Appendix F
Sample Premises Computer Search Warrant Affidavit

This form may be used when a warrant is sought to allow agents to enter a premises and remove computers or electronic media from the premises. In this document, "[[" marks indicate places that must be customized for each affidavit. Fill out your district's AO 93 Search Warrant form without any reference to computers; your agents are simply searching a premises for items particularly described in the affidavit's attachment. Consider incorporating the affidavit by reference. See Chapter 2 for a detailed discussion of issues involved in drafting computer search warrants.

UNITED STATES DISTRICT COURT
FOR THE [DISTRICT]

In the Matter of the Search of [[Premises Address]]	)	Case No.

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, [[AGENT NAME]], being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [[PREMISES ADDRESS]], hereinafter "PREMISES," for certain things particularly described in Attachment A.

2. I am a [[TITLE]] with the [[AGENCY]], and have been since [[DATE]]. [[DESCRIBE TRAINING AND EXPERIENCE INCLUDING EXPERTISE WITH COMPUTERS]].

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. [[Give facts that establish probable cause to believe that evidence, fruits, or contraband can be found on each computer that will be searched and/or seized, or to believe that the computers may be seized as contraband or instrumentalities.]]

TECHNICAL TERMS

5. [[THIS SECTION MIGHT BE UNNECESSARY; DEFINE ONLY TECHNICAL TERMS AS NECESSARY TO SUPPORT PROBABLE CAUSE.]] Based on my training and experience, I use the following technical terms to convey the following meanings:

a. 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. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. 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.

COMPUTERS AND ELECTRONIC STORAGE

6. As described above and in Attachment A, this application seeks permission to search and seize records that might be found on the PREMISES, in whatever form they are found. I submit that if a computer or electronic

medium is found on the premises, there is probable cause to believe those records will be stored in that computer or electronic medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know 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 files have been deleted, they can be recovered months or years later using readily available forensics tools. This is so because 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.

b. 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 currently being used by an active file—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.

c. Similarly, files that have been viewed via the Internet are typically automatically downloaded into a temporary Internet directory or "cache." The browser often 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 or if a user takes steps to delete them.

d. [[FOR CHILD PORNOGRAPHY CASES]] I know from training and experience 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 or computer hard drive can contain many child pornography images. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection. In my training and experience, individuals who view child pornography typically maintain their collections for many years and keep and collect items containing child pornography over long periods of time; in fact, they rarely, if ever, dispose of their sexually explicit materials.

e. [[FOR BUSINESS SEARCH CASES]] Based on actual inspection of [[spreadsheets, financial records, invoices]], I am aware that computer

equipment was used to generate, store, and print documents used in the [[tax evasion, money laundering, drug trafficking, etc.]] scheme. There is reason to believe that there is a computer system currently located on the PREMISES.

7. [[FOR CHILD PORNOGRAPHY OR OTHER CONTRABAND CASES]] 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 things constitute both evidence of crime and contraband. This affidavit also requests permission to seize the computer hardware and electronic media that may contain those things if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. [[In this case, computer hardware that was used to store child pornography is a container for evidence, a container for contraband, and also itself an instrumentality of the crime under investigation.]]

8. [[FOR CHILD PORNOGRAPHY PRODUCTION CASES]] I know from training and experience that it is common for child pornographers to use personal computers to produce both still and moving images. For example, a computer can have a camera built in, or can be connected to a camera and turn 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 scanner to transfer photographs into a computer-readable format. All of these devices, as well as the computer, constitute instrumentalities of the crime.

9. [[FOR HACKING OR OTHER INSTRUMENTALITY CASES]] I know 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. The computer is also likely to be a storage device for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

10. [[FOR CASES WHERE A RESIDENCE SHARED WITH OTHERS IS SEARCHED]] Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain computers that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is possible that the things described in this warrant could be found on those computers, this application seeks permission to search and if necessary to seize those computers as well. It may be impossible to determine, on scene, which computers contain the things described in this warrant.

11. Based upon my knowledge, training and experience, I know that searching for information stored in computers often requires agents to seize most or all electronic storage devices to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is often necessary to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine those storage devices in a laboratory setting, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the laboratory setting. This is true because of the following:

a. The volume of evidence. Computer storage devices (like hard disks or CD-ROMs) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse 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.

b. Technical requirements. Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and 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 processes 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.

12. In light of these concerns, I hereby request 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.

13. Searching computer systems for the evidence described in Attachment A may require a range of data analysis techniques. In some cases, it is possible for agents and analysts 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. 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 and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, the [[AGENCY]] intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

14. [[INCLUDE THE FOLLOWING IF THERE IS A CONCERN ABOUT THE SEARCH UNREASONABLY IMPAIRING AN OPERATIONAL, OTHERWISE LEGAL BUSINESS]] I recognize that the Company is a functioning company with many employees, and that a seizure of the Company's computers may have the unintended effect of limiting the Company's ability to provide service to its legitimate customers. In response to these concerns, the agents who execute the search anticipate taking an incremental approach to minimize the inconvenience to the Company's legitimate customers and to minimize the need to seize equipment and data. It is anticipated that, barring unexpected circumstances, this incremental approach will proceed as follows:

a. Upon arriving at the PREMISES, 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 things described in the warrant. The assistance of such an employee might allow agents to place less of a burden on the Company than would otherwise be necessary.

b. If the employees choose not to assist the agents, the agents decide that none are trustworthy, or for some other reason the agents cannot execute the warrant successfully without themselves examining the Company's computers, the agents will attempt to locate the things described in the warrant, and will attempt to make electronic copies of those things. This analysis will focus on things that may contain the evidence and information of the violations under investigation. In doing this, the agents might be able to copy only those things that are evidence of the offenses described herein, and provide only those things to the case agent. Circumstances might also require the agents to attempt to create an electronic "image" of those parts of the computer that are likely to store the things 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 agents or qualified computer experts will then conduct an off-site search for the things described in the warrant from the "mirror image" copy at a later date. If the agents successfully image the Company's computers, the agents will not conduct any additional search or seizure of the Company's computers.

c. If imaging proves impractical, or even impossible for technical reasons, then the agents will seize those components of the Company's computer system that the agents believe must be seized to permit the agents to locate the things described in the warrant at an off-site location. The seized components will be removed from the PREMISES. If employees of the Company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the Company's legitimate business. If, after inspecting the computers, the analyst determines that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it within a reasonable time.

CONCLUSION

15. I submit that this affidavit supports probable cause for a warrant to search the PREMISES and seize the items described in Attachment A.

REQUEST FOR SEALING

[[IF APPROPRIATE: It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.]]

Respectfully submitted,

[[AGENT NAME]]
Special Agent
[[AGENCY]]

Subscribed and sworn to before me on _____:

_____
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

1. All records relating to violations of the statutes listed on the warrant and involving [[SUSPECT]] since [[DATE]], including:

a. [[IDENTIFY RECORDS SOUGHT WITH PARTICULARITY; EXAMPLES FOR A DRUG CASE FOLLOW]];

b. lists of customers and related identifying information; types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

c. any information related to sources of narcotic drugs (including names, addresses, phone numbers, or any other identifying information);

d. any information recording [[SUSPECT]]'s schedule or travel from 2008 to the present;

e. all bank records, checks, credit card bills, account information, and other financial records.

2. [[IF OFFENSE INVOLVED A COMPUTER AS AN INSTRUMENTALITY OR CONTAINER FOR CONTRABAND]] Any computers or electronic media that were or may have been used as a means to commit the offenses described on the warrant, including [[receiving images of child pornography over the Internet in violation of 18 U.S.C. § 2252A.]]

3. For any computer hard drive or other electronic media (hereinafter, "MEDIA") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of user attribution showing who used or owned the MEDIA at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved usernames and passwords, documents, and browsing history;

b. passwords, encryption keys, and other access devices that may be necessary to access the MEDIA;

c. documentation and manuals that may be necessary to access the MEDIA or to conduct a forensic examination of the MEDIA.

4. [[IF CASE INVOLVED THE INTERNET]] Records and things evidencing the use of the Internet Protocol address [[e.g. 10.19.74.69]]

to communicate with [[e.g. Yahoo! mail servers or university mathematics department computers]], including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, 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 form of computer or electronic storage (such as hard disks or other media that can store data); 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).