



Technical Bulletin

featuring emerging technologies in criminal justice information management

1995

Issue Number 2

Search and Seizure of Computers: Key Legal and Practical Issues

By Alex White and
Scott Charney
Computer Crime Unit
U.S. Department of Justice

Over the past several years, as personal computers have become an increasing presence in businesses and homes throughout the United States and the world, they have also become increasingly useful to persons committing a broad range of crimes. Thus, in investigations concerning activities as disparate as child pornography and narcotics trafficking, Federal law enforcement officials have encountered situations where subjects have used computers to store information about their crimes, and, in some cases, to aid in the commission of those crimes.

In many instances, it has become necessary to search and seize computers and related items in order to obtain evidence for use in criminal prosecutions. Sometimes these searches are relatively straightforward, presenting few issues that cannot be resolved within the normal framework of analysis provided by Rule 41 of the Federal Rules of Criminal Procedure.¹ On many other occasions, however, computer searches present investigators

Bureau of Justice Assistance, SEARCH Explore New Technologies

The SEARCH *Technical Bulletin* is a quarterly publication designed to examine emerging technologies in criminal justice information management. Research and publication of the *Bulletin* is funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.

The *Bulletins* identify, describe and assess new and emerging technologies that have existing or potential application in criminal justice information management. They alert practitioners to the existence of technologies which can benefit their management of information.

If you would like to submit an article for publication in the *Technical Bulletin*, please contact SEARCH, The National Consortium for Justice Information and Statistics, at (916) 392-2550.

and prosecutors with difficult and novel First Amendment and Fourth Amendment issues. In addition, these searches are in some instances governed by complex statutory provisions involving the protection of privacy and stored electronic communications.

In 1991, the Assistant U.S. Attorney General, Criminal Division, established the Computer Crime Unit (CCU) within the General Litigation

and Legal Advice Section. The CCU is charged with, among other things, the responsibility to provide legal advice and litigation support on all matters involving the impact of computers and other emerging technologies on the investigation and prosecution of criminal cases. In line with this responsibility, the CCU recently published a monograph titled *Searching and Seizing Computers: Federal Guidelines*. This 164-page

treatise provides 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. No treatise of this length, or of any length, could possibly address every issue that is pertinent to this rapidly evolving field of criminal law. However, the guidelines provide a solid framework for analysis of those issues that are most likely to occur in cases involving computers.

This article cannot discuss the guidelines at great length, or even summarize every point contained therein. It

The *Technical Bulletin* is published by SEARCH, The National Consortium for Justice Information and Statistics, with funding from the Bureau of Justice Assistance, U.S. Department of Justice.

This document was prepared under grant number 95-DD-BX-0017, provided by the Bureau of Justice Assistance, U.S. Department of Justice. The points of view or opinions stated in the document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

SEARCH is located at 7311 Greenhaven Drive, Suite 145, Sacramento, California 95831, (916) 392-2550.

Dr. Francis J. Carney Jr.
Chairman

Gary R. Cooper
Executive Director

Sheila J. Barton
Deputy Director

George A. Buck
Deputy Director

David J. Roberts
Deputy Director

Kelly J. Harris
Editor

will, however, discuss some of the key issues that arise in connection with searches and seizures involving computers. (See the section on **For more information** at the end of this article.)

Need for technical expertise

At the outset, one of the most important observations to be made with respect to the search and seizure of computers is that the agents involved need to be trained with respect to the technical aspects of computers. Although law enforcement personnel face many different types of physical facilities and locations in carrying out searches pursuant to Rule 41, there is no area comparable to computers in terms of complexity and pitfalls for the unwary. For example, in most cases, the actual object of the search will be information stored in a computer's permanent storage medium, usually a rigid metal device known as a hard disk. The information itself consists of digitized bits of data recorded magnetically on the disk. In order to read this information, the agents must understand the particular syntax of the operating system used by the computer, and the syntax of the commands associated with the program used to create, store or retrieve the evidentiary data.

Even beyond the intricacies of knowing how to read the data stored in the computer, agents conducting a search may be confronted with additional problems when computer-literate targets attempt to frustrate the proper execution of the warrant. For example, an ingenious com-

puter owner might have installed hidden commands that could delete important data if certain start-up procedures are not followed. If they suspect such a booby trap, experts will take special precautions before carrying out the search, such as starting (booting) the computer from a clean floppy diskette, rather than from the operating software installed on the hard disk. The experts also may have to overcome other obstacles such as encryption, passwords, and files or directories that are "hidden" so that their names do not normally show up on the computer's monitor.

Thus, there are technical problems inherent in computer searches that are unlike the problems faced in any other type of search. And, beyond those problems, such searches have the potential of raising particularly complex legal issues. Because computer searches often are directed at information stored in computers, rather than at the computers themselves, the searches are likely to involve issues arising from the nature of the information. For example, some data in a seized computer may constitute speech protected under the First Amendment or under a specific statutory provision, such as the Privacy Protection Act, which is discussed later in this article.

With that introduction, this article will address just a few of the many legal and practical issues that confront those who carry out searches involving computers and related equipment.

Scope and location of search

The first point to emphasize is that a computer system is really a combination of connected components (often connected by wire, but increasingly by wireless means). To say that the government has probable cause to seize a "computer" does not necessarily mean it has probable cause to seize the entire computer system (i.e., the computer and all connected peripheral devices). Each component in a computer system should be considered independently. Thus, for example, a particular computer that is the target of a search may be connected to other devices, such as a printer and, in some cases, other computers on a local or wider network. However, it is not appropriate to seize those other devices merely because they are connected to the targeted computer; if they are to be seized, it should only be upon probable cause that is separately and specifically articulated as to each item.

Moreover, apart from the legal reasons to limit seizures of hardware, there are practical reasons making it advisable to seize the minimum amount of equipment that is necessary to accomplish the object of the search. One important reason is that investigative agencies do not have the personnel or the storage space required to seize and retain custody of large amounts of computer hardware. Another factor weighing against wholesale seizures is that, using the latest analytic techniques and appropriate equipment, well-trained agents now are able to con-

duct many searches on-site, rather than having to remove the computers and storage media to the laboratory. Technically proficient agents can copy the pertinent data from a computer's hard disk using specialized software that enables them to overcome obstacles such as hidden files and directories.

In making the decision whether to conduct a computer search on-site or in agency facilities, it is necessary to consider many factors, such as the volume of the evidence, the scope of the warrant, and the special problems that may arise when attempting to search computers. Courts have recognized that where a warrant justifiably authorizes a broad search through large volumes of material, it is appropriate for agents to remove the material to an off-site location for examination. Also, when the seized materials are located in a home rather than an office, the greater intrusiveness of having agents in a home is a factor that can weigh in favor of removing the materials for detailed searching elsewhere.

There also may be technical concerns that make it advisable and appropriate to remove computer equipment for an off-site search. For example, savvy computer users may know how to trip-wire their computers with "hot keys" or other self-destruct programs that could erase vital evidence if the system were examined by anyone other than an expert. Or a person could write a very short program that would cause the computer to demand a password periodically

and, if the correct password is not entered within 10 seconds, the program would destroy data automatically. If the searching agents suspect such a possibility, it probably would be advisable to remove the computer to an agency facility for careful analysis before the agents attempt to gain access to the data stored in the computer. In other cases, data on the computer may be encrypted, and agents may need to engage in lengthy decryption procedures that are not practical to be carried out on-site.

Commingled information

Another important issue in the developing field of computer searches is the extent to which the presence of privileged or protected material in a computer system can have an impact on the government's ability to conduct a search. This issue can arise in various contexts, but it is particularly likely to arise in connection with an electronic bulletin board system (BBS). A BBS is essentially a computer system set up to permit individuals using their computers and modems to communicate over telephone lines, and to post and read messages, much like traditional bulletin boards. In addition, a BBS may permit users to communicate via private electronic mail, to engage in real-time "chat sessions," to upload and download files, and to share information on topics of common interest, ranging from politics to photography to any other topic.

Some BBSs, often known as "pirate bulletin boards," are

maintained for illegal purposes, such as distributing illegally copied software, stolen credit card numbers or obscene materials. The distribution of such illegal material is not protected by the First Amendment's guarantee of freedom of speech. Many BBSs are of a hybrid nature, however, containing both illegal and legal material. To complicate matters further, the legitimate material on the BBS (or on the computer that runs the BBS) may be statutorily protected. For example, some private electronic mail may be covered under the Stored Wire and Electronic Communications provisions at 18 U.S.C. § 2701, et seq. (discussed later in this article), and some material may be protected from search and seizure by the Privacy Protection Act, a complex statute at 42 U.S.C. § 2000aa that was enacted in response to a Supreme Court decision that upheld a search of a newspaper's offices for evidence against third parties. This statute, among other provisions, makes it unlawful, unless an exception applies, for government personnel to "search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication" The statutory exceptions permit the seizure of contraband or the fruits or instrumentalities of a crime and permit the seizing of "work product" when life and limb are at stake, or when the material is evidence of a crime probably

committed by the person who possesses them. Even these exceptions have exceptions, however.

The main point to be emphasized here is that there are difficult and complex legal issues to be addressed whenever the government contemplates searching a BBS or computer that may contain material intended for publication. Even though there may be protected material on a computer, it may be necessary for the searching agents to seize the entire computer and search through all of the data stored in it in order to determine which materials are protected and which are not. The courts have yet to delineate exactly how some of these issues involving commingling of information will be resolved.

Stored electronic communications

Another statutory provision that, like the Privacy Protection Act, protects certain computerized data is the statute governing stored electronic communications, found at 18 U.S.C. § 2701, et seq. Although this provision is quite complex, and will not be discussed fully here, it is necessary for those conducting searches involving stored electronic mail to be generally familiar with the statutory requirements, so they can seek detailed guidance before embarking on the search.

Essentially, anyone who provides an electronic communication service or remote computing services to the public is prohibited from voluntarily disclosing the contents of the electronic

communications it stores or maintains on the service. There are several exceptions to this rule, including a provision allowing disclosure of the contents of a communication with the consent of the originator or addressee of the communication, and a provision allowing disclosure to a law enforcement agency of contents that were inadvertently obtained and appear to pertain to the commission of a crime.

For the government to obtain access to a stored electronic communication from an electronic communication service provider, it must follow the dictates of 18 U.S.C. § 2703, which sets out different rules depending upon how long the particular communication has been in electronic storage in an electronic communications system. If the communication has been in storage with an electronic communication service provider for 180 days or less, the government can require the service provider to disclose it only upon the authority of a search warrant issued under Rule 41. For communications stored for more than 180 days, or held by a remote computing service, the Government can require disclosure pursuant to various types of process, depending on whether or not notice is to be supplied to the person whose communications are being obtained.

In most cases, because of the nature of electronic mail, electronic communications sought by the government will be in storage with an electronic communication service provider for 180 days

or less and, therefore, may be obtained only pursuant to a warrant under Rule 41. Whenever preparing a warrant to search a computer, investigators should specifically indicate whether there is electronic mail on the target computer. If the agents intend to read those electronic communications, the warrant should identify whose mail is to be read, and establish that those electronic communications are subject to search under Rule 41(b).

Other issues

There are, of course, many other legal and technical issues of importance in the area of computer searches. One legal issue is whether network system administrators can give effective consent for a search of the files of users on the network, or provide copies of those files to law enforcement officials. A technical issue is whether in some cases it may be necessary to search unlikely places for data. For example, laser printers, computer monitors, and certain other types of devices may retain data that should be searched under some circumstances. A joint legal/technical issue arises when information is sought in a networked environment since it may not be clear, based on the technical configuration of the network, where the information sought is physically located. Thus, although an informant has seen information on a computer terminal in one location, it may turn out the file server actually containing that information was physically located in another building, or

in another Federal district, another state, or even another country.

Conclusion

The brief discussion of computer searches in this article should serve to illustrate the wide range of novel and challenging issues faced by law enforcement personnel who seek to gather evidence for criminal prosecutions through searches and seizures involving computers and related equipment. It is because of the complexities of the legal and practical problems in this area that the U.S. Department of Justice issued its guidelines for such searches and seizures. Any prosecutor or investigative agent who plans to conduct such a search for the first time would be well advised to consult those guidelines, and should feel free to contact the Computer Crime Unit's attorneys, before beginning to draft the affidavit and the warrant.

For more information

For further information, Federal, state, and local law enforcement officials can obtain copies of the complete document, *Searching and Seizing Computers: Federal Guidelines*, by contacting the CCU, U.S. Department of Justice, at (202) 514-1026. Other persons can request a copy of the guidelines from the Freedom of Information Act Office, Criminal Division, U.S. Department of Justice, at (202) 616-0207.

Endnote

¹ USCS Fed Rules Crim Proc R 41 (1995) Rule 41. Search and seizure

(a) Authority to issue warrant. Upon the request of a federal law enforcement officer or an attorney for the government, a search warrant authorized by this rule may be issued (1) by a federal magistrate judge, or a state court of record within the federal district, for a search of property or for a person within the district and (2) by a federal magistrate judge for a search of property or for a person either within or outside the district if the property or person is within the district when the warrant is sought but might move outside the district before the warrant is executed.

(b) Property or persons which may be seized with a warrant. A warrant may be issued under this rule to search for and seize any (1) property that constitutes evidence of the commission of a criminal offense; 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; or (4) person for whose arrest there is probable cause, or who is unlawfully restrained.

(c) Issuance and contents.

(1) Warrant upon affidavit. A warrant other than a warrant upon oral testimony under paragraph (2) of this subdivision shall issue only on an affidavit or affidavits sworn to before the federal magistrate judge or state judge and establishing the grounds for issuing the warrant. If the federal magistrate judge or state judge is satisfied that grounds for the application exist or that there is probable cause to believe that they exist, that magistrate judge or state judge shall issue a warrant identifying the property or person to be seized and naming or describing the person or place to be searched. The finding of probable cause may be based upon hearsay evidence in whole or in part. Before ruling on a request for a warrant the federal magistrate judge or state judge may require the affiant to appear personally and may examine under oath the affiant and any witnesses the affiant may produce, provided that such proceeding shall be taken down by a court reporter or recording equipment and made part of the affidavit. The warrant shall be directed to a civil officer of the United States authorized to enforce or assist in enforcing any law thereof or to a person so authorized by the President of the United States. It shall command the officer to search, within a specified period of time not to exceed 10 days, the person or place named for the property or person specified.

This report was written by Alex White and Scott Charney of the U.S. Department of Justice Computer Crime Unit. Points of view or opinions are those of the author and do not necessarily represent those of SEARCH or the SEARCH Membership Group.

The warrant shall be served in the daytime, unless the issuing authority, by appropriate provision in the warrant, and for reasonable cause shown, authorizes its execution at times other than daytime. It shall designate a federal magistrate judge to whom it shall be returned.

(2) Warrant upon oral testimony.

(A) General rule. If the circumstances make it reasonable to dispense, in whole or in part, with a written affidavit, a Federal magistrate judge may issue a warrant based upon sworn testimony communicated by telephone or other appropriate means including facsimile transmission.

(B) Application. The person who is requesting the warrant shall prepare a document to be known as a duplicate original warrant and shall read such duplicate original warrant, verbatim, to the Federal magistrate judge. The Federal magistrate judge shall enter, verbatim, what is so read to such magistrate judge on a document to be known as the original warrant. The Federal magistrate judge may direct that the warrant be modified.

(C) Issuance. If the Federal magistrate judge is satisfied that the circumstances are such as to make it reasonable to dispense with a written affidavit and that grounds for the application exist or that there is probable cause to believe that they exist, the Federal magistrate judge shall order the issuance of a warrant by directing the person requesting the warrant to sign the Federal magistrate judge's name on the duplicate original warrant. The Federal magistrate judge shall immediately sign the original warrant and enter on the face of the original warrant the exact time when the warrant was ordered to be issued. The finding of probable cause for a warrant upon oral testimony may be based on the same kind of evidence as is sufficient for a warrant upon affidavit.

(D) Recording and certification of testimony. When a caller informs the Federal magistrate judge that the purpose of the call is to request a warrant, the Federal magistrate judge shall immediately place under oath each person whose testimony forms a basis of the application and each person ap-

plying for that warrant. If a voice recording device is available, the Federal magistrate judge shall record by means of such device all of the call after the caller informs the Federal magistrate judge that the purpose of the call is to request a warrant. Otherwise a stenographic or longhand verbatim record shall be made. If a voice recording device is used or a stenographic record made, the Federal magistrate judge shall have the record transcribed, shall certify the accuracy of the transcription, and shall file a copy of the original record and the transcription with the court. If a longhand verbatim record is made, the Federal magistrate judge shall file a signed copy with the court.

(E) Contents. The contents of a warrant upon oral testimony shall be the same as the contents of a warrant upon affidavit.

(F) Additional rule for execution. The person who executes the warrant shall enter the exact time of execution on the face of the duplicate original warrant.

(G) Motion to suppress precluded. Absent a finding of bad faith, evidence obtained pursuant to a warrant issued under this paragraph is not subject to a motion to suppress on the ground that the circumstances were not such as to make it reasonable to dispense with a written affidavit.

(d) Execution and return with inventory. The officer taking property under the warrant shall give to the person from whom or from whose premises the property was taken a copy of the warrant and a receipt for the property taken or shall leave the copy and receipt at the place from which the property was taken. The return shall be made promptly and shall be accompanied by a written inventory of any property taken. The inventory shall be made in the presence of the applicant for the warrant and the person from whose possession or premises the property was taken, if they are present, or in the presence of at least one credible person other than the applicant for the warrant or the person from whose possession or premises the property was taken, and shall be verified by the officer. The federal magistrate judge shall upon request deliver a copy of the inventory to the person from whom or

from whose premises the property was taken and to the applicant for the warrant.

(e) Motion for return of property. A person aggrieved by an unlawful search and seizure or by the deprivation of property may move the district court for the district in which the property was seized for the return of the property on the ground that such person is entitled to lawful possession of the property. The court shall receive evidence on any issue of fact necessary to the decision of the motion. If the motion is granted, the property shall be returned to the movant, although reasonable conditions may be imposed to protect access and use of the property in subsequent proceedings. If a motion for return of property is made or comes on for hearing in the district of trial after an indictment or information is filed, it shall be treated also as a motion to suppress under Rule 12.

(f) Motion to suppress. A motion to suppress evidence may be made in the court of the district of trial as provided in Rule 12.

(g) Return of papers to clerk. The federal magistrate judge before whom the warrant is returned shall attach to the warrant a copy of the return, inventory and all other papers in connection therewith and shall file them with the clerk of the district court for the district in which the property was seized.

(h) Scope and definition. This rule does not modify any act, inconsistent with it, regulating search, seizure and the issuance and execution of search warrants in circumstances for which special provision is made. The term "property" is used in this rule to include documents, books, papers and any other tangible objects. The term "daytime" is used in this rule to mean the hours from 6:00 a.m. to 10:00 p.m. according to local time. The phrase "federal law enforcement officer" is used in this rule to mean any government agent, other than an attorney for the government as defined in Rule 54(c), who is engaged in the enforcement of the criminal laws and is within any category of officers authorized by the Attorney General to request the issuance of a search warrant.



Technical Bulletin

featuring emerging technologies in criminal justice information management

NONPROFIT ORG.
U.S. POSTAGE
PAID
Permit No. 1632
Sacramento, CA

SEARCH

The National Consortium for Justice Information and Statistics

7311 Greenhaven Drive, Suite 145 • Sacramento, California 95831
Telephone (916) 392-2550