms. Electronic search tools are designed to search for information whose precise location is not known, and so the tools generally operate against entire disks or directories, searching all files within the target location. Limiting the scope of a keyword search can only be accomplished if the user of the search software manually isolates

177. *See supra* Part II.

178. *See supra* Part II(D).

179. On very large systems, it may not be possible to create a copy of the entire system in a timely fashion. It is beyond the scope of this paper to deal with the special problems inherent in the search of very large computer systems.

180. Large-file searches usually are conducted pursuant to investigations into large-scale criminal activity, such as drug-dealing or white-collar crimes, and are usually concerned with locating records of that criminal activity.

the files to be searched before the search begins. For example, the user might select files to be searched based on the dates the files were modified, copy all files of interest to a specific location, and then search the files in the new location, thereby excluding all files that were outside the scope of the relevant dates. The inspection of the text files identified by the search is a manual process, and can be limited quite easily. It can be limited based on factors such as the context in which a keyword is found, the creation date of the files, the file location, owner, or other similar criteria.

Another alternative is to let the officers assume the risk of exceeding the scope of their warrant. The officers would perform the search and if the search yields evidence that is to be used against the owner of the searched files, the owner should move to suppress that evidence. The motion should be based on the grounds that the evidence was discovered during an unauthorized search, a search that exceeded the scope of the warrant.[181] If the owner showed that the officers did exceed the scope of the warrant, the court would suppress the evidence.[182]

This solution is unacceptable for two reasons. First, the solution does not protect innocent property owners, who are never charged with crime, from having their files subjected to an unconstitutionally broad search.[183] Second, the solution undercuts one premise of the preference for warrants. The premise that officers are to be perceived as acting within constraints established by the Fourth Amendment.[184]

Instead, the better solution is based on procedures set out in the American Law Institute's ("ALI")Model Code of Pre-Arraignment Procedure.[185] A quarter of a century ago, the ALI suggested a set of procedures for handling large-document searches, an alternative to the off-site document searches discussed above.[186] Section 220.5 of the ALI's Model Code of Pre-Arraignment Procedure suggested the following:

181. *See Ellis*, 1999 WL 823741 *34.

182. *See id.*

183. *See* Steve Jackson Games, Inc. vs. United States Secret Service, 816 F.Supp 432 (W.D. Tex. 1993), *aff'd* 36 F.3d 457 (5th Cir. 1994)

184. *See, e.g.*, Illinois v. Gates, 462 U.S. 213, 236 (1983) ("[T]he possession of a warrant by officers conducting an arrest or search warrant greatly reduces the perception of unlawful or intrusive police conduct, by assuring 'the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.' " (citing United State v. Chadwick, 433 U.S. 1, 9 (1977)).

185. A MODEL CODE OF PRE-ARRAIGNMENT PROCEDURE § 220.5 (1975). *See also* MODEL CODE OF CYBERCRIME INVESTIGATIVE PROCEDURE, art. VII § 4(f)(j)(2) (1998) *at* http://www.cybercrimes.net/MCCIP/art1.htm.

186. *See supra* Part II(O).

> (1) Identification of Documents to Be Seized. If the warrant authorizes documentary seizure . . . , the executing officer shall endeavor by all appropriate means to search for and identify the documents to be seized without examining the contents of documents not covered by the warrant. . . .
>
> (2) Intermingled Documents. If the documents to be seized cannot be searched for or identified without examining the contents of other documents, or if they constitute items or entries in account books, diaries, or other documents containing matter not specified in the warrant, the executing officer shall not examine the documents but shall either impound them under appropriate protection where found, or seal and remove them for safekeeping pending further proceedings pursuant to Subsection (3) of this Section.
>
> (3) Return of Intermingled Documents. An executing officer who has impounded or removed documents pursuant to Subsection (2) of this Section shall, as promptly as practicable, report the fact and circumstances of the impounding or removal to the issuing official. As soon thereafter as the interests of justice permit, and upon due and reasonable notice to all interested persons, a hearing shall be held before the issuing official, or, if he [has] no jurisdiction, before a judicial officer having such jurisdiction, at which the person from whose possession or control the documents were taken, and any other person asserting any right or interest in the document, may appear, in person or by counsel, and move (a) for the return of the documents under Article 280 hereof, in whole or in part, or (b) for specification of such conditions and limitations on the further search for the documents to be seized as may be appropriate to prevent unnecessary or unreasonable invasion of privacy. If the motion for the return of the documents is granted, in whole or in part, the documents covered by the granting order shall forthwith be returned or released from impoundment. If the motion is not granted, the search shall proceed under such conditions and limitations as the order shall prescribe, and at the conclusion of the search all documents other than those covered by the warrant, or otherwise subject to seizure, shall be returned or released from impoundment.[187]

187. A MODEL CODE OF PRE-ARRAIGNMENT PROCEDURE § 220.5 (1975).

> The following procedures shall be utilized whenever officers execute a warrant authorizing the officers to search computer files or data:

On-site or off-site search: The default assumption is that a computer search will be executed on-site.[188] An off-site search must be authorized by a search warrant. To authorize an off-site search, the Magistrate Judge must find there is reasonable suspicion to believe an on-site search is not feasible.[189] An off-site search authorization can be contained in an original warrant, e.g., the warrant used to initiate a search, or in a supplemental warrant, a warrant officers obtain after they realize an on-site search is not practicable.

Scope of search: An application for a warrant to search text files must include a specification of the method(s) to be used in the search, including the search terms that are to be used.[190] When a Magistrate Judge issues a warrant based on such an application, the warrant must specify the method(s) and search terms to be used in conducting the search.[191] In executing the warrant, the officers are limited to the method(s) and search terms specified in the warrant.

Intermingled files: If the officer(s) executing a warrant to search and seize computer files can identify the files that fall within the scope of the warrant without having to review the contents of files that may not fall within its scope, they can proceed as authorized by the warrant.[192] If the

188. Search and seizure must adhere to the requirements of the Fourth Amendment. U.S. CONST amend. IV. The presumption of on-site search forces law enforcement to treat electronic evidence as it would other forms of evidence. The mere fact that evidence is in electronic format should not condone wholesale seizure. There must be a compelling need to treat electronic evidence differently from more traditional evidence. There is no justification for favoring those who are capable of storing their records on computer over those who keep hard copies of their records. *See* United States v. Abbell, 963 F. Supp. 1178 (S.D. Fla. 1997). However, unless a compelling need to seize hardware is found, there is no reason to punish those who do store their records on computer by strictly seizing their hardware and conducting an off-site search. Citizens have a right to expect that their possessions will not be subject to government seizure except upon showing of probable cause. *See* Roderick T. McCarvel, *Taking the Fourth Amendment to Bits: The Department of Justice Guidelines for Computer Searches and Seizures*, (1996) *available at* http://www/seanet.com/~rod/comp_4a.html (last visited Feb. 1, 2002). Law enforcement officials and agents must overcome this basic presumption and be able to seize computer hardware only upon showing a compelling need to search off-site. *See* MCCIP, art. VII § 4(f)(I) Commentary.

189. For more on the showing required to authorize an off-site search, *see supra* Part II(D).

190. *See* FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS § II(C) Step 3 at 47–48 (2001) *available at* http://www.cybercrime.gov/searchmanual.pdf.

191. *See id.* § II(C)(1) at 42–43.

192. This alternative will apply when officers are executing a warrant calling for a relatively limited search, such as searching the text-based files on an individual's computer to

officer(s) executing a warrant reasonably believe they cannot identify the files that fall within its scope without having to review the contents of files that may not fall within its scope, they shall not review the contents of any files but shall seek a supplemental warrant which authorizes them to make back-up copies of the files. If the officers reasonably believe they cannot identify and/or analyze the files that fall within the scope of the original warrant without having access to the computer equipment on which those files were generated and/or stored, the officers can seek a supplemental warrant which authorizes the officers to seize the computer equipment in which the files were stored. If a seizure of computer equipment is authorized, the equipment is to be taken to an off-site location and impounded pending further proceedings. One of the back-up copies of the files is to be given to the person on whom the warrant was served; the remaining back-up copies are to be sealed and remanded to the custody of a special master pending further proceedings under subsection (5), below.

Return of seized property and execution of search: An officer who has impounded computer equipment and/or made back-up copies of computer files under subsection (3), above, shall, as soon as possible, report what he or she has done to the Magistrate Judge issuing the original warrant. As soon thereafter as the interests of justice permit, and upon due and reasonable notice to all interested persons, a hearing shall be held before the Magistrate Judge at which the person whose computer equipment was taken and/or whose files were copied, and any other person asserting a right or interest in those files, can appear in person or by counsel and move (a) for the return of the seized equipment or files or (b) for the imposition of such specified limitations on any search to be conducted of the files as are needed to limit the search to items that are reasonably likely to fall within the scope of the warrant. If the motion to return seized equipment is granted, the equipment is to be returned to the movant as soon as possible; if the motion is not granted, the equipment is to remain impounded and cannot be searched or otherwise accessed except in accordance with an order issued by the Magistrate Judge, specifying the conditions under which the equipment can be searched and/or can be reassembled and used to conduct a search of seized files,[193] in accordance with the provisions of subsection (5), below. If the motion for the return of the files is granted, in whole or in part, the files covered by the granting order, including the originals and all copies made of

determine if he has sent harassing email messages to another person or searching the files on someone's computer to locate child pornography.

193. *See* New Technologies, Inc., *Seized*, *at* http://www.forensics-intl.com/seized.html (last visited Feb. 21, 2002) (advertising a software program that can be used to limit the access to a seized computer).

those files, shall immediately be returned to their rightful owner. If the motion is not granted, the files are to be searched in accordance with the limitations prescribed by the Magistrate Judge, one of which shall be the appointment of a special master in accordance with the provisions of subsection (5), and after the search has been completed, all files not covered by the warrant or otherwise subject to seizure shall be returned to their rightful owner.

Special master: Whenever original or back-up copies of intermingled computer files are to be searched, the court must appoint a special master who will supervise the conduct of the search in accordance with substantive and technical limitations set out by the court.[194] The officers charged with executing the search of the computer files shall provide the special master with copies of all the files seized pursuant to the warrant, while retaining a complete back-up copy of those files under seal. The special master will review the files provided to him or her and will determine (a) whether each file is encompassed by the provisions of the search warrant or, if not, falls within some valid exception to the search warrant which would justify the file's review by the officers executing the warrant and (b) whether each file is protected by an applicable evidentiary or constitutional privilege and, if so, if any exception to that privilege defeats its application and allows the file to be reviewed by the officers executing the warrant.[195] If no claim of privilege is raised as to the files at issue, the special master can allow the officers charged with executing the warrant to review the files using a search process and search terms approved by, and monitored by, the special master. After the files have been reviewed,[196] the special master shall issue a report which lists the files that are encompassed by the provisions of the warrant, and/or by an exception to the warrant requirement, and that are not protected by any valid privilege. The officers charged with executing the warrant shall be allowed to review these files. The remaining files, if any, are not to be reviewed by the officers executing the warrant. The costs of these procedures are to be paid by the government.[197]

194. *See* United States v. Abbell, 914 F. Supp. 519 (S.D. Fla. 1995) (appointing a special master to supervise review of documents and computer files seized from law office); People *ex rel.* Lockyer v. Superior Court, 392, 99 Cal. Rptr. 2d 646, 649 (Cal. App. 2000) (reappointing a special master to review backup tapes seized in execution of warrant authorizing search of district attorney's office and attorney's home).

195. *See id.*

196. *See* United States v. Abbell, 963 F. Supp. 1178, 1184 (S.D. Fla. 1997) (noting the efforts of special master who conducted a document by document review of computer data seized from law office).

197. *See* People v. Superior Court, 23 P.3d 563, 589 (Cal. 2001) ("[I]n the absence of an applicable statute, the services of a special master, appointed (pursuant to the court's inherent

The only effective way to limit the advertent or inadvertent exploitation of the plain view doctrine when officers must search large quantities of computer files is through the intercession of a special Magistrate Judge. The special Magistrate Judge will (a) screen all of the files at issue and determine their respective responsiveness to the warrant as well as determine whether any of the files are protected by valid privileges or (b) allow the officers charged with executing the warrant to conduct a carefully monitored process designed to identify the files which are encompassed by the scope of the warrant.[198] Under the procedure set forth above, once the special Magistrate Judge determines that a file is encompassed by the provisions of the search warrant or some applicable exception to the warrant requirement, the officers executing the search will be given access to the entirety of that file. Such a file may not only contain information about the crimes currently being investigated, the file may also contain information about other criminal activity. Since the officers have been given lawful access to the entire file, the plain view doctrine comes into play and lets the officers observe, and seize, information falling into the second category.

It is neither practicable nor reasonable to have the special master excise portions of the files that are provided to the officers. It is not practicable because redacting portions of a file could result in the officers' receiving fragmentary and essentially useless evidence, which would hamper, if not obstruct, the officers investigation. It is not unreasonable (in the sense of preventing an "unreasonable" search or seizure) to give the officers access to the entirety of a file because, as the Supreme Court stated in *Katz v. United States*, "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[199] For computer searches, the *Katz* principle means that when a person puts incriminating information of the commission of multiple crimes, into one computer file, that person cannot complain if an officer who has lawful access to that file observes all of the information.[200]

---

authority) to perform subordinate judicial duties . . . constitute an aspect of the court's operations that must be paid for by the court from public funds provided for such operations. Because statutory provisions . . . authorizing courts to impose certain court-related costs upon parties, do not apply in criminal proceedings, and because we find no statutory or common law basis for requiring the parties to subsidize the cost of the court's operations in such proceedings, we hold that the superior court possesses neither statutory nor inherent authority to require the parties, to pay any portion of the cost of a private special master . . . .").

198. *See Discussion Paper from Computer Forensics UK Ltd. On the Judicial Review Relating to Search Warrants, at* http://www.computer-forensics.com/articles/judicial.html (last visited Feb. 21, 2002).

199. Katz v. United States, 389 U.S. 347, 351 (1967).

200. *See* United States v. Isaacs, 708 F.2d 1365, 1370 (9th Cir. 1983) (holding that when officer is authorized to examine a book, the plain view doctrine allows the officer peruse the book's contents).

The owner of the seized files (and computer equipment) and anyone else who claims a valid Fourth Amendment interest in the files should be allowed to have the files returned to their rightful owner.[201] This essentially reiterates the provisions of Rule 41(e) of the Federal Rules of Criminal Procedure. It should not include a proviso that if the court grants a motion for the return of seized property, the court can impose reasonable conditions to ensure access and use of the property in subsequent proceedings.[202] Given the relative fragility and mutability of computer files, a court should deny a motion to have computer files returned if the court wants to ensure that the files will be available, in substantially unaltered form, for use in further proceedings.

If the owner of the seized files or anyone else who claims a valid Fourth Amendment interest in the files lose the motion for return of the files, that person should be allowed to move for the imposition of specific limitations on the searches to be performed on the files. The initiator of such a motion might, for example, request that the officers be limited to searches using the search terms specified in the original warrant.

IV. Is Copying Data a Search? A Seizure?

The final issue to be addressed is whether the making of copies of recovered data is a search or a seizure under the Fourth Amendment. As Part II explains, when officers search for computer information, the officers can conduct the search on-site or off-site. When the officers search on-site, they will conduct at least part of their search of the data stored on the computer system at its original location, instead of at a police laboratory. The officers may take copies of the files and/or the original files to the laboratory for a more thorough search. When officers search off-site, they will copy the files stored on the computer system and take (a) the copies or (b) the copies plus the originals of the files back to the laboratory, where the search will be conducted.[203] When officers take the original files, they usually provide the owner of that property with a copy of those files, though the owner may have to wait a few days to receive the copy.[204] Because the primary focus of all this activity is on reviewing

201. *See* Fed. R. Crim. P. Rule 41(e).

202. *See id*.

203. *See supra* Part II.

204. *See* Commonwealth v. Ellis, No. 97-192, 1999 WL 815818 (Mass. Super. Aug. 27, 1999) (ruling on a motion to suppress electronically stored evidence); Commonwealth v. Ellis, No. 97-192, 1999 WL 823741 (Mass. Super. Aug. 18, 1999) (ruling on a motion to suppress evidence). *See also supra* Part II.

the contents of the data contained in these files, the case law that has evolved from challenges brought to computer file searches focuses primarily on the propriety of that review, i.e., on whether or not the search of the files was reasonable.[205]

As noted before, the terms search and copy, as used with regard to electronic evidence, have different implications than the terms have in the physical world. When a copy is made of a computer file, the software used to create the copy does not disclose the contents of the copied file. The program merely creates a duplicate of the original. When a file is searched electronically, the entire contents of the file are not revealed to the searcher. Instead, the search will reveal whether or not the file contains a particular word or phrase, thus identifying the file as potentially relevant. It is only when the file is actually opened and read that an inspecting officer can determine the actual contents of the file.

Because of these differences, it is possible for an officer to copy files without having any opportunity to examine the files' contents. Likewise, the officer can search files without gaining full disclosure of the files' contents. Both copying and searching of a large number of files can be accomplished with a few key strokes, it is important to identify the exact scope of what can be copied or searched, within the reasonable scope of the warrant.

The question the arises is whether the simple act of copying computer files or computer data, without more, is an act encompassed by the Fourth Amendment. The focus of this inquiry is whether the related acts of making copies of computer files and taking the information contained in those files is a search or a seizure.

The Fourth Amendment prohibits unreasonable searches and/or seizures carried out by government agents while reasonable searches and seizures are permissible.[206] To be reasonable, a search or seizure must be conducted pursuant to a lawfully-issued warrant or an exception to the warrant requirement.[207] If there is no search or seizure, it is not necessary to consider whether the government action at issue was reasonable, since the existence of a search or a seizure is a threshold requirement for applying the Fourth Amendment's standards of reasonableness.

A search is a government action conducted in violation of someone's legitimate expectation of privacy.[208] A legitimate Fourth Amendment

205. *See supra* Part II.

206. U.S. CONST. amend. IV.

207. *See supra* Introduction, notes 9, 10.

208. The Fifth Amendment privilege against self-incrimination is not available to corporate and other artificial entities. However, it appears that the Fourth Amendment provides at least some protection to corporations. *See* General Motors Leasing Corp. v. United States, 429

expectation of privacy requires (a) that the person have manifested a subjective expectation of privacy in the area to be searched and (b) that this expectation be one society regards as reasonable.[209] Examples of a search include an officer to walking into someone's home,[210] or peering through a hole in a window curtain to observe the activities inside a home.[211] A search does not include an officer observing someone's movements in a public place, or noting the license plate number on a vehicle. A person may claim to have a subjective expectation of privacy in his or her movements or license plate information. However, the expectation is not one that society is prepared to regard as reasonable.[212]

A seizure " 'of property occurs when there is some meaningful interference with an individual's possessory interest in that property.' "[213] Examples of a seizure include a law enforcement officer who detains someone's luggage,[214] a police officer who padlocks a suspect's storage unit to prevent him from gaining access to the unit while a warrant is obtained.[215] However, a reasonable seizure does not violate the Fourth Amendment, but an unreasonable seizure of property does, even though the seized property was not searched.[216]

Is the act of copying computer files a search or a seizure? If it is neither, then copying data falls entirely outside the Fourth Amendment and is not subject to the constraints of reasonableness. The lack of constraint would allow an officer to copy files without having to show the files fell within the scope of the warrant the officer was executing or within the scope of a valid exception to that warrant.[217]

U.S. 338, 353 (1977) (holding corporations have some Fourth Amendment rights); Carl J. Mayer, *Personalizing the Impersonal: Corporations and the Bill of Rights*, 41 HASTINGS LAW JOURNAL 577 (1990).

209. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' ").

210. *See* State v. Norris, No. 17689, 1999 WL 1000034 at *2 (Ohio App. Nov. 5, 1999) (citing Payton v. New York, 445 U.S. 573 (1980)).

211. *See* State v. Vogel, 428 N.W.2d 272, 274 (S.D. 1988).

212. *See* State v. Donis, 723 A.2d 35, 38–39 (N.J. 1998). *See also* Smith v. Maryland, 442 U.S. 735, 742–44 (1979) (holding no reasonable expectation of privacy in telephone numbers dialed); United States v. Miller, 425 U.S. 435, 442 (1976) (holding no reasonable expectation of privacy in bank records conveyed to bank); United States v. Butler, 151 F. Supp. 2d 82, 84 (D. Me. 2001) (holding no reasonable expectation of privacy in "session logs or hard drive of . . . University owned computers.").

213. Soldal v. Cook County, 506 U.S. 56, 63 (1992) (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984).

214. *See* United States v. Ward, 144 F.3d 1024 (7th Cir. 1998).

215. *See* State v. Smith, 963 P.2d 642, 648 (Ore. 1998).

216. *See Soldal*, 506 U.S. at 63.

217. *See* LAFAVE, *supra* note 146, § 2.2.

As noted above, a search occurs when officers violate a legitimate expectation of privacy. Assume the contents of the copied computer files are protected under the Fourth Amendment because the owner of the files has an expressed subjective expectation of privacy as to the content of the files and society regards this expectation as reasonable.[218] Arguably, when officers conduct a keyword search of a file, some information about the files contents is disclosed, and so this action is properly termed a search even though the officer does not actually see the contents of the file.

But what about copies? The officers do not observe the contents of the computer files when the files are copied.[219] Therefore, it seems copying is not considered a search under the law.[220]

When copying files, officers physically remove files from the owner's possession. Therefore, it seems the act of copying should be a seizure. The officers are taking the owner's property—the information contained in the files. The difficulty with characterizing the copying of files as a seizure is that in the physical world a seizure is a zero sum concept. When officers seize property from its owner, the officers physically remove and possess the property in its entirety.[221] The owner is deprived of the possession and use of the property. When officers copy computer files, the officers take away the copies and/or the originals, but will usually leave the owner with a version of the files (either a copy or the originals). Therefore, no seizure has occurred because the owner is not deprived of the possession and use of the information contained in the files.[222]

There is little guidance available in current case law as to whether the act of copying computer data is a seizure. Only one reported decision squarely addresses this issue. In *United States v. Gorshkov,* the defendant argued that FBI agents' copying data from his computer in Russia

218. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

219. *See Discussion Paper*, *supra* note 198 (information contained in computer files "is not disclosed during copying").

220. *See Soldal*, 506 U.S. at 63–64. *But see* United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998) ("The Government conceded that the copying files . . . constituted a warrrantless search.").

221. *See Discussion Paper*, *supra* note 198 (stating the "original definition" of seizure was the "literal one", meaning "to confiscate, impound, or take possession of").

222. A seizure occurs while the copies of the files are being made. *See* United States v. Place, 462 U.S. 696, 707 (1983) (finding a seizure had occurred when officers detained person's property while obtaining a warrant because of an interference with person's possession and use of property). To the extent that the process of copying computer files deprives the owner of the files of his/her ability to use them while the copies are being made, it results in a transient seizure of the files, a period of interference with their possession and use.

constituted a seizure in violation of the Fourth Amendment.[223] The district court disagreed, holding that the

> agents' act of copying the data on the Russian computers was not a seizure under the Fourth Amendment because it did not interfere with Defendant's or anyone else's possessory interest in the data. The data remained intact and unaltered. It remained accessible to Defendant and any co-conspirators or partners with whom he had shared access. The copying of the data had absolutely no impact on his possessory rights. Therefore it was not a seizure under the Fourth Amendment.[224]

The computer which the agents accessed and from which they copied the data was located in Russia, and the Fourth Amendment does not apply outside the territorial United States.[225] It is therefore useful to consider how the Fourth Amendment might apply to domestic copying.

Lower federal and state courts have disagreed as to whether copying other kinds of information is a seizure.[226] In *Arizona v. Hicks*, the Supreme Court held that it was not a seizure for an officer to write down the serial numbers of stereo components that were in plain view because recording this information did not meaningfully interfere with the suspect's possessory interest in "either the serial numbers or the equipment."[227] While this observation might seem dispositive on the

---

223. United States v. Gorshkov, 2001 WL 1024026, No. CR))-550C (W.D. Wash. May 23, 2001).

224. *Id*. at *3 (footnote omitted).

225.

> [T]he Fourth Amendment does not apply to a search or seizure of a non-resident alien's property outside the territory of the United States. In this case, the computers accessed by the agents were located in Russia, as was the data contained on those computers that the agents copied. Until the copied data was transmitted to the United States, it was outside the territory of this country and not subject to the protections of the Fourth Amendment.

Id. at *3.

226. *Compare* United States v. Perry, 2001 WL 1230586, No. 00-6238, at * 8–9 (10th Cir. Oct. 16, 2001) (copying numbers displayed on caller identification unit was a seizure); United States v. Gray, 484 F.2d 352, 356 (6th Cir. 1973) (holding officer's copying serial numbers of rifles was a seizure); United States v. Sokolow, 450 F.2d 324, 326 (5th Cir. 1971) (copying serial numbers of air conditioning units was a seizure); United States v. Boswell, 347 A.2d 270, 273 (D.C. App. 1975) (copying television serial number was a seizure), *with* Basham v. Commonwealth, 675 S.W.2d 376, 384 (Ky. 1984) (holding "mere act" of copying down serial numbers is not a seizure); State ex rel. Eckstein v. Video Express, 695 N.E.2d 38, 43 (Ohio App. 1997) (holding officer's making copy of videotape was not a seizure).

227. 480 U.S. 321, 324 (1987); *see supra* Part IV. *See also Gorshkov* 2001 WL 1024026 at *3 (citing Hicks in holding that it was not a seizure for federal agents to copy data from a Russian computer).

question as to whether copying computer files is a seizure, further analysis will reveal that it is not dispositive.

Lower federal and state courts have also disagreed as to whether it is a seizure to photograph or videotape property.[228] Lower courts have applied the Supreme Court's reasoning in *Hicks* and held that recording a visual image of property is not a seizure because the recording does not meaningfully interfere with the owner's use and possession of that property.[229] While other lower courts have analogized the recording of visual images to the recording of conversations, and held that photographing or videotaping property is a seizure.[230] The analogy to a conversation is derived from the Supreme Court's holding in *Katz v. United States*.[231] In *Katz* the Court held that the Fourth Amendment encompasses the seizure of intangible items, including the recording of oral statements, as well as tangible property.[232] One circuit has cited *Katz* for supporting the proposition that when officers use a visual observation to collect information the officers are seizing that information.[233]

The Court's observation in *Katz* provides the correct approach for dealing with copying computer files. The Court's apparently inconsistent comment in *Hicks* can be distinguished for the holding in *Katz*.

One critical difference between writing down serial numbers in *Hicks* and the act of copying computer files is the nature of the information. The officer did not record information that belonged to Hicks. Serial numbers are not property in the sense that the number belong to one person, but are more analogous to license plates or other public records. Serial numbers are assigned by the manufacturer of a product and are used to track and identify that product. Hicks had no interest in these serial numbers because the stereo equipment was stolen from its rightful owners. Hicks had no lawful possessory interest in the equipment or in the serial numbers on the equipment.[234]

Unlike the serial numbers in *Hicks*, the information contained in computer files clearly belongs to the owner of the files. The ownership of information is similar to the contents of a private conversation in which the information belongs to the parties to the conversation.

228. *Compare* United States v. Ludwig, 902 F. Supp. 121, 125 (W.D. Tex. 1995) (holding videotaping was not a seizure) *with* People v. Matteo, 485 N.Y.S. 2d 446, 447 (N.Y. Sup. Ct. 1985) (holding photographing was a seizure) *and* Ayeni v. Mottola, 35 F.3d 680, 688 (2nd Cir. 1994) (holding videotaping was a seizure).

229. *See, e.g.*, Bills v. Aseltine, 958 F.2d 697, 707 (6th Cir. 1992).

230. *See* United States v. Villegas, 899 F.2d 1324, 1335 (2nd Cir. 1990).

231. 389 U.S. 347 (1967).

232. *See id*.

233. *See* United States v. Freitas, 800 F.2d 1451, 1455 (9th Cir. 1986).

234. *Hicks*, 480 U.S. at 323–324.

Copying computer data is analogous to recording a conversation in several ways. First, the object of both activities is the collection of information. The only difference is that the information is the data stored in the computer files while in a conversation the information is the content of the recorded conversation. Both use a collection process that duplicates the information at issue, the owner of the information is not deprived of possession or use of the information.[235] Both activities result in the creation of a body of inchoate, yet unrealized, evidence. Officers cannot ascertain whether the copy of a computer file or the tape recording of a conversation actually contain relevant evidence until the officers access and search the contents of the file or tape. Therefore, copying computer files should be treated as a seizure.[236]

A second difference between the officer's writing down the serial numbers in *Hicks* and the act of copying computer files is the fact that the process of copying computer files can be shown to interfere with the ability to access the files' contents. The more common forms of copying require dedicated access to the media in order for a copy to be created. No one may access the contents of a file or disk, while the file is copied. The more benign types of copy, which can permit access to files during the copy operation, will impact the responsiveness of the entire system . For these reasons copying should be considered a seizure because the act of copying interferes, however briefly, with the owner's use of the system.[237]

Documents filed in at least one federal case implicitly recognize that copying data is a seizure. In 1999, federal prosecutors sought a search

235. *But see* Randolph S. Sergent, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1186 (1995) (arguing that copying computer files is a seizure because the possessory interest in a computer file encompasses the ability to control the dissemination and use of the information contained therein and copying the information contained in a file interferes with the ability to exercise this control interferes with the owner's possessory interest in the file).

236. Arguably copying computer files is not a seizure in the traditional, zero sum exchange. But, copying should be treated as a seizure for the same reason that copying data can be treated as theft. Theft in the physical world is a zero sum exchange. The thief takes the physical property from the original owner, thereby completely depriving the owner of the property. The thief in the cyberworld can copy the owner's property and take the copy, leaving the owner with the possession and use of the property. But the act is theft on the premise that the owner has been deprived of something of value, namely, the right to the exclusive use and possession of that information. *See* Brenner, *supra* note 3. *See* State v. Schwartz, 21 P.3d 1128, 1136–1137 (Or. App. 2001). *But see* Miragaya v. State, 654 So.2d 262 (Fla. App. 1995) (copying suspect's video tape constituted a seizure).

237. *See* Criminal Justice and Police Act, 2001, c. 62 § 1(a) (Eng.), *at* http://www.hmso.gov.uk/acts/acts2001/20010016.htm (last visited Jan. 31, 2002) (" 'seize' includes 'take a copy' "); MODEL CODE OF CYBERCRIME INVESTIGATIVE PROCEDURE, art. I § 5(b) (1998) *at* http://www.cybercrimes.net/MCCIP/art1.htm (last visited Feb. 11, 2002).

warrant authorizing the installation of a keystroke logger on a computer belonging to Nicodemo Scarfo, whom they believed to be involved in illegal gambling and loan-sharking.[238] The warrant application sought permission to install a program to track the keystrokes of Scarfo in order seize passwords to allow the agents access to the computer.[239] The government needed the passwords to access a file agents had copied from Scarfo's computer some months before, in the course of executing a search warrant at the office.[240]

The law remains ambiguous as to whether copying data is a seizure. The warrant application filed in *Scarfo* concedes that copying is a seizure while *Gorshkov* concludes that it is not. If copying data is not a seizure, then copying cannot logically be regarded as a search and it does not violate an expectation of privacy. It is possible to copy files without examining the files. Therefore, if copying is not a seizure, it is outside the scope of the Fourth Amendment's reasonableness requirements and is an activity which can be conducted at will, requiring neither the justification of a warrant nor an exception to the warrant requirement. This is not a satisfactory result. Copying has an effect upon the "ownership" rights of the party whose information is copied. For policy reasons, the copying of data should be defined as a seizure. Doing so does not prohibit law enforcement from copying files; it merely ensures that officers comply with the standards of reasonableness set out in the Fourth Amendment.

CONCLUSION

To paraphrase Professor Lessig, cyberspace "in its nature shocks real-space law."[241] This article analyzed some of the respects in which cyberspace, in the form of searches and seizures involving computers and computer-related evidence, "shocks real-space law" in terms of the Fourth Amendment.

The Fourth Amendment evolved to deal with activities in the real-world or "real-space." The challenge that faces law in the twenty-first century is how to translate concepts that were devised to deal with real-world conduct into the virtual world of cyberspace. This article deals

238. United States v. Scarfo, 180 F.Supp. 2d 572 (D.N.J. 2001).

239. *Id.* at 574.

240. *See id.*; *see also* Convention on Cybercrime, Sept. 23, 2001, Europ. T.S. No. 185, Title 4, art 19 *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last visited Mar. 16, 2002) (recognizing that copying data is a seizure).

241. LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 199 (2001).

with a subset of that challenge—how to translate Fourth Amendment guarantees, originally designed to deal with law enforcement officers' forceful entry into real-space buildings and ransacking their contents, so that the concepts encompass the fragile realm of computer searches and seizures.

The Fourth Amendment is about privacy and the sanctity of personal possessions. While the Fourth Amendment was concededly devised to deal with transgressions against the strictures that protect real-world privacy, against doors and walls and other physical barriers, and to prohibit invasions of one's exclusive right to the possession of physical property, it is really about individual rights. The Fourth Amendment is about what Louis Brandeis and Samuel Warren called "the right to be let alone."[242] This article, in its modest way, argues that the "right to be let alone" must accompany individuals as they move into the virtual world of cyberspace. The purpose of the Fourth Amendment is to protect individuals, to protect the privacy of their activities, and the sanctity of their property. In the context of cyberspace, individuals' property often records privateactivities. Unless the Fourth Amendment is applied with this purpose in mind, the movement of American life into cyberspace may be accompanied by a corresponding diminution in the values that the Fourth Amendment was intended to protect.

242. *See* Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 193 (1890) (defining privacy as "the right to be let alone").

Draft Report and Recommendations

Joint Administrative Office/Department of Justice Working Group on Electronic Technology in the Criminal Justice System

I. Background and Charter of the Working Group

As a by-product of the Report on Costs and Recommendations for the Control of Costs of the Defender Services Program, transmitted to Congress in January 1998, the Director of the Administrative Office of the U.S. Courts (AOUSC) and the Attorney General of the United States created the Administrative Office of the United States Courts/Department of Justice Joint Working Group on Electronic Technology in the Criminal Justice System ("the Working Group"). The Working Group was charged with examining the use of electronic technology in the federal criminal justice system and its effect on the cost of evidence collection, analysis, and presentation. The formation of this unique "tripartisan" Working Group —with representatives of the AOUSC, the Department of Justice (DOJ), and both the public and private criminal defense bar—offered a means to explore ways in which technology might be used to promote the fair handling of electronic data in a cost-effective manner. The Working Group, which held its first meeting in June 1999, has analyzed how cooperation and coordination among participants may improve the criminal justice system while controlling costs and increasing efficiency in the context of an adversarial system and within the constraints of doctrines such as attorney work product and other privileges or ethical limitations.

II. Mission Statement

The Working Group began by developing a mission statement.

MISSION:

> To advance the fair administration of justice in the exchange and use of electronic data in a cooperative and cost-effective manner for all parties when required by the rules, when consistent with local custom and practice (compatible with privilege), or mandated by court order.

III. Issues Identified

The Working Group sought input from federal judges, Criminal Chiefs of United States Attorney's Offices, Federal Defenders, and Criminal Justice Act panel attorneys through questionnaires and interviews. Though not constituting a scientific survey, these sources provided useful insight into the leading issues arising from the use of electronic data in criminal litigation. (The results of these efforts are described more fully in Appendix 2.) In addition, the Working Group consulted with a number of different organizations working in the area of electronic data and litigation, including the Courtroom 21 Project at the College of William

and Mary's School of Law and the Federal Judicial Center. Based on the input of these groups and the Working Group's discussions, the following issues were identified:

A. Electronic Data Is Pervasive

Computers have become so commonplace that many cases now involve discovery of some computer-stored information. In fact, in a growing number of cases, relevant data exists only in electronic form. From the largest investigative and prosecutorial offices to the smallest criminal defense firms and solo practitioners, computers are used to cut costs, improve efficiency, enhance communication, store data, and improve capabilities in every aspect of practice. Indeed, the Government Paperwork Elimination Act requires that as much government business as possible be conducted by computer by October 21, 2003. Current initiatives to implement electronic case filing provide evidence of the federal judiciary's commitment to using computer-based technologies to improve the judicial process. Given the proliferation of computers, the use and involvement of computers and electronic data will only increase. Kenneth J. Withers, a Research Associate at the Federal Judicial Center who participated in a number of the Working Group's meetings, has noted that:

According to a University of California study, 93% of all information generated during 1999 was generated in digital form, on computers. Only 7% of information originated in other media, such as paper.

- Nearly all conventional documents are word-processed.
- Nearly all business activities are now computerized.
- E-mail traffic has surpassed telephone and postal communications.
- Just as legitimate activities are conducted on computers, so are illegitimate activities. Securities fraud, drug dealing, pornography distribution, illicit firearms sales – a whole panoply of bad acts – are conducted using computers and computer-mediated communications.

See Kenneth J. Withers, *Electronic Discovery: The Challenges and Opportunities of Electronic Evidence*, Presentation to Federal Judicial Center, National Workshop for Magistrate Judges, July 23-25, 2001, <http://www.kenwithers.com/articles/sandiego/>, at slide02.html—slide03.html.

1. Emerging Issues

While federal criminal justice participants report that the use of evidence in an electronic form is not yet pervasive in federal criminal litigation, they identified a number of significant issues that have arisen when such evidence has been employed.

a. Lack of Resources

Prosecutors, defense counsel, and judges all cited a lack of adequate resources to address electronic data issues, including insufficient funds to purchase appropriate hardware and software and a lack of adequately trained systems support personnel. Insufficient resources were also reported to have produced disparities among

parties where, for example, either co-defendants or the prosecution and defense have differing levels of technical resources.

b. Lack of Training

Everyone involved in the investigation, preparation and litigation of criminal cases increasingly encounters new technologies in the midst of their ongoing work. All parties identified a need for training to make the most efficient use of available electronic technology.

2. Jurisprudential Issues

While other groups are considering a variety of jurisprudential issues raised by electronic data, the Working Group focused on what electronic information is discoverable and who bears the cost for the discovery. These discovery questions, which also affect courtroom presentation, appear to be arising with increasing frequency under circumstances where one party to the litigation has used electronic tools to convert, organize, or index large quantities of documents. For example, substantive legal issues may be implicated when electronic evidence, by its very organization, may reveal trial strategies or attorney work product.

National policy makers with budgetary responsibilities representing each of the constituent groups should address issues of cost-sharing and the potential budgetary impact of the necessary use of electronic technology in criminal litigation. Costs may be larger than initially presumed. The budgetary impact should include not only the cost of producing information in an electronic form, but also of interpreting, organizing, and disclosing electronic information, using electronic technology to make courtroom presentations, and providing training on all of these matters.

IV. Recommendations

Criminal cases arise from the business of everyday life. With growing frequency, that business is conducted digitally. As a result, participants in the criminal justice system increasingly use data either conveyed to them in, or converted to, an electronic format. As law enforcement agencies, prosecutors, defense lawyers, and courts invest in new technology to process this information, additional costs will be incurred. The ability of all participants in the criminal justice system to address the issues presented by these new technologies will greatly impact that system's fairness and efficiency.

A. General

1. The AOUSC, Department of Justice, and Federal Defenders should maintain a working group to monitor, discuss and make recommendations regarding electronic information issues. The Working Group concluded that promoting awareness of new technology capabilities and the issues they generate will help criminal justice participants make more effective and efficient use of these tools.

2. Investigative agencies must be brought into the planning process. Their efforts often drive the acquisition and use of electronic information. Moreover, in order to resolve discovery policy issues, care must be taken to accommodate potential legitimate agency concerns about the security of agency investigative techniques.
3. The judiciary should urge formation of local working groups in federal judicial districts that include federal prosecutors, defense lawyers, and judges to consider how best to address emerging uses of electronic data and technology that may impact criminal prosecutions in their district.
4. The impact on juries of electronic technology, including how electronic information can best be provided to jurors during deliberations, should be studied.
5. The need, feasibility and usefulness of trial-specific document repositories on secure Web sites to facilitate access to digital discovery should be examined.
6. The National Institute of Trial Advocacy should be asked to assist the bench and bar with training by providing curricula for CLE training regarding electronic technology in criminal litigation.
7. Private "panel" attorneys providing CJA representation typically do not have the automation and litigation support resources or training available to them that are available to attorneys in U.S. Attorney and Federal Defender offices. Entities responsible for providing training and support services to panel attorneys should address this disparity.
8. Each district court (or each division in larger districts) should consider promoting and providing training on trial presentation equipment and methods not only to court personnel, but to the attorneys in the criminal justice system.
9. The national policy makers from each of the constituent groups should investigate and promote methods for providing training in electronic technology to users for all stages of the criminal justice process.
10. Consideration should be given to providing joint training for prosecutors and defense counsel at a local or regional level that addresses local issues, procedures, and practices governing the exchange, use, and presentation of electronic data in local courts and circuits.
11. Blanket rules that require digitization or electronic presentation in all cases should be avoided. Many smaller cases simply do not require this effort. Likewise, requiring a party in document-intensive cases to digitize extraneous material can be a waste of human and monetary resources.
12. Efforts should focus upon identifying required software and hardware capabilities rather than specifying use of particular software (or hardware). In an environment of accelerating change, standardization would blunt innovation and creativity on the part of designers, investigators and trial lawyers. However, the Working Group strongly believes that digitizing information in a format readable by all parties, and with commercial, non-proprietary software, is preferred for ease of discovery and use at trial.

B. Discovery Stage

1. As early in the process as possible, parties should evaluate whether digitization is appropriate, considering the costs and benefits for case presentation, enhanced comprehension by the fact-finder, and individual advocacy and trial strategy. In this regard, government investigative agencies, United States Attorney's Offices, and defense attorneys should consider the desirability of: (a) generating information in electronic form; (b) using software which is commercially available; and (c) collecting, collating, and indexing information in a manner that would, if desirable or necessary, facilitate the removal of attorney work product or other privileged information from the electronic data.
2. Absent significant justification, during the discovery process there should be no degradation of electronic data from the state in which that information is originally received by a party. For example, to the extent that a party gets discoverable information from a third party in electronic form, the party should produce the information in that same form when requested to do so.
3. To the extent a party converts discoverable information into an electronic form, or manipulates or organizes discoverable information that is in an electronic form, two important interests may become implicated: (a) a "sweat equity" interest and (b) a "value added" interest.
    a. "Sweat Equity"
        (1) A "sweat equity" interest exists when the work performed by the party does not implicate the work product or other privilege. Where the opposing party would have to perform the same or similar work to make use of the discoverable information, a cost savings may be achieved if the work product is shared with opposing party. On the other hand, simply making the work product available to the opposing party may not be fair, since both valuable trial preparation time and significant fiscal resources may have been expended in creating the work product.
        (2) For example, the government may have spent time and money converting discoverable paper documents into an electronic format and creating a basic index of the documents by entering them into an electronic database. In this circumstance, requiring a defendant to independently convert the same paper documents into an electronic format and then enter those documents into a comparable electronic data base might not only be wasteful and inefficient, but also could lead to difficulties at a trial or hearing if the parties have used different electronic formats for the documents they seek to exchange or present to a judge or jury electronically.
        (3) Recommendation
            (a) Absent significant justification, a party that converts discoverable information into an electronic form, or manipulates or organizes discoverable information that is in an electronic form, should make such products available to an opposing party, as-

suming that the work product or other privilege is not applicable to those products, and subject to any cost-sharing arrangements to which the parties may agree or the court may direct. In the example used above, the database and necessary software should be produced to the opposing party in discovery, subject to cost sharing arrangements.

(b) It may be difficult to allocate costs equitably, particularly when multiple parties with adverse interests are involved. In order to address both the trial preparation time required to perform the work and to help ensure that feasible cost-sharing arrangements are made, the parties should meet to discuss electronic information discovery issues as early in the case as possible.

b. "Value Added"

(1) A "value added" interest exists when the work performed by a party implicates the work product or other privilege.

(2) In the example used above, the government converted discoverable paper documents into an electronic format and created a basic index of the documents by entering them into an electronic database. Decisions made by the government in selecting documents for conversion, structuring the database, and choosing index topics, may reveal mental impressions, conclusions, or opinions about the documents such that disclosure of the documents selected for electronic conversion, the index, or both may implicate the work product or other privilege.

(3) Recommendation

(a) Absent significant justification, a party that converts discoverable information into an electronic form, or manipulates or organizes discoverable information that is in an electronic form, should make every effort to do so in manner that makes it possible to make such products available to an opposing party—perhaps in a redacted or other form—without implicating the work product or other privilege.

(b) In the example used above, the parties might have met and reached an early agreement regarding (i) which documents would be converted to an electronic format, (ii) the elements of a basic database indexing those converted documents, and (iii) a cost-sharing arrangement for completing this work. Such an agreement could produce overall cost-savings without inhibiting the ability of any party to convert additional documents of its own choosing, or to further index or manipulate the data base once it was created. Alternatively, the government might have been able to produce a redacted database or take some other measures that would have avoided the need to have defense counsel simply receive the documents in paper form.

C. Pre-Trial Stage

1. Effective procedures must be developed for dealing with technological issues in the trial process. All counsel should conduct a "meet and confer" session after arraignment followed by prompt notice to the Court of the possibility of electronic presentation and related issues.
2. At "meet and confer" sessions the parties should discuss: format of evidence, discovery, cost, sharing software, electronic presentation, hardware, equipment operator(s), trial court sight lines, and use of electronic information in openings, closings and witness examinations.
3. The Court should be given notice as soon as possible of the proposed use of electronic evidence, the suggested manner of presentation, relevant agreements reached by the parties, and any unresolved issues.
4. Courts should conduct timely pretrial conferences to discuss and resolve issues involving electronic discovery and presentation.
5. The parties may wish to consider having their respective automation specialist(s), if any, available to assist the Court and answer any questions.

D. Trial Stage

1. Courtrooms should be appropriately equipped to allow parties and the court to have access to digital resources and to utilize them in presentation. The Judicial Conference has endorsed the use of technologies in the courtroom and, subject to the availability of funds and priorities set by its Committee on Automation and Technology, urged that (a) courtroom technologies —including video evidence presentation systems, videoconferencing systems, and electronic methods of taking the record—be considered as necessary and integral parts of courtrooms undergoing construction or major renovation; and (b) the same courtroom technologies be retrofitted into existing courtrooms or those undergoing tenant alternations as appropriate. In support of this initiative, the Courtroom Technology Manual (1999) provides technical standards for both the infrastructures and the systems.

   Courts should offer general demonstrations and training on the use of the technology that is available in the courtroom as well as pre-trial access to the courtroom and its technology for practice and training. (Courts with courtroom technology installed often have training programs in place and allow for such access. The Federal Judicial Center presentation, "Developing Courtroom Technology Training Programs," recorded July 12, 2001, explains how to develop training programs that enable court staff and attorneys to use technology in the courtroom for the presentation of evidence.)
2. Courtrooms also should be fitted to accommodate additional hardware supplied by the parties. If either party elects to use additional hardware with capabilities different from that already provided in the courtroom, that additional hardware should be made available upon request for use by the opposing party when doing so would not unfairly disadvantage the producing party. The producing party also should provide basic training on that hardware upon request, assuming that such training does not require any significant expenditure of

time or money. The parties–and the court if necessary–should address these issues, including equitable allocation of costs, as early in the case as possible. Many of these issues are discussed in Effective Use of Courtroom Technology: A Judge's Guide to Pretrial and Trial (Federal Judicial Center and National Institute for Trial Advocacy, 2001), which describes the substantive and procedural considerations that may arise when lawyers bring electronic equipment to the courtroom or use court-provided equipment for displaying or playing evidentiary exhibits or illustrative aids during trial.

3. Appropriate means must be taken to identify and preserve electronic evidence and presentations for the appellate record in an appropriate form.

V. Conclusion

Courts, the government, and the criminal defense bar must respond to the continued development of "newer, better, and faster" data collection, electronic information, courtroom presentation and other computer systems. Whatever impacts business and the human experience will, in all likelihood be adapted for the courtroom. Each component of the criminal justice system must prepare to deal with these innovations. The Working Group concluded that promoting awareness of new technology capabilities, and identifying the issues that arise with their use, will advance the fair administration of justice by promoting more effective and efficient use of these tools. It is the hope of this Working Group that there will be continued communication among all participants in the criminal justice process, consistent with the recommendations it has offered.