Searching and Seizing Computers

Obtaining Electronic Evidence

in Criminal Investigations

Computer Crime and Intellectual Property Section

Criminal Division

United States Department of Justice

July 2002

DOWNLOADED FROM:

Sovereignty Education and Defense Ministry (SEDM) Website

http://sedm.org

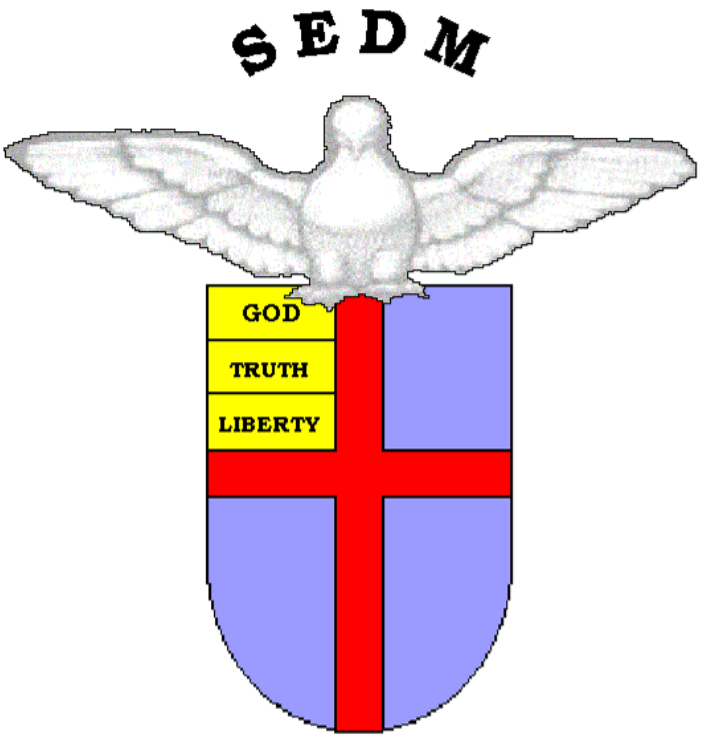

TABLE OF CONTENTS

PREFACE

Computers and Obtaining Electronic Evidence in Criminal Investigations." In addition to discussing recent caselaw, the Manual incorporates the important changes made to the laws governing electronic evidence gathering by the USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (the "PATRIOT Act"). These changes are discussed primarily in Chapters 3 and 4.

Many of the provisions of the PATRIOT Act relevant here would, unless reenacted into law, sunset on December 31, 2005. Accordingly, prosecutors and agents are urged to inform the Computer Crime and Intellectual Property Section (CCIPS), at 202-514-1026, whenever use of the new authorities proves helpful in a criminal case. This information will help ensure that Congress is fully informed when deciding whether to reenact these provision.

Nathan Judish of CCIPS took primary responsibility for the revisions in this Manual, under the supervison of Martha Stansell-Gamm, Chief of the Computer Crime and Intellectual Property Section. Assistance in editing was provided by CCIPS attorneys (in alphabetical order): Richard Downing, Mark Eckenwiler, David Green, Patricia McGarry, Paul Ohm, Richard Salgado, Michael Sussmann, and summer interns Matthew Heintz, Andrew Ting, Arun Subramanian, and Amalie Weber.

Also providing helpful suggestions were Thos. Gregory Motta and Lynn Pierce of the Office of General Counsel of the Federal Bureau of Investigation, and "Computer and Telecommunication Coordinators (CTCs)" Arif Alikhan, Mark Califano, Scott Christie, and Steven Schroeder.

This edition owes a tremendous debt to Orin S. Kerr, principal author of the 2001 edition, who departed from the Department of Justice in 2001 to teach at the George Washington University Law School. The 2001 edition superseded the 1994 Federal Guidelines for Searching and Seizing Computers, and reflected an enormous expenditure of time and thought on the part of Mr. Kerr and a number of attorneys at CCIPS, AUSAs, and specialists at the Federal Bureau of Investigation and other federal agencies. The organization and analysis of the 2001 edition hasbeen retained here - not because of inertia, but because they have proven to be sound and enduring.As is true with most efforts of this kind, the 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.

INTRODUCTION

In the last decade, computers and the Internet have entered the mainstream of American life. Millions of Americans spend several hours every day in front of computers, where they send and receive e-mail, surf the Web, maintain databases, and participate in countless other activities.

Unfortunately, those who commit crime have not missed the computer revolution. An increasing number of criminals use pagers, cellular phones, laptop computers and network servers in the course of committing their crimes. In some cases, computers provide the means of committing crime. For example, the Internet can be used to deliver a death threat via e-mail; to launch hacker attacks against a vulnerable computer network; to disseminate computer viruses; or to transmit images of child pornography. In other cases, computers merely serve as convenient storage devices for evidence of crime. For example, a drug kingpin might keep a list of who owes him money in a file stored in his desktop computer at home, or a money laundering operation might retain false financial records in a file on a network server.

The dramatic increase in computer-related crime requires prosecutors and law enforcement agents to understand how to obtain electronic evidence stored in computers. Electronic records such as computer network logs, e-mails, word processing files, and ".jpg" picture files increasingly provide the government with important (and sometimes essential) evidence in criminal cases. The purpose of this publication is to provide Federal law enforcement agents and prosecutors with systematic guidance that can help them understand the legal issues that arise when they seek electronic evidence in criminal investigations.

The law governing electronic evidence in criminal investigations has two primary sources: the Fourth Amendment to the U.S. Constitution, and the statutory privacy laws codified at 18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-12, and 18 U.S.C. §§ 3121-27. Although constitutional and statutory issues overlap in some cases, most situations present either a constitutional issue under the Fourth Amendment or a statutory issue under these three statutes. This manual reflects that division: Chapters 1 and 2 address the

Fourth Amendment law of search and seizure, and Chapters 3 and 4 focus on the statutory issues, which arise mostly in cases involving computer networks and the Internet.

Chapter 1 explains the restrictions that the Fourth Amendment places on the warrantless search and seizure of computers and computer data. The chapter begins by explaining how the courts apply the "reasonable expectation of privacy" test to computers; turns next to how the exceptions to the warrant requirement apply in cases involving computers; and concludes with a comprehensive discussion of the difficult Fourth Amendment issues raised by warrantless workplace searches of computers. Questions addressed in this chapter include: When does the government need a search warrant to search and seize a suspect's computer? Can an investigator search without a warrant through a suspect's pager found incident to arrest? Does the government need a warrant to search a government employee's desktop computer located in the employee's office?

Chapter 2 discusses the law that governs the search and seizure of computers pursuant to search warrants. The chapter begins by reviewing the steps that investigators should follow when planning and executing searches to seize computer hardware and computer data with a warrant. In particular, the chapter focuses on two issues: first, how investigators should plan to execute computer searches, and second, how they should draft the proposed search warrants and their accompanying affidavits. Finally, the chapter ends with a discussion of post-search issues. Questions addressed in the chapter include: When should investigators plan to search computers on the premises, and when should they remove the computer hardware and search it later off-site? How should investigators plan their searches to avoid civil liability under the Privacy Protection Act, 42 U.S.C. § 2000aa? How should prosecutors draft search warrant language so that it complies with the particularity requirement of the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure? What is the law governing when the government must search and return seized computers?

The focus of Chapter 3 is the stored communications portion of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-12 ("ECPA"). ECPA governs how investigators can obtain stored account records and contents from network service providers, including Internet service providers (ISPs), telephone companies, cell phone service providers, and satellite services. ECPA issues arise often in cases involving the Internet: any time investigators seek stored information concerning Internet accounts from providers of Internet service, they must comply with the statute. This chapter includes amendments to ECPA specified by the USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (the "PATRIOT Act"). The PATRIOT Act clarified and updated ECPA in light of modern technologies, and in several respects it eased restrictions on law enforcement access to stored communications. Topics covered in this section include: How can the government obtain e-mails and network account logs from ISPs? When does the government need to obtain a search warrant, as opposed to 18 U.S.C. § 2703(d) order or a subpoena? When can providers disclose e-mails and records to the government voluntarily? What remedies will courts impose when ECPA has been violated?

Chapter 4 reviews the legal framework that governs electronic surveillance, with particular emphasis on how the statutes apply to surveillance on the communications networks. In particular, the chapter discusses Title III as modified by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22 (referred to here as "Title III"),[1] as well as the Pen Register and Trap and Trace Devices statute, 18 U.S.C. §§ 3121-27. This chapter also includes amendments to these statutes specified by the PATRIOT Act. These statutes govern when and how the government can conduct real-time surveillance, such as monitoring a computer hacker's activity as he breaks into a government computer network. Topics addressed in this chapter include: When can victims of computer crime monitor unauthorized intrusions into their networks and disclose that information to law enforcement? Can network "banners" generate implied consent to monitoring? How can the government obtain a pen register/trap and trace order that

permits the government to collect packet header information from Internet communications? What remedies will courts impose when the electronic surveillance statutes have been violated?

Of course, the issues discussed in Chapters 1 through 4 can overlap in actual cases. An investigation into computer hacking may begin with obtaining stored records from an ISP according to Chapter 3, move next to an electronic surveillance phase implicating Chapter 4, and then conclude with a search of the suspect's residence and a seizure of his computers according to Chapters 1 and 2. In other cases, agents and prosecutors must understand issues raised in multiple chapters not just in the same case, but at the same time. For example, an investigation into workplace misconduct by a government employee may implicate all of Chapters 1 through 4. Investigators may want to obtain the employee's e-mails from the government network server (implicating ECPA, discussed in Chapter 3); may wish to monitor the employee's use of the telephone or Internet in real-time (raising surveillance issues from Chapter 4); and at the same time, may need to search the employee's desktop computer in his office for clues of the misconduct (raising search and seizure issues from Chapters 1 and 2). Because the constitutional and statutory regimes can overlap in certain cases, agents and prosecutors will need to understand not only all of the legal issues covered in Chapters 1 through 4, but will also need to understand the precise nature of the information to be gathered in their particular cases.

Chapters 1 through 4 are followed by a short Chapter 5, which discusses evidentiary issues that arise frequently in computer-related cases. The publication concludes with appendices that offer sample forms, language, and orders.

Computer crime investigations raise many novel issues, and the courts have only begun to interpret how the Fourth Amendment and federal statutory laws apply to computer-related cases. Agents and prosecutors who need more detailed advice can rely on several resources for further assistance. At the federal district level, every United States Attorney's Office has at least one Assistant U.S. Attorney who has been designated as a Computer and Telecommunications Coordinator ("CTC"). Every CTC receives extensive training in computer-related crime, and is primarily responsible for providing expertise relating to the topics covered in this manual within his or her district. CTCs may be reached in their district offices. Further, several sections within the Criminal Division of the United States Department of Justice in Washington, D.C., have expertise in computer-related fields. The Office of International Affairs ((202) 514-0000) provides expertise in the many computer crime investigations that raise international issues. The Office of Enforcement Operations ((202) 514-6809) provides expertise in the wiretapping laws and other privacy statutes discussed in Chapters 3 and 4. Also, the Child Exploitation and Obscenity Section ((202) 514-5780) provides expertise in computer-related cases involving child pornography and child exploitation.

Finally, agents and prosecutors are always welcome to contact the Computer Crime and Intellectual Property Section ("CCIPS") directly both for general advice and specific case-related assistance. During regular business hours, at least two CCIPS attorneys are on duty to answer questions and provide assistance to agents and prosecutors on the topics covered in this document, as well as other matters that arise in computer crime cases. The main number for CCIPS is (202) 514-1026. After hours, CCIPS can be reached through the Justice Command Center at (202) 514-5000.

I. SEARCHING AND SEIZING COMPUTERS WITHOUT A WARRANT

A. Introduction

The Fourth Amendment limits the ability of government agents to search for evidence without a warrant. This chapter explains the constitutional limits of warrantless searches in cases involving computers. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

According to the Supreme Court, a warrantless search does not violate the Fourth Amendment if one of two conditions is satisfied. First, if the government's conduct does not violate a person's "reasonable expectation of privacy," then formally it does not constitute a Fourth Amendment "search" and no warrant is required. See Illinois v. Andreas, 463 U.S. 765, 771 (1983). Second, a warrantless search that violates a person's reasonable expectation of privacy will nonetheless be "reasonable" (and therefore constitutional) if it falls within an established exception to the warrant requirement. See Illinois v. Rodriguez, 497 U.S. 177, 185 (1990). Accordingly, investigators must consider two issues when asking whether a government search of a computer requires a warrant. First, does the search violate a reasonable expectation of privacy? And if so, is the search nonetheless reasonable because it falls within an exception to the warrant requirement?

B. The Fourth Amendment's "Reasonable Expectation of Privacy" in Cases Involving Computers

1. General Principles

A search is constitutional if it does not violate a person's "reasonable" or "legitimate" expectation of privacy. Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring). This inquiry embraces two discrete questions: first, whether the individual's conduct reflects "an actual (subjective) expectation of privacy," and second, whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" Id. at 361. In most cases, the difficulty of contesting a defendant's subjective expectation of privacy focuses the analysis on the objective aspect of the Katz test, *i.e.*, whether the individual's expectation of privacy was reasonable.

No bright line rule indicates whether an expectation of privacy is constitutionally reasonable. See O'Connor v. Ortega, 480 U.S. 709, 715 (1987). For example, the Supreme Court has held that a person has a reasonable expectation of privacy in property located inside a person's home, see Payton v. New York, 445 U.S. 573, 589-90 (1980); in "the relative heat of various rooms in the home" revealed through the use of a thermal imager, see Kyllo v. United States, 533 U.S. 27 (2001); in conversations taking place in an enclosed phone booth, see Katz, 389 U.S. at 358; and in the contents of opaque containers, see United States v. Ross, 456 U.S. 798, 822-23 (1982). In contrast, a person does not have a reasonable expectation of privacy in activities conducted in open fields, see Oliver v. United States, 466 U.S. 170, 177 (1984); in garbage deposited at the outskirts of real property, see California v. Greenwood, 486 U.S. 35, 40-41 (1988); or in a stranger's house that the person has entered without the owner's consent in order to commit a theft, see Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978).

2. Reasonable Expectation of Privacy in Computers as Storage Devices

To determine whether an individual has a reasonable expectation of privacy in information stored in a computer, it helps to treat the computer like a closed container such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in a computer without a warrant if it would be prohibited from opening a closed container and examining its contents in the same situation.

The most basic Fourth Amendment question in computer cases asks whether an individual enjoys a reasonable expectation of privacy in electronic information stored within computers (or other electronic storage devices) under the individual's control. For example, do individuals have a reasonable expectation of privacy in the contents of their laptop computers, floppy disks or pagers? If the answer is "yes," then the government ordinarily must obtain a warrant before it accesses the information stored inside.

When confronted with this issue, courts have analogized electronic storage devices to closed containers, and have reasoned that accessing the information stored within an electronic storage device is akin to opening a closed container. Because individuals generally retain a reasonable expectation of privacy in the contents of closed containers, see United States v. Ross, 456 U.S. 798, 822-23 (1982), they also generally retain a reasonable expectation of privacy in data held within electronic storage devices. Accordingly, accessing information stored in a computer ordinarily will implicate the owner's reasonable expectation of privacy in the information. See United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998) (finding reasonable expectation of privacy in files stored on hard drive of personal computer); United States v. Reyes, 922 F. Supp. 818, 832-33 (S.D.N.Y. 1996) (finding reasonable expectation of privacy in data stored in a pager); United States v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995) (same); United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (same); United States v. Blas, 1990 WL 265179, at *21 (E.D. Wis. Dec. 4, 1990) ("[A]n individual has the same expectation of privacy in a pager, computer, or other electronic data storage and retrieval device as in a closed container.").

Although courts have generally agreed that electronic storage devices can be analogized to closed containers, they have reached differing conclusions over whether each individual file stored on a computer or disk should be treated as a separate closed container. In two cases, the Fifth Circuit has determined that a computer disk containing multiple files is a single container for Fourth Amendment purposes. First, in United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2001), in which private parties had searched certain files and found child pornography, the Fifth Circuit held that the police did not exceed the scope of the private search when they examined additional files on any disk that had been, in part, privately searched. Analogizing a disk to a closed container, the court explained that "police do not exceed the private search when they examine more items within a closed container than did the private searchers." Id. at 464. Second, in United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002), the court held that when a warrantless search of a portion of a computer and zip disk had been justified, the defendant no longer retained any reasonable expectation of privacy in the remaining contents of the computer and disk, and thus a comprehensive search by law enforcement personnel did not violate the Fourth Amendment.

In contrast to the Fifth Circuit's approach, the Tenth Circuit has refused to allow such exhaustive searches of a computer's hard in the absence of a warrant or some exception to the warrant requirement. See United States v. Carey, 172 F.3d 1268, 1273-75 (10th Cir. 1999) (ruling that agent exceeded the scope of a warrant to search for evidence of drug sales when he "abandoned that search" and instead searched for evidence of child pornography for five hours). In particular, the Tenth Circuit cautioned in a later case that "[b]ecause computers can hold so much information touching on many different areas of a person's life, there is greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer." United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).

Although individuals generally retain a reasonable expectation of privacy in computers under their control, special circumstances may eliminate that expectation. For example, an individual will not retain a reasonable expectation of privacy in information from a computer that the person has made openly available. In United States v. David, 756 F. Supp. 1385 (D. Nev. 1991), agents looking over the defendant's shoulder read the defendant's password from the screen as the defendant typed his password into a handheld computer. The court found no Fourth Amendment violation in obtaining the password, because the defendant did not enjoy a reasonable expectation of privacy "in the display that appeared on the screen." Id. at 1389. See also Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment

protection."); United States v. Gorshkov, 2001 WL 1024026, at *2 (W.D. Wash. May 23, 2001) (holding that defendant did not have a reasonable expectation of privacy in use of a private computer network when undercover federal agents looked over his shoulder, when he did not own the computer he used, and when he knew that the system administrator could monitor his activities). Nor will individuals generally enjoy a reasonable expectation of privacy in the contents of computers they have stolen. See United States v. Lyons, 992 F.2d 1029, 1031-32 (10th Cir. 1993).

3. Reasonable Expectation of Privacy and Third-Party Possession

Individuals who retain a reasonable expectation of privacy in stored electronic information under their control may lose Fourth Amendment protections when they relinquish that control to third parties. For example, an individual may offer a container of electronic information to a third party by bringing a malfunctioning computer to a repair shop, or by shipping a floppy diskette in the mail to a friend. Alternatively, a user may transmit information to third parties electronically, such as by sending data across the Internet. When law enforcement agents learn of information possessed by third parties that may provide evidence of a crime, they may wish to inspect it. Whether the Fourth Amendment requires them to obtain a warrant before examining the information depends first upon whether the third-party possession has eliminated the individual's reasonable expectation of privacy.

To analyze third-party possession issues, it helps first to distinguish between possession by a carrier in the course of transmission to an intended recipient, and subsequent possession by the intended recipient. For example, if A hires B to carry a package to C, A's reasonable expectation of privacy in the contents of the package during the time that B carries the package on its way to C may be different than A's reasonable expectation of privacy after C has received the package. During transmission, contents generally retain Fourth Amendment protection. The government ordinarily may not examine the contents of a package in the course of transmission without a warrant. Government intrusion and examination of the contents ordinarily violates the reasonable expectation of privacy of both the sender and receiver. See United States v. Villarreal, 963 F.2d 770, 774 (5th Cir. 1992); but see United States v. Walker, 20 F. Supp. 2d 971, 973-74 (S.D.W. Va. 1998) (concluding that packages sent to an alias in furtherance of a criminal scheme do not support a reasonable expectation of privacy). This rule applies regardless of whether the carrier is owned by the government or a private company. Compare Ex Parte Jackson, 96 U.S. (6 Otto) 727, 733 (1877) (public carrier) with Walter v. United States, 447 U.S. 649, 651 (1980) (private carrier).

A government "search" of an intangible electronic signal in the course of transmission may also implicate the Fourth Amendment. See Berger v. New York, 388 U.S. 41, 58-60 (1967) (applying the Fourth Amendment to a wire communication in the context of a wiretap). The boundaries of the Fourth Amendment in such cases remain hazy, however, because Congress addressed the Fourth Amendment concerns identified in Berger by passing Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), 18 U.S.C. §§ 2510-2522. Title III, which is discussed fully in Chapter 4, provides a comprehensive statutory framework that regulates real-time monitoring of wire and electronic communications. Its scope encompasses, and in many significant ways exceeds, the protection offered by the Fourth Amendment. See United States v. Torres, 751 F.2d 875, 884 (7th Cir. 1985); Chandler v. United States Army, 125 F.3d 1296, 1298 (9th Cir. 1997). As a practical matter, then, the monitoring of wire and electronic communications in the course of transmission generally raises many statutory questions, but few constitutional ones. See generally Chapter 4.

Individuals may lose Fourth Amendment protection in their computer files if they lose control of the files.

Once an item has been received by the intended recipient, the sender's reasonable expectation of privacy generally depends upon whether the sender can reasonably expect to retain control over the item and its contents. When a person leaves a package with a third party for temporary safekeeping, for example, he usually retains control of the package, and thus retains a reasonable expectation of privacy in its contents. See, e.g., United States v. Most, 876 F.2d 191, 197-98 (D.C. Cir. 1989) (finding reasonable expectation of privacy in contents of plastic bag left with grocery store clerk); United States v. Barry, 853 F.2d 1479, 1481-83 (8th Cir. 1988) (finding reasonable expectation of privacy in locked suitcase stored at airport baggage counter); United States v. Presler, 610 F.2d 1206, 1213-14 (4th Cir. 1979) (finding reasonable expectation of privacy in locked briefcases stored with defendant's friend for safekeeping). See also United States v. Barth, 26 F. Supp. 2d 929, 936-37 (W.D. Tex. 1998) (holding that defendant retains a reasonable expectation of privacy in computer files contained in hard drive left with computer technician for limited purpose of repairing computer).

If the sender cannot reasonably expect to retain control over the item in the third party's possession, however, the sender no longer retains a reasonable expectation of privacy in its contents. For example, in United States v. Horowitz, 806 F.2d 1222 (4th Cir. 1986), the defendant e-mailed confidential pricing information relating to his employer to his employer's competitor. After the FBI searched the competitor's computers and found the pricing information, the defendant claimed that the search violated his Fourth Amendment rights. The Fourth Circuit disagreed, holding that the defendant relinquished his interest in and control over the information by sending it to the competitor for the competitor's future use. See id. at 1225-26. See also United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) (holding that defendant does not retain reasonable expectation of privacy in contents of e-mail message sent to America Online chat room after the message has been received by chat room participants) (citing Hoffa v. United States, 385 U.S. 293, 302 (1966)). In some cases, the sender may initially retain a right to control the third party's possession, but may lose that right over time. The general rule is that the sender's Fourth Amendment rights dissipate as the sender's right to control the third party's possession diminishes. For example, in United States v. Poulsen, 41 F.3d 1330 (9th Cir. 1994), computer hacker Kevin Poulsen left computer tapes in a locker at a commercial storage facility but neglected to pay rent for the locker. Following a warrantless search of the facility, the government sought to use the tapes against Poulsen. The Ninth Circuit held that the search did not violate Poulsen's reasonable expectation of privacy because under state law Poulsen's failure to pay rent extinguished his right to access the tapes. See id. at 1337.

An important line of Supreme Court cases states that individuals generally cannot reasonably expect to retain control over mere information revealed to third parties, even if the senders have a subjective expectation that the third parties will keep the information confidential. For example, in United States v. Miller, 425 U.S. 435, 443 (1976), the Court held that the Fourth Amendment does not protect bank account information that account holders divulge to their banks. By placing information under the control of a third party, the Court stated, an account holder assumes the risk that the information will be conveyed to the government. Id. According to the Court, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." Id. (citing Hoffa v. United States, 385 U.S. 293, 302 (1966)). See also Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (finding no reasonable expectation of privacy in phone numbers dialed by owner of a telephone because act of dialing the number effectively tells the number to the phone company); Couch v. United States, 409 U.S. 322, 335

(1973) (holding that government may subpoena accountant for client information given to accountant by client, because client retains no reasonable expectation of privacy in information given to accountant). Because computer data is "information," this line of cases suggests that individuals who send data over communications networks may lose Fourth Amendment protection in the data once it reaches the intended recipient. See United States v. Meriwether, 917 F.2d 955, 959 (6th Cir. 1990) (suggesting that an electronic message sent via a pager is "information" under the Smith/Miller line of cases); Charbonneau, 979 F. Supp. at 1184 ("[A]n e-mail message . . . cannot be afforded a reasonable expectation of privacy once that message is received."). But see C. Ryan Reetz, Note, *Warrant Requirement for Searches of Computerized Information,* 67 B.U. L. Rev. 179, 200-06 (1987) (arguing that certain kinds of remotely stored computer files should retain Fourth Amendment protection, and attempting to distinguish United States v. Miller and Smith v. Maryland). Of course, the absence of constitutional protections does not necessarily mean that the government can access the data without a warrant or court order. Statutory protections exist that generally protect the privacy of electronic communications stored remotely with service providers, and can protect the privacy of Internet users when the Fourth Amendment may not. See 18 U.S.C. §§ 2701-2712 (discussed in Chapter 3, infra). Defendants will occasionally raise a Fourth Amendment challenge to the acquisition of account records and subscriber information held by Internet service providers using less process than a full search warrant. As discussed in a later chapter, the Electronic Communications Privacy Act permits the government to obtain transactional records with an "articulable facts" court order, and basic subscriber information with a subpoena. See 18 U.S.C. §§ 2701-2712 (discussed in Chapter 3, infra). These statutory procedures comply with the Fourth Amendment because customers of Internet service providers do not have a reasonable expectation of privacy in customer account records maintained by and for the provider's business. See United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), aff'd, 225 F.3d 656 (4th Cir. 2000) (unpublished opinion) (finding no Fourth Amendment protection for network account holder's basic subscriber information obtained from Internet service provider); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110) (D. Kan. 2000) (same). This rule accords with prior cases considering the scope of Fourth Amendment protection in customer account records. See, e.g., United States v. Fregoso, 60 F.3d 1314, 1321 (8th Cir. 1995) (holding that a telephone company customer has no reasonable expectation of privacy in account information disclosed to the telephone company); In re Grand Jury Proceedings, 827 F.2d 301, 302-03 (8th Cir. 1987) (holding that customer account records maintained and held by Western Union are not entitled to Fourth Amendment protection).

4. Private Searches

The Fourth Amendment does not apply to searches conducted by private parties who are not acting as agents of the government.

The Fourth Amendment "is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." United States v. Jacobsen, 466 U.S. 109, 113 (1984) (internal quotation omitted). As a result, no violation of the Fourth Amendment occurs when a private individual acting on his own accord conducts a search and makes the results available to law enforcement. See id. For example, in United States v. Hall, 142 F.3d 988 (7th Cir. 1998), the defendant took his computer to a private computer specialist for repairs. In the course of evaluating the defendant's computer, the repairman observed that many files stored on the computer had filenames characteristic of child pornography. The repairman accessed the files, saw that they did in fact contain child pornography, and

then contacted the state police. The tip led to a warrant, the defendant's arrest, and his conviction for child pornography offenses. On appeal, the Seventh Circuit rejected the defendant's claim that the repairman's warrantless search through the computer violated the Fourth Amendment. Because the repairman's search was conducted on his own, the court held, the Fourth Amendment did not apply to the search or his later description of the evidence to the state police. See id. at 993. See also United States v. Kennedy, 81 F. Supp. 2d 1103, 1112 (D. Kan. 2000) (concluding that searches of defendant's computer over the Internet by an anonymous caller and employees of a private ISP did not violate Fourth Amendment because there was no evidence that the government was involved in the search).

In United States v. Jacobsen, 466 U.S. 109 (1984), the Supreme Court presented the framework that should guide agents seeking to uncover evidence as a result of a private search. According to Jacobsen, agents who learn of evidence via a private search can reenact the original private search without violating any reasonable expectation of privacy. What the agents cannot do without a warrant is "exceed[] the scope of the private search." Id. at 115. See also United States v. Miller, 152 F.3d 813, 815-16 (8th Cir. 1998); United States v. Donnes, 947 F.2d 1430, 1434 (10th Cir. 1991). But see United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1999) (dicta) (stating in dicta that Jacobsen does not permit law enforcement to reenact a private search of a private home or residence). This standard requires agents to limit their investigation to the scope of the private search when searching without a warrant after a private search has occurred. So long as the agents limit themselves to the scope of the private search, the agents' search will not violate the Fourth Amendment. However, as soon as agents exceed the scope of the private warrantless search, any evidence uncovered may be vulnerable to a motion to suppress.

In computer cases, law enforcement use of the private search doctrine will depend in part on whether law enforcement examination of files not examined during the private search is seen as exceeding the scope of the private warrantless search. See United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2001) (holding that police did not exceed the scope of a private search when they examined more files on privately searched disks than had the private searchers). Under the approach adopted by the Fifth Circuit in Runyan, a third-party search of a single file on a computer allows a warrantless search by law enforcement of the computer's entire contents. Other courts, however, may reject the Fifth Circuit's approach and rule that government searchers can view only those files whose contents were revealed in the private search. See United States v. Barth, 26 F. Supp. 2d 929, 937 (W.D. Tex. 1998) (holding, in a pre-Runyan case, that agents who viewed more files than private searcher exceeded the scope of the private search). Even if courts follow the more restrictive approach, the information gleaned from the private search will often be useful in providing the probable cause needed to obtain a warrant for a further search.[(2)]

Although most private search issues arise when private third parties intentionally examine property and offer evidence of a crime to law enforcement, the same framework applies when third parties inadvertently expose evidence of a crime to plain view. For example, in United States v. Procopio, 88 F.3d 21 (1st Cir. 1996), a defendant stored incriminating files in his brother's safe. Later, thieves stole the safe, opened it, and abandoned it in a public park. Police investigating the theft of the safe found the files scattered on the ground nearby, gathered them, and then used them against the defendant in an unrelated case. The First Circuit held that the use of the files did not violate the Fourth Amendment, because the files were made openly available by the thieves' private search. See id. at 26-27 (citing Jacobsen, 466 U.S. at 113).

Importantly, the fact that the person conducting a search is not a government employee does not always mean that the search is "private" for Fourth Amendment purposes. A search by a private party will be considered a Fourth Amendment government search "if the private party act[s] as an instrument or agent

of the Government." Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614 (1989). The Supreme Court has offered little guidance on when private conduct can be attributed to the government; the Court has merely stated that this question "necessarily turns on the degree of the Government's participation in the private party's activities, . . . a question that can only be resolved 'in light of all the circumstances.'" Id. at 614-15 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971)). In the absence of a more definitive standard, the various federal Courts of Appeals have adopted a range of approaches for distinguishing between private and government searches. About half of the circuits apply a "totality of the circumstances" approach that examines three factors: whether the government knows of or acquiesces in the intrusive conduct; whether the party performing the search intends to assist law enforcement efforts at the time of the search; and whether the government affirmatively encourages, initiates or instigates the private action. See, e.g., United States v. Pervaz, 118 F.3d 1, 6 (1st Cir. 1997); United States v. Smythe, 84 F.3d 1240, 1242-43 (10th Cir. 1996); United States v. McAllister, 18 F.3d 1412, 1417-18 (7th Cir. 1994); United States v. Malbrough, 922 F.2d 458, 462 (8th Cir. 1990). Other circuits have adopted more rule-like formulations that focus on only two of these factors. See, e.g., United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982) (holding that private action counts as government conduct if, at the time of the search, the government knew of or acquiesced in the intrusive conduct, and the party performing the search intended to assist law enforcement efforts); United States v. Paige, 136 F.3d 1012, 1017 (5th Cir. 1998) (same); United States v. Lambert, 771 F.2d 83, 89 (6th Cir. 1985) (holding that a private individual is a state actor for Fourth Amendment purposes if the police instigated, encouraged or participated in the search, and the individual engaged in the search with the intent of assisting the police in their investigative efforts).

5. Use of Technology to Obtain Information

The government's use of innovative technology to obtain information about a target can implicate the Fourth Amendment. See Kyllo v. United States, 533 U.S. 27 (2001). In Kyllo, the Supreme Court held that the warrantless use of a thermal imager to reveal the relative amount of heat released from the various rooms of a suspect's home was a search that violated the Fourth Amendment. In particular, the Court held that where law enforcement "uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without a physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." Id. at 40. Use by the government of innovative technology not in general public use to obtain information stored on or transmitted through computers or networks may implicate this rule from Kyllo and thus may require a warrant. Whether a technology falls within the scope of the Kyllo rule depends on at least two factors. First, the use of technology should not implicate Kyllo if the technology is in "general public use," see id. at 34 & 39 n.6, although courts have not yet defined the standard for determining whether a given technology meets this requirement. Second, the Supreme Court restricted its holding in Kyllo to the use of technology to reveal information about "the interior of the home." See id. at 40 ("We have said that the Fourth Amendment draws a firm line at the entrance to the house." (internal citation omitted)).

C. Exceptions to the Warrant Requirement in Cases Involving Computers

Warrantless searches that violate a reasonable expectation of privacy will comply with the Fourth Amendment if they fall within an established exception to the warrant requirement. Cases involving computers often raise questions relating to how these "established" exceptions apply to new technologies.

1. Consent

Agents may search a place or object without a warrant or even probable cause if a person with authority has voluntarily consented to the search. See Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973). This consent may be explicit or implicit. See United States v. Milian-Rodriguez, 759 F.2d 1558, 1563-64 (11th Cir. 1985). Whether consent was voluntarily given is a question of fact that the court must decide by considering the totality of the circumstances. While no single aspect controls the result, the Supreme Court has identified the following important factors: the age, education, intelligence, physical and mental condition of the person giving consent; whether the person was under arrest; and whether the person had been advised of his right to refuse consent. See Schneckloth, 412 U.S. at 226. The government carries the burden of proving that consent was voluntary. See United States v. Matlock, 415 U.S. 164, 177 (1974); United States v. Price, 599 F.2d 494, 503 (2d Cir. 1979).
In computer crime cases, two consent issues arise particularly often. First, when does a search exceed the scope of consent? For example, when a target consents to the search of a machine, to what extent does the consent authorize the retrieval of information stored in the machine? Second, who is the proper party to consent to a search? Do roommates, friends, and parents have the authority to consent to a search of another person's computer files?[(3)]

a) Scope of Consent

"The scope of a consent to search is generally defined by its expressed object, and is limited by the breadth of the consent given." United States v. Pena, 143 F.3d 1363, 1368 (10th Cir. 1998) (internal quotation omitted). The standard for measuring the scope of consent under the Fourth Amendment is objective reasonableness: "What would the typical reasonable person have understood by the exchange between the [agent] and the [person granting consent]?" Florida v. Jimeno, 500 U.S. 248, 251 (1991). This requires a fact-intensive inquiry into whether it was reasonable for the agent to believe that the scope of consent included the items searched. Id. Of course, when the limits of the consent are clearly given, either before or during the search, agents must respect these bounds. See Vaughn v. Baldwin, 950 F.2d 331, 333 (6th Cir. 1991).
The permitted scope of consent searches depends on the facts of each case.

Computer cases often raise the question of whether consent to search a location or item implicitly includes consent to access the memory of electronic storage devices encountered during the search. In such cases, courts look to whether the particular circumstances of the agents' request for consent implicitly or explicitly limited the scope of the search to a particular type, scope, or duration. Because this approach ultimately relies on fact-driven notions of common sense, results reached in published opinions have hinged upon subtle (if not entirely inscrutable) distinctions. Compare United States v. Reyes, 922 F. Supp. 818, 834 (S.D.N.Y. 1996) (holding that consent to "look inside" a car included consent to retrieve numbers stored inside pagers found in car's back seat) with United States v. Blas, 1990 WL 265179, at *20 (E.D. Wis. Dec. 4, 1990) (holding that consent to "look at" a pager did not include consent to activate pager and retrieve numbers, because looking at pager could be construed to mean "what the device is, or how small it is, or what brand of pager it may be"). See also United States v. Carey, 172 F.3d 1268, 1274 (10th Cir. 1999) (reading written consent form extremely narrowly, so that consent to seizure of "any property" under the defendant's control and to "a complete search of the premises and property" at the defendant's address merely permitted the agents to seize the defendant's computer from his apartment, not to search the computer off-site because it was no longer located at the defendant's address). Prosecutors can strengthen their argument that the scope of consent included consent to search electronic storage devices by relying on analogous cases involving closed containers. See, e.g., United States v. Galante, 1995 WL 507249, at *3 (S.D.N.Y. Aug. 25, 1995) (holding that general consent to search car included consent to have officer access memory of cellular telephone found in the car, relying on circuit precedent involving closed containers); Reyes, 922 F. Supp. at 834.
Agents should be especially careful about relying on consent as the basis for a search of a computer when they obtain consent for one reason but then wish to conduct a search for another reason. In two recent cases, the Courts of Appeals suppressed images of child pornography found on computers after agents procured the defendant's consent to search his property for other evidence. In United States v. Turner, 169 F.3d 84 (1st Cir. 1999), detectives searching for physical evidence of an attempted sexual assault obtained written consent from the victim's neighbor to search the neighbor's "premises" and "personal property." Before the neighbor signed the consent form, the detectives discovered a large knife and blood stains in his apartment, and explained to him that they were looking for more evidence of the assault that the suspect might have left behind. See id. at 86. While several agents searched for physical evidence, one detective searched the contents of the neighbor's personal computer and discovered stored images of child pornography. The neighbor was charged with possessing child pornography. On interlocutory appeal, the First Circuit held that the search of the computer exceeded the scope of consent and suppressed the evidence. According to the Court, the detectives' statements that they were looking for signs of the assault limited the scope of consent to the kind of physical evidence that an intruder might have left behind. See id. at 88. By transforming the search for physical evidence into a search for computer files, the detective had exceeded the scope of consent. See id. See also Carey, 172 F.3d at 1277 (Baldock, J., concurring) (concluding that agents exceeded scope of consent by searching computer after defendant signed broadly-worded written consent form, because agents told defendant that they were looking for drugs and drug-related items rather than computer files containing child pornography) (citing Turner).
It is a good practice for agents to use written consent forms that state explicitly that the scope of consent includes consent to search computers and other electronic storage devices.
Because the decisions evaluating the scope of consent to search computers have reached sometimes unpredictable results, investigators should indicate the scope of the search explicitly when obtaining a suspect's consent to search a computer.

b) Third-Party Consent

i) General Rules

It is common for several people to use or own the same computer equipment. If any one of those people gives permission to search for data, agents may generally rely on that consent, so long as the person has authority over the computer. In such cases, all users have assumed the risk that a co-user might discover everything in the computer, and might also permit law enforcement to search this "common area" as well.

The watershed case in this area is United States v. Matlock, 415 U.S. 164 (1974). In Matlock, the Supreme Court stated that one who has "common authority" over premises or effects may consent to a search even if an absent co-user objects. Id. at 171. According to the Court, the common authority that establishes the right of third-party consent requires

> mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.

Id. at 171 n.7.

Under the Matlock approach, a private third party may consent to a search of property under the third party's joint access or control. Agents may view what the third party may see without violating any reasonable expectation of privacy so long as they limit the search to the zone of the consenting third party's common authority. See United States v. Jacobsen, 466 U.S. 109, 119 (1984) (noting that the Fourth Amendment is not violated when a private third party invites the government to view the contents of a package under the third party's control). This rule often requires agents to inquire into third parties's rights of access before conducting a consent search, and to draw lines between those areas that fall within the third party's common authority and those areas outside of the third party's control. See United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978) (holding that a mother could consent to a general search of her 23-year-old son's room, but could not consent to a search of a locked footlocker found in the room). Because the joint access test does not require a unity of interests between the suspect and the third party, however, Matlock permits third-party consent even when the target of the search is present and refuses to consent to the search. See United States v. Sumlin, 567 F.2d 684, 687-88 (6th Cir. 1977) (holding that woman had authority to consent to search of apartment she shared with her boyfriend even though boyfriend refused consent).

Co-users of a computer will generally have the ability to consent to a search of its files under Matlock. See United States v. Smith, 27 F. Supp. 2d 1111, 1115-16 (C.D. Ill. 1998) (concluding that a woman could consent to a search of her boyfriend's computer located in their house, and noting that the boyfriend had not password-protected his files). However, when an individual protects her files with passwords and has not shared the passwords with others who also use the computer, the Fourth Circuit has held that the authority of those other users to consent to search of the computer will not extend to the password-protected files. See Trulock v. Freeh, 275 F.3d 391, 403-04 (4th Cir. 2001) (analogizing password-protected files to locked footlockers inside a bedroom, which the court had previously held to be outside the scope of common authority consent). Conversely, if the co-user has been given the password by the suspect, then she probably has the requisite common authority to consent to a search of the files under Matlock. See United States v. Murphy, 506 F.2d 529, 530 (9th Cir. 1974) (per curiam) (concluding that an employee could consent to a search of an employer's locked warehouse because the

employee possessed the key, and finding "special significance" in the fact that the employer had himself delivered the key to the employee).

As a practical matter, agents may have little way of knowing the precise bounds of a third party's common authority when the agents obtain third-party consent to conduct a search. When queried, consenting third parties may falsely claim that they have common authority over property. In Illinois v. Rodriguez, 497 U.S. 177 (1990), the Supreme Court held that the Fourth Amendment does not automatically require suppression of evidence discovered during a consent search when it later comes to light that the third party who consented to the search lacked the authority to do so. See id. at 188-89. Instead, the Court held that agents can rely on a claim of authority to consent if based on "the facts available to the officer at the moment, . . . a man of reasonable caution . . . [would believe] that the consenting party had authority" to consent to a search of the premises. Id. (internal quotations omitted) (quoting Terry v. Ohio, 392 U.S. 1, 21-22 (1968)). When agents reasonably rely on apparent authority to consent, the resulting search does not violate the Fourth Amendment.

ii) Spouses and Domestic Partners

Most spousal consent searches are valid.

Absent an affirmative showing that the consenting spouse has no access to the property searched, the courts generally hold that either spouse may consent to search all of the couple's property. See, e.g., United States v. Duran, 957 F.2d 499, 504-05 (7th Cir. 1992) (concluding that wife could consent to search of barn she did not use because husband had not denied her the right to enter barn); United States v. Long, 524 F.2d 660, 661 (9th Cir. 1975) (holding that wife who had left her husband could consent to search of jointly-owned home even though husband had changed the locks). For example, in United States v. Smith, 27 F. Supp. 2d 1111 (C.D. Ill. 1998), a man named Smith was living with a woman named Ushman and her two daughters. When allegations of child molestation were raised against Smith, Ushman consented to the search of his computer, which was located in the house in an alcove connected to the master bedroom. Although Ushman used Smith's computer only rarely, the district court held that she could consent to the search of Smith's computer. Because Ushman was not prohibited from entering the alcove and Smith had not password-protected the computer, the court reasoned, she had authority to consent to the search. See id. at 1115-16. Even if she lacked actual authority to consent, the court added, she had apparent authority to consent. See id. at 1116 (citing Illinois v. Rodriguez).

iii) Parents

Parents can consent to searches of their children's rooms when the children are under 18 years old. If the children are 18 or older, the parents may or may not be able to consent, depending on the facts.

In some computer crime cases, the perpetrators are relatively young and reside with their parents. When the perpetrator is a minor, parental consent to search the perpetrator's property and living space will almost always be valid. See 3 W. LaFave,Search and Seizure: A Treatise on the Fourth Amendment § 8.4(b) at 283 (2d ed. 1987) (noting that courts have rejected "even rather extraordinary efforts by [minor] child[ren] to establish exclusive use.").

When the sons and daughters who reside with their parents are legal adults, however, the issue is more complicated. Under Matlock, it is clear that parents may consent to a search of common areas in the family home regardless of the perpetrator's age. See, e.g., United States v. Lavin, 1992 WL 373486, at *6 (S.D.N.Y. Nov. 30, 1992) (recognizing right of parents to consent to search of basement room where son kept his computer and files). When agents would like to search an adult child's room or other private areas, however, agents cannot assume that the adult's parents have authority to consent. Although courts have offered divergent approaches, they have paid particular attention to three factors: the suspect's age; whether the suspect pays rent; and whether the suspect has taken affirmative steps to deny his or her parents access to the suspect's room or private area. When suspects are older, pay rent, and/or deny

access to parents, courts have generally held that parents may not consent. See United States v. Whitfield, 939 F.2d 1071, 1075 (D.C. Cir. 1991) (holding "cursory questioning" of suspect's mother insufficient to establish right to consent to search of 29-year-old son's room); United States v. Durham, 1998 WL 684241, at *4 (D. Kan. Sept. 11, 1998) (mother had neither apparent nor actual authority to consent to search of 24-year-old son's room, because son had changed the locks to the room without telling his mother, and son also paid rent for the room). In contrast, parents usually may consent if their adult children do not pay rent, are fairly young, and have taken no steps to deny their parents access to the space to be searched. See United States v. Rith, 164 F.3d 1323, 1331 (10th Cir. 1999) (suggesting that parents are presumed to have authority to consent to a search of their 18-year-old son's room because he did not pay rent); United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978) (mother could consent to police search of 23-year-old son's room when son did not pay rent).

iv) System Administrators

Every computer network is managed by a "system administrator" or "system operator" whose job is to keep the network running smoothly, monitor security, and repair the network when problems arise. System operators have "root level" access to the systems they administer, which effectively grants them master keys to open any account and read any file on their systems. When investigators suspect that a network account contains relevant evidence, they may feel inclined to seek the system administrator's consent to search the contents of that account.

As a practical matter, the primary barrier to searching a network account pursuant to a system administrator's consent is statutory, not constitutional. System administrators typically serve as agents of "provider[s] of electronic communication service" under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2701-2712. ECPA regulates law enforcement efforts to obtain the consent of a system administrator to search an individual's account. See 18 U.S.C. § 2702-2703. Accordingly, any attempt to obtain a system administrator's consent to search an account must comply with ECPA. Seegenerally Chapter 3, "The Electronic Communications Privacy Act," infra.

To the extent that ECPA authorizes system administrators to consent to searches, the resulting consent searches will in most cases comply with the Fourth Amendment. Most fundamentally, it may be that individuals retain no reasonable expectation of privacy in the remotely stored files and records that their network accounts contain. See generally Chapter I.B.3, supra. If an individual does not retain a constitutionally reasonable expectation of privacy in his remotely stored files, it will not matter whether the system administrator has the necessary joint control over the account needed to satisfy the Matlock test because a subsequent search will not violate the Fourth Amendment.

In the event that a court holds that an individual does possess a reasonable expectation of privacy in remotely stored account files, whether a system administrator's consent would satisfy Matlock would depend on the circumstances. Clearly, the system administrator's access to all network files does not by itself provide the common authority that triggers authority to consent. In the pre-Matlock case of Stoner v. California, 376 U.S. 483 (1964), the Supreme Court held that a hotel clerk lacked the authority to consent to the search of a hotel room. Although the clerk was permitted to enter the room to perform his duties, and the guest had left his room key with the clerk, the Court concluded that the clerk could not consent to the search. If the hotel guest's protection from unreasonable searches and seizures "were left to depend on the unfettered discretion of an employee of the hotel," Justice Stewart reasoned, it would "disappear." Id. at 490. See also Chapman v. United States, 365 U.S. 610 (1961) (holding that a landlord lacks authority to consent to search of premises used by tenant); United States v. Most, 876 F.2d 191, 199-200 (D.C. Cir. 1989) (holding that store clerk lacks authority to consent to search of packages left with clerk for safekeeping). To the extent that the access of a system operator to a network account is analogous to the access of a hotel clerk to a hotel room, the claim that a system operator may consent to

a search of Fourth Amendment-protected files is weak. Cf. Barth, 26 F. Supp. 2d at 938 (holding that computer repairman's right to access files for limited purpose of repairing computer did not create authority to consent to government search through files).

Of course, the hotel clerk analogy may be inadequate in some circumstances. For example, an employee generally does not have the same relationship with the system administrator of his company's network as a customer of a private ISP such as AOL might have with the ISP's system administrator. The company may grant the system administrator of the company network full rights to access employee accounts for any work-related reason, and the employees may know that the system administrator has such access. In circumstances such as this, the system administrator would likely have sufficient common authority over the accounts to be able to consent to a search. See generally Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 Harv. L. Rev. 1591, 1602-03 (1997). See also United States v. Clarke, 2 F.3d 81, 85 (4th Cir. 1993) (holding that a drug courier hired to transport the defendant's locked toolbox containing drugs had common authority under Matlock to consent to a search of the toolbox stored in the courier's trunk). Further, in the case of a government network, the Fourth Amendment rules would likely differ dramatically from the rules that apply to private networks. See generally O'Connor v. Ortega, 480 U.S. 709 (1987) (explaining how the Fourth Amendment applies within government workplaces) (discussed infra).

c) Implied Consent

Individuals often enter into agreements with the government in which they waive some of their Fourth Amendment rights. For example, prison guards may agree to be searched for drugs as a condition of employment, and visitors to government buildings may agree to a limited search of their person and property as a condition of entrance. Similarly, users of computer systems may waive their rights to privacy as a condition of using the systems. When individuals who have waived their rights are then searched and challenge the searches on Fourth Amendment grounds, courts typically focus on whether the waiver eliminated the individual's reasonable expectation of privacy against the search. See, e.g., American Postal Workers Union, Columbus Area Local AFL-CIO v. United States Postal Service, 871 F.2d 556, 56-61 (6th Cir. 1989) (holding that postal employees retained no reasonable expectation of privacy in government lockers after signing waivers).

A few courts have approached the same problem from a slightly different direction and have asked whether the waiver established implied consent to the search. According to the doctrine of implied consent, consent to a search may be inferred from an individual's conduct. For example, in United States v. Ellis, 547 F.2d 863 (5th Cir. 1977), a civilian visiting a naval air station agreed to post a visitor's pass on the windshield of his car as a condition of bringing the car on the base. The pass stated that "[a]cceptance of this pass gives your consent to search this vehicle while entering, aboard, or leaving this station." Id. at 865 n.1. During the visitor's stay on the base, a station investigator who suspected that the visitor had stored marijuana in the car approached the visitor and asked him if he had read the pass. After the visitor admitted that he had, the investigator searched the car and found 20 plastic bags containing marijuana. The Fifth Circuit ruled that the warrantless search of the car was permissible, because the visitor had impliedly consented to the search when he knowingly and voluntarily entered the base with full knowledge of the terms of the visitor's pass. See id. at 866-67.

Ellis notwithstanding, it must be noted that several circuits have been critical of the implied consent doctrine in the Fourth Amendment context. Despite the Fifth Circuit's broad construction, other courts have proven reluctant to apply the doctrine absent evidence that the suspect actually knew of the search and voluntarily consented to it at the time the search occurred. See McGann v. Northeast Illinois

Regional Commuter R.R. Corp., 8 F.3d 1174, 1180 (7th Cir. 1993) ("Courts confronted with claims of implied consent have been reluctant to uphold a warrantless search based simply on actions taken in the light of a posted notice."); Securities and Law Enforcement Employees, District Council 82 v. Carey, 737 F.2d 187, 202 n.23 (2d Cir. 1984) (rejecting argument that prison guards impliedly consented to search by accepting employment at prison where consent to search was a condition of employment). Absent such evidence, these courts have preferred to examine general waivers of Fourth Amendment rights solely under the reasonable-expectation-of-privacy test. See id.

2. Exigent Circumstances

Under the "exigent circumstances" exception to the warrant requirement, agents can search without a warrant if the circumstances "would cause a reasonable person to believe that entry . . . was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." See United States v. McConney, 728 F.2d 1195, 1199 (9th Cir. 1984) (en banc). In determining whether exigent circumstances exist, agents should consider: (1) the degree of urgency involved, (2) the amount of time necessary to obtain a warrant, (3) whether the evidence is about to be removed or destroyed, (4) the possibility of danger at the site, (5) information indicating the possessors of the contraband know the police are on their trail, and (6) the ready destructibility of the contraband. See United States v. Reed, 935 F.2d 641, 642 (4th Cir. 1991).

Exigent circumstances often arise in computer cases because electronic data is perishable. Computer commands can destroy data in a matter of seconds, as can humidity, temperature, physical mutilation, or magnetic fields created, for example, by passing a strong magnet over a disk. For example, in United States v. David, 756 F. Supp. 1385 (D. Nev. 1991), agents saw the defendant deleting files on his computer memo book, and seized the computer immediately. The district court held that the agents did not need a warrant to seize the memo book because the defendant's acts had created exigent circumstances. See id. at 1392. Similarly, in United States v. Romero-Garcia, 991 F. Supp. 1223, 1225 (D. Or. 1997), aff'd on other grounds 168 F.3d 502 (9th Cir. 1999), a district court held that agents had properly accessed the information in an electronic pager in their possession because they had reasonably believed that it was necessary to prevent the destruction of evidence. The information stored in pagers is readily destroyed, the court noted: incoming messages can delete stored information, and batteries can die, erasing the information. Accordingly, the agents were justified in accessing the pager without first acquiring a warrant. See also United States v. Gorshkov, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001) (concluding that circumstances justified download without a warrant of data from computer in Russia where probable cause existed that Russian computer contained evidence of crime, where good reason existed to fear that delay could lead to destruction of or loss of access to evidence, and where agent merely copied data and subsequently obtained search warrant); United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996) (in conducting search incident to arrest, agents were justified in retrieving numbers from pager because pager information is easily destroyed).

Of course, in computer cases, as in all others, the existence of exigent circumstances is absolutely tied to the facts. Compare Romero-Garcia, 911 F. Supp. at 1225 with David, 756 F. Supp at 1392 n.2 (dismissing as "lame" the government's argument that exigent circumstances supported search of a battery-operated computer because the agent did not know how much longer the computer's batteries would live) and United States v. Reyes, 922 F. Supp. 818, 835-36 (S.D.N.Y. 1996) (concluding that

exigent circumstances could not justify search of a pager because the government agent unlawfully created the exigency by turning on the pager).

Importantly, the existence of exigent circumstances does not permit agents to search or seize beyond what is necessary to prevent the destruction of the evidence. When the exigency ends, the right to conduct warrantless searches does as well: the need to take certain steps to prevent the destruction of evidence does not authorize agents to take further steps without a warrant. See United States v. Doe, 61 F.3d 107, 110-11 (1st Cir. 1995). Accordingly, the seizure of computer hardware to prevent the destruction of information it contains will not ordinarily support a subsequent search of that information without a warrant. See David, 756 F. Supp. at 1392.

3. Plain View

Evidence of a crime may be seized without a warrant under the plain view exception to the warrant requirement. To rely on this exception, the agent must be in a lawful position to observe and access the evidence, and its incriminating character must be immediately apparent. See Horton v. California, 496 U.S. 128 (1990). For example, if an agent conducts a valid search of a hard drive and comes across evidence of an unrelated crime while conducting the search, the agent may seize the evidence under the plain view doctrine.

The plain view doctrine does not authorize agents to open and view the contents of a computer file that they are not otherwise authorized to open and review.

Importantly, the plain view exception cannot justify violations of an individual's reasonable expectation of privacy. The exception merely permits the seizure of evidence that an agent is already authorized to view in accordance with the Fourth Amendment. In computer cases, this means that the government cannot rely on the plain view exception to justify opening a closed computer file it is not otherwise authorized to view.[4] The contents of such a file that must be opened to be viewed are not in "plain view." See United States v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996). This rule accords with decisions applying the plain view exception to closed containers. See, e.g., United States v. Villarreal, 963 F.2d 770, 776 (5th Cir. 1992) (concluding that labels fixed to opaque 55-gallon drums do not expose the contents of the drums to plain view) ("[A] label on a container is not an invitation to search it. If the government seeks to learn more than the label reveals by opening the container, it generally must obtain a search warrant.").

As discussed above, see Chapter I.B.2., courts have reached differing conclusions over whether each individual file stored on a computer should be treated as a separate closed container, and this distinction has important ramifications for the scope of the plain view exception. United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999), provides a cautionary example of the restrictive approach. In Carey, a police detective searching a hard drive with a warrant for drug trafficking evidence opened a "jpg" file and instead discovered child pornography. At that point, the detective spent five hours accessing and downloading several hundred "jpg" files in a search not for evidence of the narcotics trafficking that he was authorized to seek and gather pursuant to the original warrant, but for more child pornography. When the defendant moved to exclude the child pornography files on the ground that they were seized beyond the scope of the warrant, the government argued that the detective had seized the "jpg" files properly because the contents of the contraband files were in plain view. The Tenth Circuit rejected this argument with respect to all of the files except for the first "jpg" file the detective discovered. See id. at 1273, 1273 n.4. As best as can be discerned, the rule in Carey seems to be that the detective could seize the first "jpg" file that came into plain view when the detective was executing the search warrant, but could not rely on the plain view exception to justify the search solely for additional "jpg" files

containing child pornography on the defendant's computers, evidence beyond the scope of the warrant. Cf. United States v.Walser, 275 F.3d 981, 986-87 (10th Cir. 2001) (finding no Fourth Amendment violation when officer with warrant to search for electronic records of drug transactions opened single computer file containing child pornography, suspended search, and then returned to magistrate for second warrant to search for child pornography).

In contrast to the Tenth Circuit's approach in Carey, the doctrine set forth by the Fifth Circuit in United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2001), and United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002), suggests that plain view of a single file on a computer or storage device could provide a basis for a more extensive search. In those two cases, the court held that when a warrantless search of a portion of a computer or storage device had been proper, the defendant no longer retained any reasonable expectation of privacy in the remaining contents of the computer or storage device. See Slanina, 283 F.3d at 680; Runyan, 275 F.3d at 464-65. Thus, a more extensive search of the computer or storage device by law enforcement did not violate the Fourth Amendment. This rationale may also apply when a file has been placed in plain view.

4. Search Incident to a Lawful Arrest

Pursuant to a lawful arrest, agents may conduct a "full search" of the arrested person, and a more limited search of his surrounding area, without a warrant. See United States v. Robinson, 414 U.S. 218, 235 (1973); Chimel v. California, 395 U.S. 752, 762-63 (1969). For example, in Robinson, a police officer conducting a patdown search incident to an arrest for a traffic offense discovered a crumpled cigarette package in the suspect's left breast pocket. Not knowing what the package contained, the officer opened the package and discovered fourteen capsules of heroin. The Supreme Court held that the search of the package was permissible, even though the officer had no articulable reason to open the package. See id. at 234-35. In light of the general need to preserve evidence and prevent harm to the arresting officer, the Court reasoned, it was per se reasonable for an officer to conduct a "full search of the person" pursuant to a lawful arrest. Id. at 235.

Due to the increasing use of handheld and portable computers and other electronic storage devices, agents often encounter computers when conducting searches incident to lawful arrests. Suspects may be carrying pagers, cellular telephones, Personal Digital assistants (such as Palm Pilots), or even laptop computers when they are arrested. Does the search-incident-to-arrest exception permit an agent to access the memory of an electronic storage device found on the arrestee's person during a warrantless search incident to arrest? In the case of electronic pagers, the answer clearly is "yes." Relying on Robinson, courts have uniformly permitted agents to access electronic pagers carried by the arrested person at the time of arrest. See United States v. Reyes, 922 F. Supp. 818, 833 (S.D.N.Y. 1996) (holding that accessing numbers in a pager found in bag attached to defendant's wheelchair within twenty minutes of arrest falls within search-incident-to-arrest exception); United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993); United States v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995); Yu v. United States, 1997 WL 423070, at *2 (S.D.N.Y. Jul. 29, 1997); United States v. Thomas, 114 F.3d 403, 404 n.2 (3d Cir. 1997) (dicta). See also United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996) (same holding, but relying on an exigency theory).

Courts have not yet addressed whether Robinson will permit warrantless searches of electronic storage devices that contain more information than pagers. In the paper world, certainly, cases have allowed extensive searches of written materials discovered incident to lawful arrests. For example, courts have uniformly held that agents may inspect the entire contents of a suspect's wallet found on his person. See, e.g., United States v. Castro, 596 F.2d 674, 676 (5th Cir. 1979); United States v. Molinaro, 877 F.2d

1341, 1347 (7th Cir. 1989) (citing cases). Similarly, one court has held that agents could photocopy the entire contents of an address book found on the defendant's person during the arrest, see United States v. Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993), and others have permitted the search of a defendant's briefcase that was at his side at the time of arrest. See, e.g., United States v. Johnson, 846 F.2d 279, 283-84 (5th Cir. 1988); United States v. Lam Muk Chiu, 522 F.2d 330, 332 (2d Cir. 1975). If agents can examine the contents of wallets, address books, and briefcases without a warrant, it could be argued that they should be able to search their electronic counterparts (such as electronic organizers, floppy disks, and Palm Pilots) as well. Cf. United v. Tank, 200 F.3d 627, 632 (9th Cir. 2000) (holding that agents searching a car incident to a valid arrest properly seized a Zip disk found in the car, but failing to discuss whether the agents obtained a warrant before searching the disk for images of child pornography).
The limit on this argument is that any search incident to an arrest must be reasonable. See Swain v. Spinney, 117 F.3d 1, 6 (1st Cir. 1997). While a search of physical items found on the arrestee's person may always be reasonable, more invasive searches in different circumstances may violate the Fourth Amendment. See, e.g. Mary Beth G. v. City of Chicago, 723 F.2d 1263, 1269-71 (7th Cir. 1983) (holding that Robinson does not permit strip searches incident to arrest because such searches are not reasonable in context). For example, the increasing storage capacity of handheld computers suggests that Robinson's bright line rule may not always apply in the case of electronic searches. When in doubt, agents should consider whether to obtain a search warrant before examining the contents of electronic storage devices that might contain large amounts of information.

5. Inventory Searches

Law enforcement officers routinely inventory the items they have seized. Such "inventory searches" are reasonable -- and therefore fall under an exception to the warrant requirement -- when two conditions are met. First, the search must serve a legitimate, non-investigatory purpose (e.g., to protect an owner's property while in custody; to insure against claims of lost, stolen, or vandalized property; or to guard the police from danger) that outweighs the intrusion on the individual's Fourth Amendment rights. See Illinois v. Lafayette, 462 U.S. 640, 644 (1983); South Dakota v. Opperman, 428 U.S. 364, 369-70 (1976). Second, the search must follow standardized procedures. See Colorado v. Bertine, 479 U.S. 367, 374 n.6 (1987); Florida v. Wells, 495 U.S. 1, 4-5 (1990).
It is unlikely that the inventory-search exception to the warrant requirement would support a search through seized computer files. See United States v. O'Razvi, 1998 WL 405048, at *6-7 (S.D.N.Y. July 17, 1998) (noting the difficulties of applying the inventory-search requirements to computer disks); see also United States v. Flores, 122 F. Supp. 2d 491, 493-95 (S.D.N.Y. 2000) (finding search of cellular telephone "purely investigatory" and thus not lawful inventory search). Even assuming that standard procedures authorized such a search, the legitimate purposes served by inventory searches in the physical world do not translate well into the intangible realm. Information does not generally need to be reviewed to be protected, and does not pose a risk of physical danger. Although an owner could claim that his computer files were altered or deleted while in police custody, examining the contents of the files would offer little protection from tampering. Accordingly, agents will generally need to obtain a search warrant in order to examine seized computer files held in custody.

6. Border Searches

In order to protect the government's ability to monitor contraband and other property that may enter or exit the United States illegally, the Supreme Court has recognized a special exception to the warrant requirement for searches that occur at the border of the United States. According to the Court, "routine searches" at the border or its functional equivalent do not require a warrant, probable cause, or even reasonable suspicion that the search may uncover contraband or evidence. United States v. Montoya De Hernandez, 473 U.S. 531, 538 (1985). Searches that are especially intrusive, however, require at least reasonable suspicion. See id. at 541. These rules apply to people and property both entering and exiting the United States. See United States v. Oriakhi, 57 F.3d 1290, 1297 (4th Cir. 1995).

In at least one case, courts have addressed whether the border search exception permits a warrantless search of a computer disk for contraband computer files. In United States v. Roberts, 86 F. Supp. 2d 678 (S.D. Tex. 2000), aff'd on other grounds, 274 F.3d 1007 (5th Cir. 2001), United States Customs Agents learned that William Roberts, a suspect believed to be carrying computerized images of child pornography, was scheduled to fly from Houston, Texas to Paris, France on a particular day. On the day of the flight, the agents set up an inspection area in the jetway at the Houston airport with the sole purpose of searching Roberts. Roberts arrived at the inspection area and was told by the agents that they were searching for "currency" and "high technology or other data" that could not be exported legally. Id. at 681. After the agents searched Roberts' property and found a laptop computer and six Zip diskettes, Roberts agreed to sign a consent form permitting the agents to search his property. A subsequent search revealed several thousand images of child pornography. See id. at 682.

The district court rejected the defendant's motion to suppress the computer files, holding that the search of Roberts' luggage had been a "routine search" for which no suspicion was required, even though the justification for the search offered by the agents merely had been a pretext. See id. at 686, 688 (citing Whren v. United States, 517 U.S. 806 (1996)). The court also concluded that Roberts' consent justified the search of the laptop and diskettes, and indicated that even if Roberts had not consented to the search, "[t]he search of the defendant's computer and diskettes would have been a routine export search, valid under the Fourth Amendment." See Roberts, 98 F. Supp. 2d at 688. On appeal, the Fifth Circuit affirmed the district court's refusal to suppress the evidence on the grounds that the initial jetway search of Roberts was justified by reasonable suspicion that Roberts possessed child pornography, and that the subsequent search and seizure of computer equipment was justified by probable cause. See id. at 1017. The court did not reach the issue of whether the seizure of Roberts' computer equipment could be considered routine.

Importantly, agents and prosecutors should not interpret Roberts as permitting the interception of data transmitted electronically to and from the United States. Any real-time interception of electronically transmitted data in the United States must comply strictly with the requirements of Title III, 18 U.S.C. §§ 2510-2522, or the Pen/Trap statute, 18 U.S.C. §§ 3121-3127. See generally Chapter 4. Further, once electronically transferred data from outside the United States arrives at its destination within the United States, the government ordinarily cannot rely on the border search exception to search for and seize the data because the data is no longer at the border or its functional equivalent. Cf. Almeida-Sanchez v. United States, 413 U.S. 266, 273-74 (1973) (concluding that a search that occurred 25 miles from the United States border did not qualify for the border search exception, even though the search occurred on a highway known as a common route for illegal aliens, because it did not occur at the border or its functional equivalent).

7. International Issues

Increasingly, electronic evidence necessary to prevent, investigate, or prosecute a crime may be located outside the borders of the United States. This can occur for several reasons. Criminals can use the Internet to commit or facilitate crimes remotely, e.g., when Russian hackers steal money from a bank in New York, or when the kidnappers of an American deliver demands by e-mail for release of their captive. Communications also can be "laundered" through third countries, such as when a criminal in Brooklyn uses the Internet to pass a communication through Tokyo, Tel Aviv, and Johannesburg, before it reaches its intended recipient in Manhattan - much the way monies can be laundered through banks in different countries in order to hide their source. In addition, provider architecture may route or store communications in the country where the provider is based, regardless of the location of its users.

When United States authorities investigating a crime believe electronic evidence is stored by an Internet service provider or on a computer located abroad (in "Country A"), U.S. law enforcement usually must seek assistance from law enforcement authorities in Country A. Since, in general, law enforcement officers exercise their functions in the territory of another country with the consent of that country, U.S. law enforcement should only make direct contact with an ISP located in Country A with (1) prior permission of the foreign government; (2) approval of DOJ's Office of International Affairs ("OIA") (which would know of particular sensitivities and/or accepted practices); or (3) other clear indicia that such practice would not be objectionable in Country A. (There is general agreement that access to publicly available materials in Country A, such as those posted to a public Web site, and access to materials in Country A with the consent of the owner/custodian of those materials, are permissible without prior consultations.)

Under certain circumstances, foreign law enforcement authorities may be able to share evidence informally with U.S. counterparts. However, finding the appropriate official in Country A with which to explore such cooperation is an inexact science, at best. Possible avenues for entree to foreign law enforcement are: (1) the designated expert who participates in the G8's network of international high-tech crime points of contact (discussed below); (2) law enforcement contacts maintained by OIA; (3) representatives of U.S. law enforcement agencies who are stationed at the relevant American Embassy (e.g., FBI Legal Attaches, or "LegAtts," and agents from the U.S. Secret Service and U.S. Customs Service); and (4) the Regional Security Officer (from the Diplomatic Security Service) at the American Embassy (who may have good in-country law enforcement contacts). OIA can be reached at 202-514-0000.

Where Country A cannot otherwise provide informal assistance, requests for evidence usually will be made under existing Mutual Legal Assistance Treaties (MLATs) or Mutual Legal Assistance Agreements, or through the Letters Rogatory process. See 28 U.S.C. § 1781-1782. These official requests for assistance are made by OIA to the designated "Central Authority" of Country A or, in the absence of an MLAT, to other appropriate authorities. (Central Authorities are usually located within the Justice Ministry, or other Ministry or office in Country A that has law enforcement authority.) OIA has attorneys responsible for every country and region of the world. Since official requests of this nature require specified documents and procedures, and can take some time to produce results, law enforcement should contact OIA as soon as a request for international legal assistance becomes a possibility.

When U.S. law enforcement has reason to believe that electronic evidence exists on a computer or computer network located abroad, and expects a delay before that evidence is secured in Country A, a request to foreign law enforcement for preservation of the evidence should be made as soon as possible. Such request, similar to a request under 18 U.S.C. § 2703(f) to a U.S. provider (see Chapter 3.G.1, p.

101), will have varying degrees of success based on several factors, most notably whether Country A has a data preservation law, and whether the U.S. has sufficient law enforcement contacts in Country A to ensure prompt execution of the request. The Council of Europe Cybercrime Convention, completed in 2001, obligates all signatories to have the ability to affect cross-border preservation requests, and the availability of this critical form of assistance therefore is expected to increase greatly in the near future. To secure preservation, or in emergencies when immediate international assistance is required, the international Network of 24-hour Points of Contact established by the High-tech Crime Subgroup of the G8 countries can provide assistance. This network, created in 1997, is comprised of approximately twenty-eight member countries, and continues to grow every year.(5) Participating countries have a dedicated computer crime expert and a means to contact that office or person twenty-four hours a day. See generally Michael A. Sussmann, *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium*, 9 Duke J. Comp. & Int'l L. 451, 484 (1999). CCIPS is the point of contact for the United States and can be contacted at 202-514-1026 during regular business hours or at other times through the Department of Justice Command Center at 202-514-5000. The Council of Europe's Cybercrime Convention obligates all signatory countries to have a 24-hour point of contact for cybercrime cases, and international 24-hour response capabilities are therefore expected to continue to increase. In addition, CCIPS has high-tech law enforcement contacts in many countries that are not a part of the G8's network or the Council of Europe; agents and prosecutors should call CCIPS for assistance.

In the event that United States law enforcement inadvertently accesses a computer located in another country, CCIPS, OIA, or another appropriate authority should be consulted immediately, as issues such as sovereignty and comity may be implicated. Likewise, if exigencies such as terrorist threats raise the possibility of direct access of a computer located abroad by United States law enforcement, appropriate U.S. authorities should be consulted immediately.

Searching, seizing, or otherwise obtaining electronic evidence located outside of the United States can raise difficult questions of both law and policy. For example, the Fourth Amendment may apply under certain circumstances, but not under others. See generally, United States v. Verdugo-Urquidez, 494 U.S. 259 (1990) (considering the extent to which the Fourth Amendment applies to searches outside of the United States). This manual does not attempt to provide detailed guidance on how to resolve difficult international issues that may arise in cases involving electronic evidence located beyond our borders. Investigators and prosecutors should contact CCIPS or OIA for assistance in particular cases.

D. Special Case: Workplace Searches

Warrantless workplace searches occur often in computer cases and raise unusually complicated legal issues. The starting place for such analysis is the Supreme Court's complex decision in O'Connor v. Ortega, 480 U.S. 709 (1987). Under O'Connor, the legality of warrantless workplace searches depends on often-subtle factual distinctions such as whether the workplace is public sector or private sector, whether employment policies exist that authorize a search, and whether the search is work-related. Every warrantless workplace search must be evaluated carefully on its facts. In general, however, law enforcement officers can conduct a warrantless search of private (i.e., non-government) workplaces only if the officers obtain the consent of either the employer or another employee with common authority over the area searched. In public (i.e., government) workplaces, officers cannot rely on an employer's consent, but can conduct searches if written employment policies or office practices establish that the government employees targeted by the search cannot reasonably expect privacy in their workspace. Further, government employers and supervisors can conduct reasonable work-related searches of employee workspaces without a warrant even if the searches violate employees' reasonable expectation of privacy.

One cautionary note is in order here. This discussion evaluates the legality of warrantless workplace searches of computers under the Fourth Amendment. In many cases, however, workplace searches will implicate federal privacy statutes in addition to the Fourth Amendment. For example, efforts to obtain an employee's files and e-mail from the employer's network server raise issues under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701-2712 (discussed in Chapter 3), and workplace monitoring of an employee's Internet use implicates Title III, 18 U.S.C. §§ 2510-2522 (discussed in Chapter 4). Before conducting a workplace search, investigators must make sure that their search will not violate either the Fourth Amendment or relevant federal privacy statutes. Investigators should contact CCIPS at (202) 514-1026 or the CTC in their district (see Introduction, p. ix) for further assistance.

1. Private Sector Workplace Searches

The rules for conducting warrantless searches and seizures in private-sector workplaces generally mirror the rules for conducting warrantless searches in homes and other personal residences. Private company employees generally retain a reasonable expectation of privacy in their workplaces. As a result, searches by law enforcement of a private workplace will usually require a warrant unless the agents can obtain the consent of an employer or a co-worker with common authority.

a) Reasonable Expectation of Privacy in Private-Sector Workplaces

Private-sector employees will usually retain a reasonable expectation of privacy in their office space. In Mancusi v. DeForte, 392 U.S. 364 (1968), police officers conducted a warrantless search of an office at a local union headquarters that defendant Frank DeForte shared with several other union officials. In response to DeForte's claim that the search violated his Fourth Amendment rights, the police officers argued that the joint use of the space by DeForte's co-workers made his expectation of privacy unreasonable. The Court disagreed, stating that DeForte "still could reasonably have expected that only [his officemates] and their personal or business guests would enter the office, and that records would not be touched except with their permission or that of union higher-ups." Id. at 369. Because only a specific group of people actually enjoyed joint access and use of DeForte's office, the officers' presence violated DeForte's reasonable expectation of privacy. See id. See also United States v. Most, 876 F.2d 191, 198 (D.C. Cir. 1989) ("[A]n individual need not shut himself off from the world in order to retain his fourth amendment rights. He may invite his friends into his home but exclude the police; he may share his office with co-workers without consenting to an official search."); United States v. Lyons, 706 F.2d 321, 325 (D.C. Cir. 1983) ("One may freely admit guests of one's choosing -- or be legally obligated to admit specific persons -- without sacrificing one's right to expect that a space will remain secure against all others."). As a practical matter, then, private employees will generally retain an expectation of privacy in their work space unless that space is "open to the world at large." Id. at 326.

b) Consent in Private Sector-Workplaces

Although most non-government workplaces will support a reasonable expectation of privacy from a law enforcement search, agents can defeat this expectation by obtaining the consent of a party who exercises common authority over the area searched. See Matlock, 415 U.S. at 171. In practice, this means that agents can often overcome the warrant requirement by obtaining the consent of the target's employer or supervisor. Depending on the facts, a co-worker's consent may suffice as well.

Private-sector employers and supervisors generally enjoy a broad authority to consent to searches in the workplace. For example, in United States v. Gargiso, 456 F.2d 584 (2d Cir. 1972), a pre-Matlock case, agents conducting a criminal investigation of an employee of a private company sought access to a locked, wired-off area in the employer's basement. The agents explained their needs to the company's vice-president, who took the agents to the basement and opened the basement with his key. When the employee attempted to suppress the evidence that the agents discovered in the basement, the court held that the vice-president's consent was effective. Because the vice-president shared supervisory power over the basement with the employee, the court reasoned, he could consent to the agents' search of that area. See id. at 586-87. See also United States v. Bilanzich, 771 F.2d 292, 296-97 (7th Cir. 1985) (holding that the owner of a hotel could consent to search of locked room used by hotel employee to store records, even though owner did not carry a key, because employee worked at owner's bidding); J.L. Foti Constr. Co. v. Donovan, 786 F.2d 714, 716-17 (6th Cir. 1986) (per curiam) (holding that a general contractor's superintendent could consent to an inspection of an entire construction site, including subcontractor's work area). In a close case, an employment policy or computer network banner that establishes the employer's right to consent to a workplace search can help establish the employer's common authority to consent under Matlock. See Appendix A.

Agents should be careful about relying on a co-worker's consent to conduct a workplace search. While employers generally retain the right to access their employees' work spaces, co-workers may or may not, depending on the facts. When co-workers do exercise common authority over a workspace, however, investigators can rely on a co-worker's consent to search that space. For example, in United States v. Buettner-Janusch, 646 F.2d 759 (2d Cir. 1981), a professor and an undergraduate research assistant at New York University consented to a search of an NYU laboratory managed by a second professor suspected of using his laboratory to manufacture LSD and other drugs. Although the search involved opening vials and several other closed containers, the Second Circuit held that Matlock authorized the search because both consenting co-workers had been authorized to make full use of the lab for their research. See id. at 765-66. See also United States v. Jenkins, 46 F.3d 447, 455-58 (5th Cir. 1995) (allowing an employee to consent to a search of the employer's property); United States v. Murphy, 506 F.2d 529, 530 (9th Cir. 1974) (per curiam) (same); United States v. Longo, 70 F. Supp. 2d 225, 256 (W.D.N.Y. 1999) (allowing secretary to consent to search of employer's computer). But see United States v. Buitrago Pelaez, 961 F. Supp. 64, 67-68 (S.D.N.Y. 1997) (holding that a receptionist could consent to a general search of the office, but not of a locked safe to which receptionist did not know the combination).

c) Employer Searches in Private-Sector Workplaces

Warrantless workplace searches by private employers rarely violate the Fourth Amendment. So long as the employer is not acting as an instrument or agent of the Government at the time of the search, the search is a private search and the Fourth Amendment does not apply. See Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614 (1989).

2. Public-Sector Workplace Searches

Although warrantless computer searches in private-sector workplaces follow familiar Fourth Amendment rules, the application of the Fourth Amendment to public-sector workplace searches of computers presents a different matter. In O'Connor v. Ortega, 480 U.S. 709 (1987), the Supreme Court introduced a distinct framework for evaluating warrantless searches in government workplaces, a framework that applies to computer searches. According to O'Connor, a government employee can enjoy a reasonable expectation of privacy in his workplace. See id. at 717 (O'Connor, J., plurality opinion); id. at 721 (Scalia, J., concurring). However, an expectation of privacy becomes unreasonable if "actual office practices and procedures, or . . . legitimate regulation" permit the employee's supervisor, co-workers, or the public to enter the employee's workspace. Id. at 717 (O'Connor, J., plurality opinion). Further, employers can conduct "reasonable" warrantless searches even if the searches violate an employee's reasonable expectation of privacy. Such searches include work-related, noninvestigatory intrusions (e.g., entering an employee's locked office to retrieve a file) and reasonable investigations into work-related misconduct. See id. at 725-26 (O'Connor, J., plurality opinion); id. at 732 (Scalia, J., concurring).

a) Reasonable Expectation of Privacy in Public Workplaces

The reasonable expectation of privacy test formulated by the O'Connor plurality asks whether a government employee's workspace is "so open to fellow employees or to the public that no expectation of privacy is reasonable." O'Connor, 480 U.S. at 718 (plurality opinion). This standard differs significantly from the standard analysis applied in private workplaces. Whereas private-sector employees enjoy a reasonable expectation of privacy in their workspace unless the space is "open to the world at large," Lyons, 706 F.2d at 326, government employees retain a reasonable expectation of privacy in the workplace only if a case-by-case inquiry into "actual office practices and procedures" shows that it is reasonable for employees to expect that others will not enter their space. See O'Connor, 480 U.S. at 717 (plurality opinion); Rossi v. Town of Pelham, 35 F. Supp. 2d. 58, 63-64 (D.N.H. 1997). See also O'Connor, 480 U.S. at 730-31 (Scalia, J., concurring) (noting the difference between the expectation-of-privacy analysis offered by the O'Connor plurality and that traditionally applied in private workplace searches). From a practical standpoint, then, public employees are less likely to retain a reasonable expectation of privacy against government searches at work than are private employees. Courts evaluating public employees' reasonable expectation of privacy in the wake of O'Connor have considered the following factors: whether the work area in question is assigned solely to the employee; whether others have access to the space; whether the nature of the employment requires a close working relationship with others; whether office regulations place employees on notice that certain areas are subject to search; and whether the property searched is public or private. See Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174, 179-80 (1st Cir. 1997) (summarizing cases); United States v. Mancini, 8 F.3d 104, 109 (1st Cir. 1993). In general, the courts have rejected claims of an expectation of privacy in an office when the employee knew or should have known that others could access the employee's workspace. See, e.g., Sheppard v. Beerman, 18 F.3d 147, 152 (2d Cir. 1994) (holding that judge's search through his law clerk's desk and file cabinets did not violate the clerk's reasonable expectation of privacy because of the clerk's close working relationship with the judge); Schowengerdt v. United States, 944 F.2d 483, 488 (9th Cir. 1991) (holding that civilian engineer employed by the Navy who worked with classified documents at an ordinance plant had no reasonable expectation of privacy in his office because investigators were known to search employees' offices for evidence of misconduct on a regular basis). But see United States v. Taketa, 923 F.2d 665, 673 (9th Cir. 1991) (concluding in *dicta* that public employee retained expectation of privacy in office shared with several co-workers). In contrast, the courts have found that a search violates a public employee's reasonable expectation of privacy when the employee had no reason to expect that others would access the space searched. See O'Connor, 480 U.S. at 718-19 (plurality) (holding that physician at state hospital retained expectation of privacy in his desk and file cabinets where there was no evidence that other employees could enter his office and access its contents); Rossi, 35 F. Supp. 2d at 64 (holding that town clerk enjoyed reasonable expectation of privacy in 8' x 8' office that the public could not access and other town employees did not enter). While agents must evaluate whether a public employee retains a reasonable expectation of privacy in the workplace on a case-by-case basis, official written employment policies can simplify the task dramatically. See O'Connor, 480 U.S. at 717 (plurality) (noting that "legitimate regulation" of the work place can reduce public employees' Fourth Amendment protections). Courts have uniformly deferred to public employers' official policies that expressly authorize access to the employee's workspace, and have relied on such policies when ruling that the employee cannot retain a reasonable expectation of privacy in the workplace. See American Postal Workers Union, Columbus Area Local AFL-CIO v. United States Postal Serv., 871 F.2d 556, 59-61 (6th Cir. 1989) (holding that postal employees retained no reasonable expectation of privacy in contents of government lockers after signing waivers stating that

lockers were subject to inspection at any time, even though lockers contained personal items); United States v. Bunkers, 521 F.2d 1217, 1219-1221 (9th Cir. 1975) (same, noting language in postal manual stating that locker is "subject to search by supervisors and postal inspectors"). Of course, whether a specific policy eliminates a reasonable expectation of privacy is a factual question. Employment policies that do not explicitly address employee privacy may prove insufficient to eliminate Fourth Amendment protection. See, e.g., Taketa, 923 F.2d at 672-73 (concluding that regulation requiring DEA employees to "maintain clean desks" did not defeat workplace expectation of privacy of non-DEA employee assigned to DEA office).

When planning to search a government computer in a government workplace, agents should look for official employment policies or "banners" that can eliminate a reasonable expectation of privacy in the computer.

Written employment policies and "banners" are particularly important in cases that consider whether government employees enjoy a reasonable expectation of privacy in government computers. Banners are written notices that greet users before they log on to a computer or computer network, and can inform users of the privacy rights that they do or do not retain in their use of the computer or network. See generally Appendix A.

In general, government employees who are notified that their employer has retained rights to access or inspect information stored on the employer's computers can have no reasonable expectation of privacy in the information stored there. For example, in United States v. Simons, 206 F.3d 392 (4th Cir. 2000), computer specialists at a division of the Central Intelligence Agency learned that an employee named Mark Simons had been using his desktop computer at work to obtain pornography available on the Internet, in violation of CIA policy. The computer specialists accessed Simons' computer remotely without a warrant, and obtained copies of over a thousands picture files that Simons had stored on his hard drive. Many of these picture files contained child pornography, which were turned over to law enforcement. When Simons filed a motion to suppress the fruits of the remote search of his hard drive, the Fourth Circuit held that the CIA division's official Internet usage policy eliminated any reasonable expectation of privacy that Simons might otherwise have in the copied files. See id. at 398. The policy stated that the CIA division would "periodically audit, inspect, and/or monitor [each] user's Internet access as deemed appropriate," and that such auditing would be implemented "to support identification, termination, and prosecution of unauthorized activity." Id. at 395-96. Simons did not deny that he was aware of the policy. See id. at 398 n.8. In light of the policy, the Fourth Circuit held, Simons did not retain a reasonable expectation of privacy "with regard to the record or fruits of his Internet use," including the files he had downloaded. Id. at 398.

Other courts have agreed with the approach articulated in Simons and have held that banners and policies generally eliminate a reasonable expectation of privacy in contents stored in a government employee's network account. See United States v. Angevine, 281 F.3d 1130, 1134-35 (10th Cir. 2002) (holding that banner and computer policy eliminated a public employee's reasonable expectation of privacy in data downloaded from Internet); Wasson v. Sonoma County Junior College, 4 F. Supp. 2d 893, 905-06 (N.D. Cal. 1997) (holding that public employer's computer policy giving the employer "the right to access all information stored on [the employer's] computers" defeats an employee's reasonable expectation of privacy in files stored on employer's computers); Bohach v. City of Reno, 932 F. Supp. 1232, 1235 (D. Nev. 1996) (holding that police officers did not retain a reasonable expectation of privacy in their use of a pager system, in part because the Chief of Police had issued an order announcing that all messages would be logged); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (holding that Air Force sergeant did not have a reasonable expectation of privacy in his government e-mail account because e-mail use was reserved for official business and network banner

informed each user upon logging on to the network that use was subject to monitoring). But see DeMaine v. Samuels, 2000 WL 1658586, at *7 (D. Conn. Sept. 25, 2000) (suggesting that the existence of an employment manual explicitly authorizing searches "weighs heavily" in the determination of whether a government employee retained a reasonable expectation of privacy at work, but "does not, on its own, dispose of the question"). Conversely, a court may note the absence of a banner or computer policy in finding that an employee has a reasonable expectation of privacy in the use of his computer. See United States v. Slanina, 283 F.3d 670, 676-77 (5th Cir. 2002).

Of course, whether a specific policy eliminates a reasonable expectation of privacy is a factual question. Agents and prosecutors must consider whether a given policy is broad enough to reasonably contemplate the search to be conducted. If the policy is narrow, it may not waive the government employee's reasonable expectation of privacy against the search that the government plans to execute. For example, in Simons, the Fourth Circuit concluded that although the CIA division's Internet usage policy eliminated Simons' reasonable expectation of privacy in the fruits of his Internet use, it did *not* eliminate his reasonable expectation of privacy in the physical confines of his office. See Simons, 206 F.3d at 399 n.10. Accordingly, the policy by itself was insufficient to justify a physical entry into Simons' office. See id. at 399. See also Taketa, 923 F.2d at 672-73 (concluding that regulation requiring DEA employees to "maintain clean desks" did not defeat workplace expectation of privacy of non-DEA employee assigned to DEA office). Sample banners appear in Appendix A.

b) "Reasonable" Workplace Searches Under O'Connor v. Ortega

Government employers and their agents can conduct "reasonable" work-related searches even if those searches violate an employee's reasonable expectation of privacy.

In most circumstances, a warrant must be obtained before a government actor can conduct a search that violates an individual's reasonable expectation of privacy. In the context of government employment, however, the government's role as an employer (as opposed to its role as a law-enforcer) presents a special case. In O'Connor, the Supreme Court held that a public employer or the employer's agent can conduct a workplace search that violates a public employee's reasonable expectation of privacy so long as the search is "reasonable." See O'Connor, 480 U.S. at 722-23 (plurality); Id. at 732 (Scalia, J., concurring). The Court's decision adds public workplace searches by employers to the list of "special needs" exceptions to the warrant requirement. The "special needs" exceptions permit the government to dispense with the usual warrant requirement when its officials infringe upon protected privacy rights in the course of acting in a non-law enforcement capacity. See, e.g., New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring) (applying the "special needs" exception to permit public school officials to search student property without a warrant in an effort to maintain discipline and order in public schools); National Treasury Employees Union v. Von Raab, 489 U.S. 656, 677 (1989) (applying the "special needs" exception to permit warrantless drug testing of Customs employees who seek promotions to positions where they would handle sensitive information). In these cases, the Court has held that the need for government officials to pursue legitimate non-law-enforcement aims justifies a relaxing of the warrant requirement because "the burden of obtaining a warrant is likely to frustrate the [non-law-enforcement] governmental purpose behind the search." O'Connor, 480 U.S. at 720 (quoting Camara v. Municipal Court, 387 U.S. 523, 533 (1967)).

According to O'Connor, a warrantless search must satisfy two requirements to qualify as "reasonable." First, the employer or his agents must participate in the search for a work-related reason, rather than merely to obtain evidence for use in criminal proceedings. Second, the search must be justified at its inception and permissible in its scope.

i) The Search Must Be Work-Related

The first element of O'Connor's reasonableness test requires that the employer or his agents must participate in the search for a work-related reason, rather than merely to obtain evidence for use in criminal proceedings. See O'Connor, 480 U.S. at 721. This element limits the O'Connor exception to circumstances in which the government actors who conduct the search act in their capacity as employers, rather than law enforcers. The O'Connor Court specified two such circumstances. First, the Court concluded that public employers can conduct reasonable work-related noninvestigatory intrusions, such as entering an employee's office to retrieve a file or report while the employee is out. See id. at 721-22 (plurality); Id. at 732 (Scalia, J., concurring). Second, the Court concluded that employers can conduct reasonable investigations into an employee's work-related misconduct, such as entering an employee's office to investigate employee misfeasance that threatens the efficient and proper operation of the office. See id. at 724 (plurality); Id. at 732 (Scalia, J., concurring).

The line between a legitimate work-related search and an illegitimate search for criminal evidence is clear in theory, but often blurry in fact. Public employers who learn of misconduct at work may investigate it with dual motives: they may seek evidence both to root out "inefficiency, incompetence, mismanagement, or other work-related misfeasance," id. at 724, and also to collect evidence for a criminal prosecution. Indeed, the two categories may merge altogether. For example, government officials who have criminal investigators under their command may respond to allegations of work-related misconduct by directing the investigators to search employee offices for evidence of a crime. The courts have adopted fairly generous interpretations of O'Connor when confronted with mixed-motive searches. In general, the presence and involvement of law enforcement officers will not invalidate the search so long as the employer or his agent participates in the search for legitimate work-related reasons. See, e.g., United States v. Slanina, 283 F.3d 670, 678 (5th Cir. 2002) (approving search by official in charge of fire and police departments and stating that "O'Connor's goal of ensuring an efficient workplace should not be frustrated simply because the same misconduct that violates a government employer's policy also happens to be illegal"); Gossmeyer v. McDonald, 128 F.3d 481, 492 (7th Cir. 1997) (concluding that presence of law enforcement officers in a search team looking for evidence of work-related misconduct does not transform search into an illegitimate law enforcement search); Taketa, 923 F.2d at 674 (concluding that search of DEA office space by DEA agents investigating allegations of illegal wiretapping "was an internal investigation directed at uncovering work-related employee misconduct."). Shields v. Burge, 874 F.2d 1201, 1202-05 (7th Cir. 1989) (applying the O'Connor exception to an internal affairs investigation of a police sergeant that paralleled a criminal investigation); Ross v. Hinton, 740 F. Supp. 451, 458 (S.D. Ohio 1990) (concluding that a public employer's discussions with law enforcement officer concerning employee's alleged criminal misconduct, culminating in officer's advice to "secure" the employee's files, did not transform employer's subsequent search of employee's office into a law enforcement search).

Although the presence of law enforcement officers ordinarily will not invalidate a work-related search, a few courts have indicated that whether O'Connor applies depends as much on the identity of the personnel who conduct the search as whether the purpose of the search is work-related. For example, in United States v. Simons, 206 F.3d 392, 400 (4th Cir. 2000), the Fourth Circuit concluded that O'Connor authorized the search of a government employee's office by his supervisor even though the dominant purpose of the search was to uncover evidence of a crime. Because the search was conducted by the employee's supervisor, the Court indicated, it fell within the scope of O'Connor. See id. ("[The employer] did not lose its special need for the efficient and proper operation of the workplace merely because the evidence obtained was evidence of a crime.") (internal quotations and citations omitted). Conversely, one district court has held that the O'Connor exception did not apply when a government

employer sent a uniformed police officer to an employee's office, even though the purpose of the police officer's presence was entirely work-related. See Rossi v. Town of Pelham, 35 F. Supp. 2d 58, 65-66 (D.N.H. 1997) (civil action pursuant to 42 U.S.C. § 1983) (concluding that O'Connor exception did not apply when town officials sent a single police officer to town clerk's office to ensure that clerk did not remove public records from her office before a scheduled audit could occur; the resulting search was a "police intrusion" rather than an "employer intrusion").

Of course, courts will invalidate warrantless workplace searches when the facts establish that law enforcement provided the true impetus for the search, and the search violated an employee's reasonable expectation of privacy. See United States v. Hagarty, 388 F.2d 713, 717 (7th Cir. 1968) (holding that surveillance installed by criminal investigators violated the Fourth Amendment where purpose of surveillance was "to detect criminal activity" rather than "to supervise and investigate" a government employee); United States v. Kahan, 350 F. Supp. 784, 791 (S.D.N.Y. 1972) (invalidating warrantless search of INS employee's wastebasket by INS criminal investigator who searched the employee's wastebasket for evidence of a crime every day after work with the employer's consent), rev'd in part on other grounds, 479 F.2d 290 (2d Cir. 1973), rev'd with directions to reinstate the district court judgment, 415 U.S. 239 (1974).

ii) The Search Must Be Justified At Its Inception And Permissible In Its Scope

To be "reasonable" under the Fourth Amendment, a work-related employer search of the type endorsed in O'Connor must also be both "justified at its inception," and "permissible in its scope." O'Connor, 480 U.S. at 726 (plurality). A search will be justified at its inception "when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose." Id. See, e.g., Simons, 206 F.3d at 401 (holding that entrance into employee's office to seize his computer was justified at its inception because employer knew that employee had used the computer to download child pornography); Gossmeyer, 128 F.3d at 491 (holding that co-worker's specific allegations of serious misconduct made Sheriff's search of Child Protective Investigator's locked desk and file cabinets justified at its inception); Taketa, 923 F.2d at 674 (concluding that report of misconduct justified initial search of employee's office); Shields, 874 F.2d at 1204 (suggesting in *dicta* that search of police officer's desk for narcotics pursuant to internal affairs investigation might be reasonable following an anonymous tip); DeMaine v. Samuels, 2000 WL 1658586, at * 10 (D. Conn. Sept. 25, 2000) (holding that search of police officer's day planner was justified by information from two reliable sources that the officer kept detailed attendance notes relevant to overtime investigation involving other officers); Williams v. Philadelphia Housing Auth., 826 F. Supp. 952, 954 (E.D. Pa. 1993) (concluding that employee's search for a computer disk in employee's office was justified at its inception because employer needed contents of disk for official purposes). Compare Ortega v. O'Connor, 146 F.3d 1149, 1162 (9th Cir. 1998) (concluding that vague, uncorroborated and stale complaints of misconduct do not justify a decision to search an employee's office).

A search will be "permissible in its scope" when "the measures adopted are reasonably related to the objectives of the search and [are] not excessively intrusive in light of the nature of the misconduct." O'Connor, 480 U.S. at 726 (plurality) (internal quotations omitted). This standard requires employers and their agents to tailor work-related searches to the alleged misfeasance. See, e.g., Leventhal v. Knapek, 266 F.3d 64, 75-77 (2d Cir. 2001) (holding that search for the presence of non-agency-approved software on employee's computer was not excessively intrusive because officials searched only file names at first and then searched only suspicious directories on subsequent visits); Simons, 206 F.3d at 401 (holding that search for child pornography believed to be stored in employee's computer was permissible in scope because individual who conducted the search "simply crossed the floor of [the

defendant's] office, switched hard drives, and exited"); Gossmeyer, 128 F.3d at 491 (concluding that workplace search for images of child pornography was permissible in scope because it was limited to places where such images would likely be stored); Samuels, 2000 WL 1658586, at *10 (holding that search through police officer's day planner was reasonable because Internal Affairs investigators had reason to believe day planner contained information relevant to investigation of overtime abuse). If employers conduct a search that unreasonably exceeds the scope necessary to pursue the employer's legitimate work-related objectives, the search will be "unreasonable" and will violate the Fourth Amendment. See O'Connor, 146 F.3d at 1163 (concluding that "a general and unbounded" search of an employee's desk, cabinets, and personal papers was impermissible in scope where the search team did not attempt to limit their investigation to evidence of alleged misconduct).

c) Consent in Public-Sector Workplaces

Although public employers may search employees' workplaces without a warrant for work-related reasons, public workplaces offer a more restrictive milieu in one respect. In government workplaces, employers acting in their official capacity generally cannot consent to a law enforcement search of their employees' offices. See United States v. Blok, 188 F.2d 1019, 1021 (D.C. Cir. 1951) (concluding that a government supervisor cannot consent to a law enforcement search of a government employee's desk); Taketa, 923 F.2d at 673; Kahan, 350 F. Supp. at 791. The rationale for this result is that the Fourth Amendment cannot permit one government official to consent to a search by another. See Blok, 188 F.2d at 1021 ("Operation of a government agency and enforcement of criminal law do not amalgamate to give a right of search beyond the scope of either."). Accordingly, law enforcement searches conducted pursuant to a public employer's consent must be evaluated under O'Connor rather than the third-party consent rules of Matlock. The question in such cases is not whether the public employer had common authority to consent to the search, but rather whether the combined law enforcement and employer search satisfied the Fourth Amendment standards of O'Connor v. Ortega. </SPAN

II. SEARCHING AND SEIZING COMPUTERS WITH A WARRANT

A. Introduction

The legal framework for searching and seizing computers with a warrant largely mirrors the legal framework for other searches and seizures. As with any kind of search pursuant to a warrant, law enforcement must establish "probable cause, supported by Oath or affirmation," and must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. Amend. 4. Despite the common legal framework, computer searches differ from other searches because computer technologies frequently force agents to execute computer searches in nontraditional ways. Consider the traditional case of a warrant to seize a stolen car from a private parking lot. Agents generally can assume that the lot will still exist in its prior location when the agents execute the search, and can assume they will be able to identify the stolen car quickly based on the car's model, make, license plate, or Vehicle Identification Number. As a result, the process of drafting the warrant and executing the search is relatively simple. After the agents establish probable cause and describe the car and lot to the magistrate judge, the magistrate judge can issue the warrant authorizing the agents to go to the lot and retrieve the car.

Searches for computer files tend to be more complicated. Because computer files consist of electrical impulses that can be stored on the head of a pin and moved around the world in an instant, agents may not know where computer files are stored, or in what form. Files may be stored on a floppy diskette, on a hidden directory in a suspect's laptop, or on a remote server located thousands of miles away. The files may be encrypted, misleadingly titled, stored in unusual file formats, or commingled with millions of unrelated, innocuous, and even statutorily protected files. As a result of these uncertainties, agents cannot simply establish probable cause, describe the files they need, and then "go" and "retrieve" the data. Instead, they must understand the technical limits of different search techniques, plan the search carefully, and then draft the warrant in a manner that authorizes the agents to take necessary steps to obtain the evidence they need.

Searching and seizing computers with a warrant is as much an art as a science. In general, however, agents and prosecutors have found that they can maximize the likelihood of a successful search and seizure by following these four steps:

1) Assemble a team consisting of the case agent, the prosecutor, and a technical expert as far in advance of the search as possible.

Although the lead investigating agent is the central figure in most searches, computer searches generally require a team with three important players: the agent, the prosecutor, and a technical specialist with expertise in computers and computer forensics. In most computer searches, the case agent organizes and directs the search, learns as much as possible about the computers to be searched, and writes the affidavit establishing probable cause. The technical specialist explains the technical limitations that govern the search to the case agent and prosecutor, creates the plan for executing the search, and in many cases takes the lead role in executing the search itself. Finally, the prosecutor reviews the affidavit and warrant and makes sure that the entire process complies with the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure. Of course, each member of the team should collaborate with the others to help ensure an effective search.

There are many sources of technical expertise in the federal government. Most agencies that have law enforcement investigators also have technical specialists trained in computer forensics. For example, the FBI has Computer Analysis Response Team (CART) examiners, the Internal Revenue Service has Seized Computer Evidence Recovery (SCER) specialists, and the Secret Service has the Electronic Crime Special Agent Program (ECSAP). Investigating agents should contact the technical experts within their own agency. Further, some agencies offer case agents sufficient technical training that they may also be able to act as technical specialists. In such cases, the case agents normally do not need to consult with technical experts and can serve as technical specialists and case agents simultaneously.

2) Learn as much as possible about the computer system that will be searched before devising a search strategy or drafting the warrant.

After assembling the team, the case agent should begin acquiring as much information as possible about the computer system targeted by the search. It is difficult to overstate the importance of this step. For the most part, the need for detailed and accurate information about the targeted computer results from practical considerations. Until the agent has learned what kinds of computers and operating systems the target uses, it is impossible to know how the information the system contains can be retrieved, or even where the information may be located. Every computer and computer network is different, and subtle differences in hardware, software, operating systems, and system configuration can alter the search plan dramatically. For example, a particular search strategy may work well if a targeted network runs the Linux operating system, but might not work if the network runs Windows NT instead.

These concerns are particularly important when searches involve complicated computer networks (as opposed to stand-alone PCs). For example, the mere fact that a business uses computers in its offices does not mean that the devices found there actually contain any useful information. Businesses may contract with network service providers that store the business's information on remote network servers located miles (possibly thousands of miles) away. As a result of these considerations, a technical specialist cannot advise the case agent on the practical aspects of different search strategies without knowing the nature of the computer system to be searched. Agents need to learn as much as possible about the targeted computer before drafting the warrant, including (if possible) the hardware, the software, the operating system, and the configuration of the network.

Obtaining detailed and accurate information about the targeted computer also has important legal implications. For example, the incidental seizure of First Amendment materials such as drafts of newsletters or web pages may implicate the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the incidental seizure and subsequent search through network accounts may raise issues under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2701-2712 (see generally Parts B.2 and B.3, infra). To minimize liability under these statutes, agents should conduct a careful investigation into whether and where First Amendment materials and network accounts may be stored on the computer system targeted by the search. At least one court has suggested that a failure to conduct such an investigation can deprive the government of a good faith defense against liability under these statutes. 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).

On a practical level, agents may take various approaches to learning about a targeted computer network. In some cases, agents can interview the system administrator of the targeted network (sometimes in an undercover capacity), and obtain all or most of the information the technical specialist needs to plan and execute the search. When this is impossible or dangerous, more piecemeal strategies may prove effective. For example, agents sometimes conduct on-site visits (often undercover) that at least reveal some elements of the hardware involved. A useful source of information for networks connected to the Internet is the Internet itself. It is often possible for members of the public to use network queries to

determine the operating system, machines, and general layout of a targeted network connected to the Internet (although it may set off alarms at the target network).

3) Formulate a strategy for conducting the search (including a backup plan) based on the known information about the targeted computer system.

With a team in place and the targeted system researched, the next step is to formulate a strategy for conducting the search. For example, will the agents search through the targeted computer(s) on the premises, or will they simply enter the premises and remove all of the hardware? Will the agents make copies of individual files, or will they make exact copies of entire hard drives? What will the agents do if their original plan fails, or if the computer hardware or software turns out to be significantly different from what they expected? These decisions hinge on a series of practical and legal considerations. In most cases, the search team should decide on a preferred search strategy, and then plan a series of backup strategies if the preferred strategy proves impractical.

In many cases agents will be unable to learn enough about the computer system to be searched to devise a single or comprehensive search strategy. As a result, agents should recognize how the aspects of the system that they do *not* know about can affect the search strategy. Even where a considerable amount is known about a system, the agents and technicians conducting a review of the data often have to use a number of different techniques in order to thoroughly search a computer and its storage media. Sometimes, seemingly commonplace data or configurations cannot be copied, reviewed or analyzed by one search program or protocol, so another - or several different ones - must be tried. Keyword searches may not be possible until a careful review of a portion of the files is conducted; moreover, a careful data search may reveal other, otherwise unapparent aspects of how the system was used and data generated, accessed, transmitted and stored. It is important for agents to keep such possibilities in mind and to consider and address them as they formulate their strategy.

The issues that must be considered when formulating a strategy to search and seize a computer are discussed in greater depth in section B of this chapter. In general, however, the issues group into four questions: First, what is the most effective search strategy that will comply with Rule 41 and the Fourth Amendment? Second, does the search strategy need to be modified to minimize the possibility of violating either the PPA or ECPA? Third, will the search require multiple warrants? And fourth, should agents ask for special permission to conduct a no-knock or sneak-and-peek search?

4) Draft the warrant, taking special care to describe the object of the search and the property to be seized accurately and particularly, and explain the possible search strategies (as well as the practical and legal issues that helped shape it) in the supporting affidavit.

The essential ingredients for drafting a successful search warrant are covered in Section C, and a practical guide to drafting warrants and affidavits appears in Appendix F. In general, however, the keys to drafting successful computer search warrants are first to describe carefully and particularly the object of the warrant that investigators have probable cause to seize, and second to explain adequately the search strategy in the supporting affidavit. On a practical level, these steps help focus and guide the investigators as they execute the search. As a legal matter, the first step helps to overcome particularity challenges, and the latter helps to thwart claims that the agents executed the search in "flagrant disregard" of the warrant.

B. Planning the Search

1. Basic Strategies for Executing Computer Searches

Computer searches may be executed in a variety of ways. For the most part, there are four possibilities:

- Search the computer and print out a hard copy of particular files at that time;
- Search the computer and make an electronic copy of particular files at that time;
- Create a duplicate electronic copy of the entire storage device on-site, and then later recreate a working copy of the storage device off-site for review;[6] and
- Seize the equipment, remove it from the premises, and review its contents off-site.

Which option is best for any particular search depends on many factors. The single most important consideration is the role of the computer hardware in the offense. It should be noted that the first option, printing out hard copies of particular files, is rarely a good choice. That option may lead to substantial loss of information, including file date and time stamps, file path name, "undo" history, comment fields, and more.

Although every computer search is unique, search strategies often depend on the role of the hardware in the offense. If the 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. If the hardware is merely a storage device for evidence, agents generally will only seize the hardware if less disruptive alternatives are not feasible.

In general, computer hardware can serve one of two roles in a criminal case. First, the computer hardware can be a storage device for evidence of crime. For example, if a suspect keeps evidence of his fraud schemes stored in his personal computer, the hardware itself is merely a container for evidence. The purpose of searching the suspect's computer will be to recover the evidence the computer hardware happens to contain.

In other cases, however, computer hardware can itself be contraband, evidence, an instrumentality, or a fruit of crime. For example, a computer used to transmit child pornography is an instrumentality of crime, and stolen computers are fruits of crime. In such cases, Federal Rule of Criminal Procedure 41 grants agents the right to seize the computer itself, independently from the materials that the hardware happens to contain. See generally Appendix F (explaining the scope of materials that may be seized according to Rule 41). Because Rule 41 authorizes agents to seize hardware in the latter case but not the former, the search strategy for a particular computer search hinges first on the role of the hardware in the offense.[7]

a) When Hardware Is Itself Contraband, Evidence, or an Instrumentality or Fruit of Crime

Under Fed. R. Crim. P. 41(b), agents may obtain search warrants to seize computer hardware if the hardware is contraband, evidence, or an instrumentality or fruit of crime. See Rule 41(b); Appendix F. When the hardware itself may be seized according to Rule 41, agents will usually conduct the search by seizing the computer and searching it off-site. For example, a home personal computer used to store and transmit contraband images is itself an instrumentality of the crime. See Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (computer used to store obscene images); United States v. Lamb, 945 F.

Supp. 441, 462 (N.D.N.Y. 1996) (computer used to store child pornography). Accordingly, Rule 41 permits agents to obtain a warrant authorizing the seizure of the computer hardware. In most cases, investigators will simply 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. In such cases, the agents should explain clearly in the supporting affidavit that they plan to search the computer for evidence and/or contraband after the computer has been seized and removed from the site of the search.

Notably, exceptions exist when agents will not want to seize computer hardware even when the hardware is used as an instrumentality, evidence, contraband, or a fruit of crime. When the "computer" involved is not a stand-alone PC but rather part of a complicated network, the collateral damage and practical headaches that can arise from seizing the entire network often counsel against a wholesale seizure. 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 perhaps obtain a warrant to seize the entire network. However, carting off the entire network might cripple a legitimate, 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. §§ 2701-2712. See generally Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432, 440, 443 (W.D. Tex. 1993) (discussed infra). In such circumstances, agents will want to take a more nuanced approach to obtain the evidence they need. On the other hand, where a network is owned and operated by a criminal enterprise, it may be appropriate to seize the network to stop ongoing criminal activity and prevent further, substantial loss to victims. Such a seizure may require a significant commitment of resources and advanced planning. Agents faced with such a situation can call the Computer Crime and Intellectual Property Section at (202) 514-1026 or the Assistant U.S. Attorney designated as a Computer and Telecommunications Coordinator (CTC) in their district (see Introduction, p. ix) for more specific guidance.

b) When Hardware is Merely a Storage Device for Evidence of Crime

The strategy for conducting a computer search is significantly different if the computer hardware is merely a storage device for evidence of a crime. In such cases, Rule 41(b) authorizes agents to obtain a warrant to seize the electronic evidence, but arguably does not directly authorize the agents to seize the hardware that happens to contain that evidence. Cf. United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982) (noting that probable cause to seize specific paper files enumerated in warrant technically does permit the seizure of commingled innocent files). The hardware is merely a storage container for evidence, not evidence itself. This 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 effective recovery of the evidence is infeasible in the particular circumstances of the case. Cf. id. at 596.

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. See United States v. Santarelli, 778 F.2d 609, 615-16 (11th Cir. 1985). Given that personal computers sold in the year 2002 usually can store the equivalent of thirty 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 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.

In light of these uncertainties, agents often plan to try to search on-site, with the understanding that they will seize the equipment if circumstances discovered on-site make an on-site search infeasible. Once on-site to execute the search, the agents will assess the hardware, software, and resources available to determine whether an on-site search is possible. In many cases, the search strategy will depend on the sensitivity of the environment in which the search occurs. For example, agents seeking to obtain information 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's computers, if possible. In such situations, a tiered search strategy designed to use the least intrusive approach that will recover the information is generally appropriate. Such approaches are discussed in Appendix F. Whatever search strategy is chosen, it should be explained fully in the affidavit supporting the warrant application.

Sometimes, conducting a search on-site will be possible. A friendly employee or system administrator may agree to pinpoint a file or record or may have a recent backup, permitting the agents to obtain a hard copy of the files they seek while on-site. See, e.g., United States v. Longo, 70 F. Supp. 2d 225 (W.D.N.Y. 1999) (upholding pinpoint search aided by suspect's secretary for two particular computer files). Alternatively, agents may be able to locate the targeted set of files and make electronic copies, or may be able to mirror a segment of the storage drive based on knowledge that the information exists within that segment of the drive. Of course, such strategies will frequently prove insufficient. Relatively few cases call for a limited set of known files; searches for evidence of a particular crime are usually more open-ended. If the agents cannot learn where the information is stored or cannot create a working mirror image for technical reasons, they may have no choice but to seize the computer and remove it. Because personal computers are easily moved and can be searched effectively off-site using special forensics tools, agents are particularly likely to seize personal computers absent unusual circumstances.

The general strategy is to pursue the quickest, least intrusive, and most direct search strategy that is consistent with securing the evidence described in the warrant. This strategy will permit agents to search on-site in some cases, and will permit them to seize the computers for off-site review in others. Flexibility is the key.

2. The Privacy Protection Act

When agents have reason to believe that a search may result in a seizure of materials relating to First Amendment activities such as publishing or posting materials on the World Wide Web, they must consider the effect of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa. Every federal computer search that implicates the PPA must be approved by the Justice Department, coordinated through CCIPS at (202) 514-1026.

Under the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, law enforcement must take special steps when planning a search that agents have reason to believe may result in the seizure of certain First Amendment materials. Federal law enforcement searches that implicate the PPA must be pre-approved by a Deputy Assistant Attorney General of the Criminal Division. The Computer Crime and Intellectual Property Section serves as the contact point for all such searches involving computers, and should be contacted directly at (202) 514-1026.

a) A Brief History of the Privacy Protection Act

Before the Supreme Court decided Warden v. Hayden, 387 U.S. 294, 309 (1967), law enforcement officers could not obtain search warrants to search for and seize "mere evidence" of crime. Warrants were permitted only to seize contraband, instrumentalities, or fruits of crime. See Boyd v. United States, 116 U.S. 616 (1886). In Hayden, the Court reversed course and held that the Fourth Amendment permitted the government to obtain search warrants to seize mere evidence. This ruling set the stage for a collision between law enforcement and the press. Because journalists and reporters often collect evidence of criminal activity in the course of developing news stories, they frequently possess "mere evidence" of crime that may prove useful to law enforcement investigations. By freeing the Fourth Amendment from Boyd's restrictive regime, Hayden created the possibility that law enforcement could use search warrants to target the press for evidence of crime it had collected in the course of investigating and reporting news stories.

It did not take long for such a search to occur. On April 12, 1971, the District Attorney's Office in Santa Clara County, California obtained a search warrant to search the offices of The Stanford Daily, a Stanford University student newspaper. The DA's office was investigating a violent clash between the police and demonstrators that had occurred at the Stanford University Hospital three days earlier. The Stanford Daily had covered the incident, and published a special edition featuring photographs of the clash. Believing that the newspaper probably had more photographs of the clash that could help the police identify the demonstrators, the police obtained a warrant and sent four police officers to search the newspaper's office for further evidence that could assist the investigation. The officers found nothing. A month later, however, the Stanford Daily and its editors brought a civil suit against the police claiming that the search had violated their First and Fourth Amendment rights. The case ultimately reached the Supreme Court, and in Zurcher v. Stanford Daily, 436 U.S. 547 (1978), the Court rejected the newspaper's claims. Although the Court noted that "the Fourth Amendment does not prevent or advise against legislative or executive efforts to establish nonconstitutional protections" for searches of the press, it held that neither the Fourth nor First Amendment prohibited such searches. Id. at 567.

Congress passed the PPA in 1980 in response to Stanford Daily. According to the Senate Report, the PPA protected "the press and certain other persons not suspected of committing a crime with protections not provided currently by the Fourth Amendment." S. Rep. No. 96-874, at 4 (1980), reprinted in 1980 U.S.C.C.A.N. 3950. The statute was intended to grant publishers certain statutory rights to discourage

law enforcement officers from targeting publishers simply because they often gathered "mere evidence" of crime. As the legislative history indicates,

the purpose of this statute is to limit searches for materials held by persons involved in First Amendment activities who are themselves not suspected of participation in the criminal activity for which the materials are sought, and not to limit the ability of law enforcement officers to search for and seize materials held by those suspected of committing the crime under investigation.

Id. at 11.

b) The Terms of the Privacy Protection Act

Subject to certain exceptions, the PPA makes it unlawful for a government officer "to search for or seize" materials when

(a) the materials are "work product materials" prepared, produced, authored, or created "in anticipation of communicating such materials to the public," 42 U.S.C. § 2000aa-7(b)(1);

(b) the materials include "mental impressions, conclusions, or theories" of its creator, 42 U.S.C. § 2000aa-7(b)(3); and

(c) the materials are possessed for the purpose of communicating the material to the public by a person "reasonably believed to have a purpose to disseminate to the public" some form of "public communication," 42 U.S.C. §§ 2000aa-7(b)(3), 2000aa(a);

or

(a) the materials are "documentary materials" that contain "information,"

42 U.S.C. § 2000aa-7(a); and

(b) the materials are possessed by a person "in connection with a purpose to disseminate to the public" some form of "public communication." 42 U.S.C. §§ 2000aa(b), 2000aa-7(a).

Although the language of the PPA is broad, the statute contains several exceptions. Searches will not violate the PPA when

1) the only materials searched for or seized are contraband, instrumentalities, or fruits of crime, see 42 U.S.C. § 2000aa-7(a),(b);

2) there is reason to believe that the immediate seizure of such materials is necessary to prevent death or serious bodily injury, see 42 U.S.C. §§ 2000aa(a)(2), 2000aa(b)(2);

3) there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate (an exception which is itself subject to several exceptions), see 42 U.S.C. §§ 2000aa(a)(1), 2000aa(b)(1); and

4) in a search for or seizure of "documentary materials" as defined by § 2000aa-7(a), a subpoena has proven inadequate or there is reason to believe that a subpoena would not result in the production of the materials, see 42 U.S.C. § 2000aa(b)(3)-(4).

Violations of the PPA do not result in suppression of the evidence, see 42 U.S.C. § 2000aa-6(d), but can result in civil damages against the sovereign whose officers or employees execute the search. See § 2000aa-6(a), (e); Davis v. Gracey, 111 F.3d 1472, 1482 (10th Cir. 1997) (dismissing PPA suit against municipal officers in their personal capacities because such suits must be filed only against the "government entity" unless the government entity has not waived sovereign immunity). If State officers or employees violate the PPA and the state does not waive its sovereign immunity and is thus immune from suit, see Barnes v. State of Missouri, 960 F.2d 63, 65 (8th Cir. 1992), individual State officers or employees may be held liable for acts within the scope or under the color of their employment subject to a reasonable good faith defense. See § 2000aa-6(a)(2),(b).

c) Application of the PPA to Computer Searches and Seizures

PPA issues frequently arise in computer cases for two reasons that Congress could not have foreseen in 1980. First, the use of personal computers for publishing and the World Wide Web has dramatically expanded the scope of who is "involved in First Amendment activities." Today, anyone with a computer and access to the Internet may be a publisher who possesses PPA-protected materials on his or her computer.

The second reason that PPA issues arise frequently in computer cases is that the language of the statute does not explicitly rule out liability following *incidental* seizures of PPA-protected materials, and such seizures may result when agents search for and seize computer-stored contraband or evidence of crime that is commingled with PPA-protected materials. For example, investigations into illegal businesses that publish images of child pornography over the Internet have revealed that such businesses frequently support other publishing materials (such as drafts of adult pornography) that may be PPA-protected. Seizing the computer for the contraband necessarily results in the seizure of the PPA-protected materials, because the contraband is commingled with PPA-protected materials on the business's computers. If the PPA were interpreted to forbid such seizures, the statute would not merely deter law enforcement from targeting innocent publishers for their evidence, but also would bar the search and seizure of a criminal suspect's computer if the computer included PPA- protected materials, even incidentally.

The legislative history and text of the PPA indicate that Congress probably intended the PPA to apply only when law enforcement intentionally targeted First Amendment material that related to a crime, as in Stanford Daily. For example, the so-called "suspect exception" eliminates PPA liability when "there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense *to which the materials relate*," 42 U.S.C. § 2000aa(a)(1), § 2000aa(b)(1) (emphasis added). This text indicates that Congress believed that PPA-protected materials would necessarily relate to a criminal offense, as when investigators target the materials as evidence. When agents collaterally seize PPA-protected materials because they are commingled on a computer with other materials properly targeted by law enforcement, however, the PPA-protected materials will not necessarily relate to any crime at all. For example, the PPA-protected materials might be drafts of a horticulture newsletter that just happen to sit on the same hard drive as images of child pornography or records of a fraud scheme.

The Sixth Circuit has explicitly ruled that the incidental seizure of PPA-protected material commingled on a suspect's computer with evidence of a crime does not give rise to PPA liability. Guest v. Leis, 255 F.3d 325 (6th Cir. 2001), involved two lawsuits brought against the Sheriff's Department in Hamilton County, Ohio. The suits arose from the seizures of two servers that had been used to host bulletin board systems suspected of housing evidence and contraband relating to obscenity, phone tapping, child pornography, credit card theft, and software piracy. The Sixth Circuit noted that "when police execute a search warrant for documents on a computer, it will often be difficult or impossible (particularly without the cooperation of the owner) to separate the offending materials from other 'innocent' material on the computer" at the site of the search. Id. at 341-42. Given these pragmatic concerns, the court refused to find PPA-liability for incidental seizures; to construe the PPA otherwise would "prevent police in many cases from seizing evidence located on a computer." Id. at 342. Instead, the court held that "when protected materials are commingled on a criminal suspect's computer with criminal evidence that is unprotected by the act, we will not find liability under the PPA for seizure of the PPA-protected materials." Id. The Guest court cautioned, however, that although the incidental seizure of PPA-related

work-product and documentary materials did not violate the Act, the subsequent search of such material was probably forbidden. Id.

The Sixth Circuit's decision in Guest verifies that the suspect exception works as the legislature intended: limiting the scope of PPA protection to "the press and certain other persons not suspected of committing a crime." S. Rep. No. 96-874, at 4 (1980), reprinted in 1980 U.S.C.C.A.N. 3950. At least one other court has also reached this result by broadly interpreting the suspect exception's phrase "to which materials relate" when an inadvertent seizure of commingled matter occurs. See United States v. Hunter, 13 F. Supp. 2d 574, 582 (D. Vt. 1998) (concluding that materials for weekly legal newsletter published by the defendant from his law office "relate" to the defendant's alleged involvement in his client's drug crimes when the former was inadvertently seized in a search for evidence of the latter). See also Carpa v. Smith, 208 F.3d 220, 2000 WL 189678, at *1 (9th Cir. Feb. 8, 2000) (unpublished) ("[T]he Privacy Protection Act . . . does not apply to criminal suspects.").

The Sixth Circuit's decision in Guest does not address the commingling issue when the owner of the seized computer is not a suspect. In the only published decision to date directly addressing this issue, a district court held the United States Secret Service liable for the inadvertent seizure of PPA-protected materials. See Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), aff'd on other grounds, 36 F.3d 457 (5th Cir. 1994).[8] Steve Jackson Games, Inc. ("SJG") was primarily a publisher of role-playing games, but it also operated a network of thirteen computers that provided its customers with e-mail, published information about SJG products, and stored drafts of upcoming publications. Believing that the system administrator of SJG's computers had stored evidence of crimes, the Secret Service obtained a warrant and seized two of the thirteen computers connected to SJG's network, in addition to other materials. The Secret Service did not know that SJG's computers contained publishing materials until the day after the search. However, the Secret Service did not return the computers it seized until months later. At no time did the Secret Service believe that SJG itself was involved in the crime under investigation.

The district court in Steve Jackson Games ruled that the Secret Service violated the PPA; unfortunately, the exact contours of the court's reasoning are difficult to discern. For example, the court did not explain exactly which of the materials the Secret Service seized were covered by the PPA; instead, the court merely recited the property that had been seized, and concluded that some PPA-protected materials "were obtained" during the search. Id. at 440. Similarly, the court indicated that the search of SJG and the initial seizure of its property did not violate the PPA, but that the Secret Service's continued retention of SJG's property after it learned of SJG's publisher status, and despite a request by SJG for return of the property, was the true source of the PPA violation - something that the statute itself does not appear to contemplate. See id. at 441. The court also suggested that it might have ruled differently if the Secret Service had made "copies of all information seized" and returned the hardware as soon as possible, but did not answer whether in fact it would have reached a different result in such case. Id.

Incidental seizure of PPA-protected materials on a non-suspect's computer continues to be an uncertain area of the law, in part because PPA issues are infrequently litigated. As a practical matter, agents can often avoid the seizure of PPA-protected materials on a non-suspect's computer by using a subpoena or process under ECPA to require the non-suspect to produce the desired information, as described in Chapter 3. To date, no other court has followed the PPA approach of Steve Jackson Games. See, e.g., State v. One (1) Pioneer CD-ROM Changer, 891 P.2d 600, 607 (Okla. App. 1995) (questioning the apparent premise of Steve Jackson Games that the seizure of computer equipment could violate the PPA merely because the equipment "also contained or was used to disseminate potential 'documentary materials'"). Moreover, even if courts eventually refuse to restrict the PPA to cases in which law enforcement intentionally seizes First Amendment material that is merely evidence of a crime, courts

may conclude that other PPA exceptions, such as the "contraband or fruits of a crime" exception, should be read as broadly as the Guest court read the suspect exception.

The additional handful of federal courts that have resolved civil suits filed under the PPA have ruled against the plaintiffs with little substantive analysis. See, e.g., Davis v. Gracey, 111 F.3d 1472, 1482 (10th Cir. 1997) (dismissing for lack of jurisdiction PPA suit improperly filed against municipal employees in their personal capacities); Berglund v. City of Maplewood, 173 F. Supp. 2d 935, 949-50 (D. Minn. 2001) (holding that the police seizure of a defendant's videotape fell under the "criminal suspect" and "destruction of evidence" exceptions to the PPA because the tape might have contained documentary evidence of the defendant's disorderly conduct); DePugh v. Sutton, 917 F. Supp. 690, 696-97 (W.D. Mo. 1996) (rejecting pro se PPA challenge to seizure of materials relating to child pornography because there was probable cause to believe that the person possessing the materials committed the criminal offense to which the materials related), aff'd, 104 F.3d 363 (8th Cir. 1996); Powell v. Tordoff, 911 F. Supp. 1184, 1189-90 (N.D. Iowa 1995) (dismissing PPA claim because plaintiff did not have standing to challenge search and seizure under the Fourth Amendment). See also Lambert v. Polk County, 723 F. Supp. 128, 132 (S.D. Iowa 1989) (rejecting PPA claim after police seized videotape because officers could not reasonably believe that the owner of the tape had a purpose to disseminate the material to the public).

Agents and prosecutors who have reason to believe that a computer search may implicate the PPA should contact the Computer Crime and Intellectual Property Section at (202) 514-1026 or the CTC in their district (see Introduction, p. ix) for more specific guidance.

3. Civil Liability Under the Electronic Communications Privacy Act

When a search may result in the incidental seizure of network accounts belonging to innocent third parties, agents should take every step to protect the integrity of the third party accounts to avoid potential ECPA liability.

When law enforcement executes a search of an Internet service provider and seizes the accounts of customers and subscribers, those customers and subscribers may bring civil actions claiming that the search violated the Electronic Communications Privacy Act (ECPA). ECPA governs law enforcement access to the contents of electronic communications stored by third-party service providers. See 18 U.S.C. § 2703; Chapter 3, infra (discussing the Electronic Communications Privacy Act). In addition, ECPA has a criminal provision that prohibits unauthorized access to electronic or wire communications in "electronic storage." See 18 U.S.C. § 2701; Chapter 3, infra (discussing the definition of "electronic storage").

The concern that a search executed pursuant to a valid warrant might violate ECPA derives from Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), discussed in Section B.2.c supra. In Steve Jackson Games, the district court held the Secret Service liable under ECPA after it seized, reviewed, and (in some cases) deleted stored electronic communications seized pursuant to a valid search warrant. See id. at 442-43. The court's holding appears to be rooted in the mistaken belief that ECPA requires that search warrants also comply with 18 U.S.C. § 2703(d) and the various notice requirements of § 2703. See id. In fact, ECPA makes quite clear that § 2703(d) and the notice requirements § 2703 are implicated only when law enforcement does not obtain a search warrant. Compare 18 U.S.C. § 2703(b)(1)(A) with 18 U.S.C. § 2703(b)(1)(B). See generally Chapter 3, infra. Indeed, the text of ECPA does not appear to contemplate civil liability for searches and seizures authorized by valid Rule 41 search warrants: ECPA expressly authorizes government access to stored communications pursuant to a warrant issued under the Federal Rules of Criminal Procedure, see 18 U.S.C. § 2703(a), (b), (c)(1)(A); Davis v. Gracey, 111 F.3d 1472, 1483 (10th Cir. 1997), and the criminal prohibition of § 2701 does not apply when access is authorized under § 2703. See 18 U.S.C. § 2701(c)(3).[9] Further, objectively reasonable good faith reliance on a warrant, court order, or statutory authorization is a complete defense to an ECPA violation. See 18 U.S.C. § 2707(e); Gracey, 111 F.3d at 1484 (applying good faith defense because seizure of stored communications incidental to a valid search was objectively reasonable). Compare Steve Jackson Games, 816 F. Supp. at 443 (stating without explanation that the court "declines to find this defense").

The best way to square the result in Steve Jackson Games with the plain language of ECPA is to exercise great caution when agents need to execute searches of Internet service providers and other third-parties holding stored wire or electronic communications. In most cases, investigators will want to avoid a wholesale search and seizure of the provider's computers. When investigators have no choice but to execute the search, such as where the entity owning the system is suspected of deep involvement in the criminal conduct, they must take special care. For example, if agents have reason to believe that they may seize customer accounts belonging to innocent persons but have no reason to believe that the evidence sought will be stored there, they should inform the magistrate judge in the search warrant affidavit that they will not search those accounts and should take steps to ensure the confidentiality of the accounts in light of the privacy concerns expressed by 18 U.S.C. § 2703. Safeguarding the accounts of innocent persons absent specific reasons to believe that evidence may be stored in the persons' accounts should satisfy the concerns expressed in Steve Jackson Games. Compare Steve Jackson Games, 816 F. Supp. at 441 (finding ECPA liability where agents read the private communications of customers not involved in the crime "and thereafter deleted or destroyed some communications either

intentionally or accidentally") with Gracey, 111 F.3d at 1483 (declining to find ECPA liability in seizure where "[p]laintiffs have not alleged that the officers attempted to access or read the seized e-mail, and the officers disclaimed any interest in doing so").

If agents believe that a hacker or system administrator might have hidden evidence of a crime in the account of an innocent customer or subscriber, agents should proceed carefully. For example, agents should inform the magistrate judge of their need to search the account in the affidavit, and should attempt to obtain the consent of the customer or subscriber if feasible. In such cases, agents should contact the Computer Crime and Intellectual Property Section at (202) 514-1026 or the CTC designated in their district (see Introduction, p. ix) for more specific guidance.

4. Considering the Need for Multiple Warrants in Network Searches

Agents should obtain multiple warrants if they have reason to believe that a network search will retrieve data stored in multiple locations.

Fed. R. Crim. P. 41(a) states that a magistrate judge located in one judicial district may issue a search warrant for "a search of property . . . within the district," or "a search of property . . . outside the district if the property . . . is within the district when the warrant is sought but might move outside the district before the warrant is executed." The Supreme Court has held that "property" as described in Rule 41 includes intangible property such as computer data. See United States v. New York Tel. Co., 434 U.S. 159, 170 (1977). Although the courts have not directly addressed the matter, the language of Rule 41 combined with the Supreme Court's interpretation of "property" may limit searches of computer data to data that resides in the district in which the warrant was issued.[(10)] Cf. United States v. Walters, 558 F. Supp. 726, 730 (D. Md. 1980) (suggesting such a limit in a case involving telephone records).

A territorial limit on searches of computer data poses problems for law enforcement because computer data stored in a computer network can be located anywhere in the world. For example, agents searching an office in Manhattan pursuant to a warrant from the Southern District of New York may sit down at a terminal and access information stored remotely on a computer located in New Jersey, California, or even a foreign country. A single file described by the warrant could be located anywhere on the planet, or could be divided up into several locations in different districts or countries. Even worse, it may be impossible for agents to know when they execute their search whether the data they are seizing has been stored within the district or outside of the district. Agents may in some cases be able to learn where the data is located before the search, but in others they will be unable to know the storage site of the data until after the search has been completed.

When agents can learn prior to the search that some or all of the data described by the warrant is stored in a different location than where the agents will execute the search, the best course of action depends upon where the remotely stored data is located. When the data is stored remotely in two or more different places within the United States and its territories, agents should obtain additional warrants for each location where the data resides to ensure compliance with a strict reading of Rule 41(a). For example, if the data is stored in two different districts, agents should obtain separate warrants from the two districts. Agents should also include a thorough explanation of the location of the data and the proposed means of conducting the search in the affidavits accompanying the warrants.

When agents learn before a search that some or all of the data is stored remotely outside of the United States, matters become more complicated. The United States may be required to take actions ranging from informal notice to a formal request for assistance to the country concerned. Further, some countries may object to attempts by U.S. law enforcement to access computers located within their borders. Although the search may seem domestic to a U.S. law enforcement officer executing the search in the

United States pursuant to a valid warrant, other countries may view matters differently. Agents and prosecutors should contact the Office of International Affairs at (202) 514-0000 for assistance with these difficult questions.

When agents do not and even cannot know that data searched from one district is actually located outside the district, evidence seized remotely from another district ordinarily should not lead to suppression of the evidence obtained. The reasons for this are twofold. First, courts may conclude that agents sitting in one district who search a computer in that district and unintentionally cause intangible information to be sent from a second district into the first have complied with Rule 41(a). Cf. United States v. Ramirez, 112 F.3d 849, 852 (7th Cir. 1997) (Posner, C.J.) (adopting a permissive construction of the territoriality provisions of Title III); United States v. Denman, 100 F.3d 399, 402 (5th Cir. 1996) (same); United States v. Rodriguez, 968 F.2d 130, 135-36 (2d Cir. 1992) (same).

Second, even if courts conclude that the search violates Rule 41(a), the violation will not lead to suppression of the evidence unless the agents intentionally and deliberately disregarded the Rule, or the violation leads to "prejudice" in the sense that the search might not have occurred or would not have been so "abrasive" if the Rule had been followed. See United States v. Burke, 517 F.2d 377, 386 (2d Cir. 1975) (Friendly, J.); United States v. Martinez-Zayas, 857 F.2d 122, 136 (3d Cir. 1988) (citing cases). Under the widely-adopted Burke test, courts generally deny motions to suppress when agents executing the search cannot know whether it violates Rule 41 either legally or factually. See Martinez-Zayas, 857 F.2d at 136 (concluding that a search passed the Burke test "[g]iven the uncertain state of the law" concerning whether the conduct violated Rule 41(a)). Accordingly, evidence acquired from a network search that accessed data stored in multiple districts should not lead to suppression unless the agents intentionally and deliberately disregarded Rule 41(a) or prejudice resulted. See generally United States v. Trost, 152 F.3d 715, 722 (7th Cir. 1998) ("[I]t is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the fourth amendment, that would call for suppression.").

5. No-Knock Warrants

As a general matter, agents must announce their presence and authority prior to executing a search warrant. See Wilson v. Arkansas, 514 U.S. 927, 934 (1995); 18 U.S.C. § 3109. This so-called "knock and announce" rule reduces the risk of violence and destruction of property when agents execute a search. The rule is not absolute, however. In Richards v. Wisconsin, 520 U.S. 385 (1997), the Supreme Court held that agents can dispense with the knock-and-announce requirement if they have

a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, would be dangerous or futile, or that it would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence.

Id. at 394. The Court stated that this showing was "not high, but the police should be required to make it whenever the reasonableness of a no-knock entry is challenged." Id. at 394-95. Such a showing satisfies both the Fourth Amendment and the statutory knock-and-announce rule of 18 U.S.C. § 3109. See United States v. Ramirez, 523 U.S. 65, 71-73 (1998).

Agents may need to conduct no-knock searches in computer crime cases because technically adept suspects may "hot wire" their computers in an effort to destroy evidence. For example, technically adept computer hackers have been known to use "hot keys," computer programs that destroy evidence when a special button is pressed. If agents knock at the door to announce their search, the suspect can simply press the button and activate the program to destroy the evidence.

When agents have reason to believe that knocking and announcing their presence would allow the destruction of evidence, would be dangerous, or would be futile, agents should request that the magistrate judge issue a no-knock warrant. The failure to obtain judicial authorization to dispense with the knock-and-announce rule does not preclude the agents from conducting a no-knock search, however. In some cases, agents may neglect to request a no-knock warrant, or may not have reasonable suspicion that evidence will be destroyed until they execute the search. In Richards, the Supreme Court made clear that "the reasonableness of the officers' decision [to dispense with the knock-and-announce rule] . . . must be evaluated as of the time they entered" the area to be searched. Richards, 520 U.S. at 395. Accordingly, agents may "exercise independent judgment" and decide to conduct a no-knock search when they execute the search, even if they did not request such authority or the magistrate judge specifically refused to authorize a no-knock search. Id. at 396 n.7. The question in all such cases is whether the agents had "a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, would be dangerous or futile, or that it would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence." Id. at 394.

6. Sneak-and-Peek Warrants

If certain conditions are met, a court may authorize so-called "surreptitious entry warrants" or "sneak-and-peek" warrants that excuse agents from having to notify the person whose premises are searched at the time of the search. Under 18 U.S.C. § 3103a, as amended by the USA PATRIOT Act of 2001 § 213, Pub. L. No. 107-56, 115 Stat. 272 (2001), a court may grant the delay of notice associated with the execution of a search warrant if it finds "reasonable cause" to believe that providing immediate notification of the execution of the warrant may have one of the adverse effects enumerated in 18 U.S.C. § 2705: endangering the life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardizing an investigation or unduly delaying a trial. This standard may reduce some of the inconsistencies among jurisdictions in rules governing sneak-and-peek warrants that existed prior to the PATRIOT Act. CompareUnited States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000) (45-day delay in notice of execution of warrant does not render search unconstitutional) with United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986) (warrant constitutionally defective for failing to provide explicitly for notice within "a reasonable, but short, time").

Furthermore, under section 3103a, law enforcement authorities must provide delayed notice within a "reasonable period" following a warrant's execution, but the court can further delay notification for good cause. "Reasonable period" is a flexible standard to meet the circumstances of each individual case. Cf.United States v. Villegas, 899 F.2d 1324, 1337 (2d Cir. 1990) (noting prior to the amendment of section 3103a that "[w]hat constitutes a reasonable time will depend on the circumstances of each individual case"). Courts deciding this issue prior to the amendment of the statute have made different rulings on what period of delay is "reasonable." United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000) (45-day delay in notice of execution of warrant does not render search unconstitutional); Villegas, 899 F.2d at 1337 (seven-day initial delay reasonable, subject to extensions); United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986) ("Such time should not exceed seven days except upon a strong showing of necessity.").

The provision distinguishes between delaying notice of a *search* and delaying notice of a *seizure.* Indeed, unless the court finds "reasonable necessity" for a seizure, warrants issued under this section must prohibit the seizure of any tangible property, any wire or electronic communication, or any stored wire or electronic information (except as expressly provided in chapter 121). Congress intended that if

investigators intended to make surreptitious copies of information stored on a suspect's computer, they would obtain authorization from the court in advance.
Prosecutors should exercise discretion and obtain the approval of a supervisory official within their office before seeking delayed-notice warrants or orders. In addition, every attempt should be made to ensure that the period of delayed notice will be as brief as is reasonably possible. The Executive Office of United States Attorneys should also be notified about such warrants. For more information regarding this provision, prosecutors and investigators should contact the Office of Enforcement Operations, Criminal Division, at (202) 514-0746 or (202) 514-3684.

7. Privileged Documents

Agents must exercise special care when planning a computer search that may result in the seizure of legally privileged documents such as medical records or attorney-client communications. Two issues must be considered. First, agents should make sure that the search will not violate the Attorney General's regulations relating to obtaining confidential information from disinterested third parties. Second, agents should devise a strategy for reviewing the seized computer files following the search so that no breach of a privilege occurs.

a) The Attorney General's Regulations Relating to Searches of Disinterested Lawyers, Physicians, and Clergymen

Agents should be very careful if they plan to search the office of a doctor, lawyer, or member of the clergy who is not implicated in the crime under investigation. At Congress's direction, the Attorney General has issued guidelines for federal officers who want to obtain documentary materials from such disinterested third parties. See 42 U.S.C. § 2000aa-11(a); 28 C.F.R. § 59.4(b). Under these rules, federal law enforcement officers should not use a search warrant to obtain documentary materials believed to be in the private possession of a disinterested third party physician, lawyer, or clergyman where the material sought or likely to be reviewed during the execution of the warrant contains confidential information on patients, clients, or parishioners. 28 C.F.R. § 59.4(b). The regulation does contain a narrow exception. A search warrant can be used if using less intrusive means would substantially jeopardize the availability or usefulness of the materials sought; access to the documentary materials appears to be of substantial importance to the investigation; and the application for the warrant has been recommended by the U.S. Attorney and approved by the appropriate Deputy Assistant Attorney General. See 28 C.F.R. § 59.4(b)(1) and (2).

When planning to search the offices of a lawyer under investigation, agents should follow the guidelines offered in the United States Attorney's Manual, and should consult the Office of Enforcement Operations at (202) 514-3684. See generally United States Attorney's Manual, § 9-13.420 (1997).

b) Strategies for Reviewing Privileged Computer Files

Agents contemplating a search that may result in the seizure of legally privileged computer files should devise a post-seizure strategy for screening out the privileged files and should describe that strategy in the affidavit.

When agents seize a computer that contains legally privileged files, a trustworthy third party must comb through the files to separate those files within the scope of the warrant from files that contain privileged material. After reviewing the files, the third party will offer those files within the scope of the warrant to the prosecution team. Preferred practices for determining who will comb through the files vary widely among different courts. In general, however, there are three options. First, the court itself may review the files *in camera*. Second, the presiding judge may appoint a neutral third party known as a "special master" to the task of reviewing the files. Third, a team of prosecutors or agents who are not working on the case may form a "taint team" or "privilege team" to help execute the search and review the files afterwards. The taint team sets up a so-called "Chinese Wall" between the evidence and the prosecution team, permitting only unprivileged files that are within the scope of the warrant to slip through the wall. Because a single computer can store millions of files, judges will undertake *in camera* review of computer files only rarely. See Black v. United States, 172 F.R.D. 511, 516-17 (S.D. Fla. 1997) (accepting *in camera* review given unusual circumstances); United States v. Skeddle, 989 F. Supp. 890, 893 (N.D. Ohio 1997) (declining *in camera* review). Instead, the typical choice is between using a taint team and a special master. Most prosecutors will prefer to use a taint team if the court consents. A taint team can usually screen through the seized computer files fairly quickly, whereas special masters often take several years to complete their review. See Black, 172 F.R.D. at 514 n.4. On the other hand, some courts have expressed discomfort with taint teams. See United States v. Neill, 952 F. Supp. 834, 841 (D.D.C. 1997); United States v. Hunter, 13 F. Supp. 2d 574, 583 n.2 (D. Vt. 1998) (stating that review by a magistrate judge or special master "may be preferable" to reliance on a taint team) (citing In re Search Warrant, 153 F.R.D. 55, 59 (S.D.N.Y. 1994)).

Although no single standard has emerged, courts have generally indicated that evidence screened by a taint team will be admissible only if the government shows that its procedures adequately protected the defendants' rights and no prejudice occurred. See, e.g., Neill, 952 F. Supp. at 840-42; Hunter, 13 F. Supp. 2d at 583. One approach to limit the amount of potentially privileged material in dispute is to have defense counsel review the output of the taint team to identify those documents for which counsel intends to raise a claim of privilege. Files thus identified that do not seem relevant to the investigation need not be litigated. Although this approach may not be appropriate in every case, magistrates may appreciate the fact that defense counsel has been given the chance to identify potential claims before the court decides what to provide to the prosecution team.

In unusual circumstances, the court may conclude that a taint team would be inadequate and may appoint a special master to review the files. See, e.g., United States v. Abbell, 914 F. Supp. 519 (S.D. Fla. 1995); DeMassa v. Nunez, 747 F.2d 1283 (9th Cir. 1984). In any event, the reviewing authority will almost certainly need a skilled and neutral technical expert to assist in sorting, identifying, and analyzing digital evidence for the reviewing process.

C. Drafting the Warrant and Affidavit

Law enforcement officers must draft two documents to obtain a search warrant from a magistrate judge. The first document is the affidavit, a sworn statement that (at a minimum) explains the basis for the affiant's belief that the search is justified by probable cause. The second document is the proposed warrant itself. The proposed warrant typically is a one-page form, plus attachments incorporated by reference, that describes the place to be searched, and the persons or things to be seized. If the magistrate judge agrees that the affidavit establishes probable cause, and that the proposed warrant's descriptions of the place to be searched and things to be seized are adequately particular, the magistrate judge will sign the warrant. Under the Federal Rules of Criminal Procedure, officers must execute the warrant within ten days after the warrant has been signed. See Fed. R. Crim. P. 41(b).

In general, there are three steps involved in drafting the warrant and affidavit. First, the warrant (and/or its attachments) must accurately and particularly describe the property to be seized. Second, the affidavit must establish probable cause. Third, the affidavit should include an explanation of the search strategy. These three components are discussed below.

Step 1: Accurately and Particularly Describe the Property to be Seized in the Warrant and/or Attachments to the Warrant

a. General

Agents must take special care when describing the computer files or hardware to be seized, either in the warrant itself or (more likely) in an attachment to the warrant incorporated into the warrant by reference. The Fourth Amendment requires that every warrant must "particularly describ[e] . . . the . . . things to be seized." U.S. Const. Amend. IV. The particularity requirement prevents law enforcement from executing "general warrants" that permit "exploratory rummaging" through a person's belongings in search of evidence of a crime. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

The particularity requirement has two distinct elements. See United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999). First, the warrant must describe the things to be seized with sufficiently precise language so that it tells the officers how to separate the items properly subject to seizure from irrelevant items. See Marron v. United States, 275 U.S. 192, 296 (1925) ("As to what is to be taken, nothing is left to the discretion of the officer executing the warrant."); Davis v. Gracey, 111 F.3d 1472, 1478 (10th Cir. 1997). Second, the description of the things to be seized must not be so broad that it encompasses items that should not be seized. See Upham, 168 F.3d at 535. Put another way, the description in the warrant of the things to be seized should be limited to the scope of the probable cause established in the warrant. See In re Grand Jury Investigation Concerning Solid State Devices, 130 F.3d 853, 857 (9th Cir. 1997). Considered together, the elements forbid agents from obtaining "general warrants" and instead require agents to conduct narrow seizures that attempt to "minimize[] unwarranted intrusions upon privacy." Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976).

b. Warrants to Seize Hardware vs. Warrants to Seize Information

If computer hardware is contraband, evidence, fruits, or instrumentalities of crime, the warrant should describe the hardware itself. If the probable cause relates only to information, however, the warrant should describe the information, rather than the physical storage devices which happen to contain it.

The most important decision agents must make when describing the property in the warrant is whether the seizable property according to Rule 41 is the computer hardware itself, or merely the information

that the hardware contains. If the computer hardware is itself contraband, an instrumentality of crime, or evidence, the focus of the warrant should be on the computer hardware itself and not on the information it contains. The warrant should describe the hardware and indicate that the hardware will be seized. See, e.g., Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (seizure of computer "equipment" used to store obscene pornography was proper because the equipment was an instrumentality). However, if the probable cause relates in whole or in part to information stored on the computer, the warrant should focus on the content of the relevant files rather than on the storage devices which may happen to contain them. See, e.g., United States v. Gawrysiak, 972 F. Supp. 853, 860 (D.N.J. 1997), aff'd, 178 F.3d 1281 (3d Cir. 1999) (upholding seizure of "records [that] include information and/or data stored in the form of magnetic or electronic coding on computer media . . . which constitute evidence" of enumerated federal crimes). The warrant should describe the information based on its content (e.g., evidence of a fraud scheme), and then request the authority to seize the information in whatever form the information may be stored. To determine whether the warrant should describe the computer hardware itself or the information it contains, agents should consult Appendix F and determine whether the hardware constitutes evidence, contraband, or an instrumentality that may itself be seizable according to Rule 41(a).

When conducting a search for information, agents need to consider carefully exactly what information they need. The information may be very narrow (e.g., a specific record or report), or quite broad (e.g., all records relating to an elaborate fraud scheme). Agents should tailor each warrant to the needs of each search. The warrant should describe the information to be seized, and then request the authority to seize the information in whatever form it may be stored (whether electronic or not).

Agents should be particularly careful when seeking authority to seize a broad class of information. This often occurs when agents plan to search computers at a business. See, e.g., United States v. Leary, 846 F.2d 592, 600-04 (10th Cir. 1988). Agents cannot simply request permission to seize "all records" from an operating business unless agents have probable cause to believe that the criminal activity under investigation pervades the entire business. See United States v. Ford, 184 F.3d 566, 576 (6th Cir. 1999) (citing cases); In re Grand Jury Investigation Concerning Solid State Devices, 130 F.3d 853, 857 (9th Cir. 1997). Instead, the description of the files to be seized should include limiting phrases that can modify and limit the "all records" search. For example, agents may specify the crime under investigation, the target of the investigation if known, and the time frame of the records involved. See, e.g., United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) (invalidating warrant for failure to name crime or limit seizure to documents authored during time frame under investigation); Ford, 184 F.3d at 576 ("Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad."); In the Matter of the Application of Lafayette Academy, 610 F.2d 1, 3-4, 4 n.4 (1st Cir. 1979); United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (concluding that warrant to seize "[a]ll computers" not sufficiently particular where description "did not indicate the specific crimes for which the equipment was sought, nor were the supporting affidavits or the limits contained in the searching instructions incorporated by reference.").

In light of these cases, agents should narrow "all records" searches with limiting language as necessary and appropriate. One effective approach is to begin with an "all records" description; add limiting language stating the crime, the suspects, and relevant time period if applicable; include explicit examples of the records to be seized; and then indicate that the records may be seized in any form, whether electronic or non-electronic. For example, when drafting a warrant to search a computer at a business for evidence of a drug trafficking crime, agents might describe the property to be seized in the following way:

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, USB storage devices, 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).
This language describes the general class of information to be seized ("all records"); narrows it to the extent possible (only those records involving the defendant's drug trafficking activities since 1995); offers examples of the types of records sought (such as customer lists and bank records); and then explains the various forms that the records may take (including electronic and non-electronic forms). Of course, agents do not need to follow this approach in every case; judicial review of search warrants is "commonsensical" and "practical," rather than "overly technical." United States v. Ventresca, 380 U.S. 102, 108 (1965). When agents cannot know the precise form that records will take before the search occurs, a generic description must suffice. See United States v. Logan, 250 F.3d 350, 365 (6th Cir. 2001) (approving a broadly worded warrant and noting that "the warrant's general nature" was appropriate in light of the investigation's circumstances); Davis v. Gracey, 111 F.3d 1472, 1478 (10th Cir. 1997) ("Even a warrant that describes the items to be seized in broad or generic terms may be valid when the description is as specific as the circumstances and the nature of the activity under investigation permit.") (internal quotations omitted); United States v. Lacy, 119 F.3d 742, 746-47 (9th Cir. 1997) (holding that the general description of computer equipment to be seized was sufficient as there was "no way to specify what hardware and software had to be seized to retrieve the images accurately"); United States v. London, 66 F.3d 1227, 1238 (1st Cir. 1995) (noting that where the defendant "operated a complex criminal enterprise where he mingled 'innocent' documents with apparently-innocent documents which, in fact, memorialized illegal transactions, ... [it] would have been difficult for the magistrate judge to be more limiting in phrasing the warrant's language, and for the executing officers to have been more discerning in determining what to seize."); United States v. Sharfman, 448 F.2d 1352, 1354-55 (2d Cir. 1971); Gawrysiak, 972 F. Supp. at 861. Warrants sometimes authorize seizure of all records relating to a particular criminal offense. See London, 66 F.3d at 1238 (upholding search for "books and records . . . and any other documents. . . which reflect unlawful gambling"); United States v. Riley, 906 F.2d 841, 844-45 (2d Cir. 1990) (upholding seizure of "items that constitute evidence of the offenses of conspiracy to distribute controlled substances"); United States v. Wayne, 903 F.2d 1188, 1195 (8th Cir. 1990) (upholding search for "documents and materials which may be associated with . . contraband [narcotics]"). Even an "all records" search may be appropriate in certain circumstances. See also United States v. Hargus, 128 F.3d 1358, 1362-63 (10th Cir. 1997) (upholding seizure of "any and all records relating to the business" under investigation for mail fraud and money laundering).

c. Defending Computer Search Warrants Against Challenges Based on the Description of the "Things to be Seized"

Search warrants may be subject to challenge when the description of the "things to be seized" does not comply fully with the practices suggested above. Two challenges to the scope of warrants arise particularly often. First, defendants may claim that a warrant is insufficiently particular when the warrant authorizes the seizure of hardware but the affidavit only establishes probable cause to seize information. Second, defendants may claim that agents exceeded the scope of the warrant by seizing computer equipment if the warrant failed to state explicitly that the information to be seized might be in electronic form. The former challenge argues that the description of the property to be seized was too broad, and the latter argues that the description was not broad enough.

1) When the warrant authorizes the seizure of hardware but the affidavit only establishes probable cause to seize information

Computer search warrants sometimes authorize the seizure of hardware when the probable cause in the affidavit relates solely to the computer files the hardware contains. For example, agents may have probable cause to believe that a suspect possesses evidence of a fraud scheme, and may draft the warrant to authorize the seizure of the defendant's computer equipment rather than the data stored within it. On a practical level, such a description makes sense because it accurately and precisely describes what the agents will do when they execute the warrant (i.e., seize the computer equipment). From a legal standpoint, however, the description is less than ideal: one might argue that the equipment *itself* is not evidence of a crime, an instrumentality or contraband that may be seized according to Rule 41(a). See Appendix F; cf. In re Grand Jury Subpoena Duces Tecum, 846 F. Supp. 11, 13 (S.D.N.Y. 1994) (concluding that a subpoena demanding production of computer hardware instead of the information it contained was unreasonably broad pursuant to Fed. R. Crim. P. 17(c)). The physical equipment merely stores the information that the agents have probable cause to seize. Although the agents may need to seize the equipment in order to obtain the files it contains and computer files do not exist separate from some storage medium, the better practice is to describe the information rather than the equipment in the warrant itself. When agents obtain a warrant authorizing the seizure of equipment, defendants may claim that the description of the property to be seized is fatally overbroad. See, e.g., Davis v. Gracey, 111 F.3d 1472, 1479 (10th Cir. 1997).[11]

To date, the courts have adopted a forgiving stance when faced with this challenge. The courts have generally held that descriptions of hardware can satisfy the particularity requirement so long as the subsequent searches of the seized computer hardware appear reasonably likely to yield evidence of crime. See, e.g., United States v. Hay, 231 F.3d 630, 634 (9th Cir. 2000) (upholding seizure of "computer hardware" in search for materials containing child pornography); United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000) (upholding seizure of "computer equipment which may be, or is used to visually depict child pornography," and noting that the affidavit accompanying the warrant explained why it would be necessary to seize the hardware and search it off-site for the images it contained); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (upholding seizure of "[a]ny and all computer software and hardware, . . . computer disks, disk drives" in a child pornography case because "[a]s a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the [sought after] images"); United States v. Lacy, 119 F.3d 742, 746 (9th Cir. 1997) (warrant permitting "blanket seizure" of computer equipment from defendant's apartment not insufficiently particular when there was probable cause to believe that computer would contain evidence of child pornography offenses); United States v. Henson, 848 F.2d 1374, 1382-83 (6th Cir. 1988) (permitting seizure of "computer[s], computer terminals, ... cables, printers, discs, floppy discs, [and] tapes" that could hold

evidence of the defendants' odometer-tampering scheme because such language "is directed toward items likely to provide information concerning the [defendants'] involvement in the . . . scheme and therefore did not authorize the officers to seize more than what was reasonable under the circumstances"); United States v. Albert, 195 F. Supp. 2d 267, 275-76 (D. Mass. 2002) (upholding warrant for seizure of computer and all related software and storage devices where such an expansive search was "the only practical way" to obtain images of child pornography). Cf. United States v. Lamb, 945 F. Supp. 441, 458-59 (N.D.N.Y. 1996) (not insufficiently particular to ask for "[a]ll stored files" in AOL network account when searching account for obscene pornography, because as a practical matter all files need to be reviewed to determine which files contain the pornography).

Despite these decisions, agents should comply with the technical requirements of Rule 41 when describing the "property to be seized" in a search warrant. If the property to be seized is information, the warrant should describe the information to be seized, rather than its container. Of course, seizure of computer equipment is not necessarily improper. For example, when the information to be seized is contraband (such as child pornography), the container itself may be independently seized as an instrumentality. See Gracey, 111 F.3d at 1480 (seizure of computer "equipment" was proper in case involving obscenity because the hardware was an instrumentality of the crime).

2) When agents seize computer data and computer hardware but the warrant does not expressly authorize their seizure

Search warrants sometimes fail to mention that information described in the warrant may appear in electronic form. For example, a search for "all records" relating to a conspiracy may list paper-world examples of record documents but neglect to state that the records may be stored within a computer. Agents executing the search who come across computer equipment may not know whether the warrant authorizes the seizure of the computers. If the agents do seize the computers, defense counsel may file a motion to suppress the evidence arguing that the computers seized were beyond the scope of the warrant.

The courts have generally permitted agents to seize computer equipment when agents reasonably believe that the content described in the warrant may be stored there, regardless of whether the warrant states expressly that the information may be stored in electronic form. See, e.g., United States v. Musson, 650 F. Supp. 525, 532 (D. Colo. 1986). As the Tenth Circuit explained in United States v. Reyes, 798 F.2d 380, 383 (10th Cir. 1986), "in the age of modern technology and commercial availability of various forms of items, the warrant c[an] not be expected to describe with exactitude the precise form the records would take." Accordingly, what matters is the substance of the evidence, not its form, and the courts will defer to an executing agent's reasonable construction of what property must be seized to obtain the evidence described in the warrant. See United States v. Hill, 19 F.3d 984, 987-89 (5th Cir. 1994); Hessel v. O'Hearn, 977 F.2d 299 (7th Cir. 1992); United States v. Word, 806 F.2d 658, 661 (6th Cir. 1986); United States v. Gomez-Soto, 723 F.2d 649, 655 (9th Cir. 1984) ("The failure of the warrant to anticipate the precise container in which the material sought might be found is not fatal."). See also United States v. Abbell, 963 F. Supp. 1178, 1997 (S.D. Fla. 1997) (noting that agents may legitimately seize "[a] document which is implicitly within the scope of the warrant -- even if it is not specifically identified").

3) General defenses to challenges of computer search warrants based on the description of the "things to be seized"

Prosecutors facing challenges to the particularity of computer search warrants have a number of additional arguments that may save inartfully drawn warrants. First, prosecutors can argue that the agents who executed the search had an objectively reasonable good faith belief that the warrant was sufficiently particular. See generally United States v. Leon, 468 U.S. 897, 922 (1984); Massachusetts v.

Shepard, 468 U.S. 981, 990-91 (1984). If true, the court will not order suppression of the evidence. See, e.g., United States v. Hunter, 13 F. Supp. 2d 574, 584-85 (D. Vt. 1998) (holding that good faith exception applied even though computer search warrant was insufficiently particular). Second, prosecutors may argue that the broad description in the warrant must be read in conjunction with a more particular description contained in the supporting affidavit. Although the legal standards vary widely among the circuits, see Wayne R. LaFave,Search and Seizure: A Treatise on the Fourth Amendment § 4.6(a) (1994), most circuits permit the warrant to be construed with reference to the affidavit for purposes of satisfying the particularity requirement in certain circumstances. Finally, several circuits have held that courts can redact overbroad language and admit evidence from overbroad seizures if the evidence admitted was seized pursuant to sufficiently particular language. See United States v. Christine, 687 F.2d 749, 759 (3d Cir. 1982); Gomez-Soto, 723 F.2d at 654.

Step 2: Establish Probable Cause in the Affidavit

The second step in preparing a warrant to search and seize a computer is to write a sworn affidavit establishing probable cause to believe that contraband, evidence, fruits, or instrumentalities of crime exist in the location to be searched. See U.S. Const. Amend. IV ("no Warrants shall issue, but upon probable cause, supported by Oath or affirmation"); Fed. R. Crim. P. 41(b),(c). According to the Supreme Court, the affidavit must establish "a fair probability that contraband or evidence of a crime will be found in a particular place." Illinois v. Gates, 462 U.S. 213, 238 (1983). This requires a practical, common-sense determination of the probabilities, based on a totality of the circumstances. See id. Of course, probable cause will not exist if the agent can only point to a "bare suspicion" that criminal evidence will be found in the place searched. See Brinegar v. United States, 338 U.S. 160, 175 (1949). Once a magistrate judge finds probable cause and issues the warrant, the magistrate's determination that probable cause existed is entitled to "great deference," Gates, 462 U.S. at 236, and will be upheld so long as there is a "substantial basis for concluding that probable cause existed." Id. at 238-39 (internal quotations omitted).

Importantly, the probable cause requirement does not require agents to be clairvoyant in their knowledge of the precise forms of evidence or contraband that will exist in the location to be searched. For example, agents do not need probable cause to believe that the evidence sought will be found in computerized (as opposed to paper) form. See United States v. Reyes, 798 F.2d 380, 382 (10th Cir. 1986) (noting that "in the age of modern technology . . . , the warrant could not be expected to describe with exactitude the precise forms the records would take"). Similarly, agents do not need to know exactly what statutory violation the evidence will help reveal, see United States v. Prandy-Binett, 995 F.2d 1069, 1073 (D.C. Cir. 1993), and do not need to know who owns the property to be searched and seized, see United States v. McNally, 473 F.2d 934, 942 (3d Cir. 1973). The probable cause standard simply requires agents to establish a fair probability that contraband or evidence of a crime will be found in the particular place to be searched. See Gates, 462 U.S. at 238. Of course, agents who have particular knowledge as to the form of evidence or contraband that exists at the place to be searched should articulate that knowledge fully in the affidavit.

Probable cause challenges to computer search warrants arise particularly often in cases involving the possession and transmission of child pornography images.[(12)] For example, defendants often claim that the passage of time between the warrant application and the occurrence of the incriminating facts alleged in the affidavit left the magistrate judge without sufficient reason to believe that images of child pornography would be found in the defendant's computers. The courts have generally found little merit in these "staleness" arguments, in part because the courts have taken judicial notice of the fact that

collectors of child pornography rarely dispose of such material. See, e.g., United States v. Hay, 231 F.3d 630, 636 (9th Cir. 2000); United States v. Horn, 187 F.3d 781, 786-87 (8th Cir. 1999); United States v. Lacy, 119 F.3d 742, 745-46 (9th Cir. 1997); United States v. Sassani, 139 F.3d 895, 1998 WL 89875, at *4-5 (4th Cir. Mar. 4, 1998) (unpublished) (citing cases). But see United States v. Zimmerman, 277 F.3d 426, 433-34 (3d Cir. 2002) (distinguishing retention of adult pornography from retention of child pornography and holding that evidence that adult pornography had been on computer at least six months before a warrant was issued was stale). Courts have also noted that advances in computer forensic analysis allow investigators to recover files even after they are deleted, casting greater doubt on the validity of "staleness" arguments. See Hay, 231 F.3d at 636; United States v. Cox, 190 F. Supp. 2d 330, 334 (N.D.N.Y. 2002).

Probable cause challenges may also arise when supporting evidence in an affidavit derives heavily from records of a particular Internet account or Internet Protocol ("IP") address. The problem is a practical one: generally speaking, the fact that an account or address was used does not establish conclusively the identity or location of the particular person who used it. As a result, an affidavit based heavily on account or IP address logs must demonstrate a sufficient connection between the logs and the location to be searched to establish "a fair probability that contraband or evidence of a crime will be found in [the] particular place" to be searched. Gates, 462 U.S. at 238. See, e.g., United States v. Cervini, 2001 WL 863559 (10th Cir. Jul. 31, 2001) (unpublished) (upholding finding of probable cause to search a house based on evidence that a particular IP address was used to transmit child pornography at a particular time, that the IP address and time of transmission were associated with the suspect's account with an Internet service provider, and that the suspect had two active phone lines connected to the his house); United States v. Hay, 231 F.3d 630, 634 (9th Cir. 2000) (evidence that child pornography images were sent to an IP address associated with the defendant's apartment, combined with other evidence of the defendant's interest in young children, created probable cause to search the defendant's apartment for child pornography); United States v. Grant, 218 F.3d 72, 76 (1st Cir. 2000) (evidence that an Internet account belonging to the defendant was involved in criminal activity on several occasions, and that the defendant's car was parked at his residence during at least one such occasion, created probable cause to search the defendant's residence).

Step 3: In the Affidavit Supporting the Warrant, Include an Explanation of the Search Strategy (Such as the Need to Conduct an Off-site Search) as Well as the Practical and Legal Considerations That Will Govern the Execution of the Search

The third step in drafting a successful computer search warrant is to explain both the search strategy and the practical considerations underlying the strategy in the affidavit. For example, if 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. If the search strategy has been influenced by legal considerations such as potential PPA liability, the affidavit should explain how and why in the affidavit. If the agents have authority to seize hardware because the hardware itself is evidence, contraband, or an instrumentality of crime, the affidavit should explain whether the agents intend to search the hardware following the seizure, and, if so, for what. In sum, the affidavit should address all of the relevant practical and legal issues that the agents have considered in the course of planning the search, and should explain the course of conduct that the agents will follow as a result. Although no particular language is required, Appendix F offers sample language that agents may find useful in many situations. Finally, when the search strategy is complicated or the affidavit is under seal, agents may consider whether to reproduce the explanation of the search strategy contained in the affidavit as an attachment to the warrant itself.

The reasons for articulating the search strategy in the affidavit are both practical and legal. On a practical level, explaining the search strategy in the affidavit creates a document that both the court and the agents can read and refer to as a guide to the execution of the search. See Nat'l City Trading Corp. v. United States, 635 F.2d 1020, 1026 (2d Cir. 1980) ("[W]e note with approval the care taken by the Government in the search involved here. . . . Such self-regulatory care [in executing a warrant] is conduct highly becoming to the Government."). Similarly, if the explanation of the search strategy is reproduced as an attachment to the warrant and given to the subject of the search pursuant to Rule 41(d), the explanation permits the owner of the searched property to satisfy himself during the search that the agents' conduct is within the scope of the warrant. See Michigan v. Tyler, 436 U.S. 499, 508 (1978) (noting that "a major function of the warrant is to provide the property owner with sufficient information to reassure him of the entry's legality"). Finally, as a legal matter, explaining the search strategy in the affidavit helps to counter defense counsel motions to suppress based on the agents' alleged "flagrant disregard" of the warrant during the execution of the search. However, agents must also beware of articulating an excessively narrow or restrictive search strategy: defense counsel may also allege flagrant disregard of a warrant if agents transgress the strategy described in the warrant.

To understand motions to suppress based on the "flagrant disregard" standard, agents and prosecutors should recall the limitations on search and seizure imposed by Rule 41 and the Fourth Amendment. In general, the Fourth Amendment and Rule 41 limit agents to searching for and seizing property described in the warrant that is itself evidence, contraband, fruits, or instrumentalities of crime. See United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982); see also Appendix F (describing property that may be seized according to Rule 41). If agents execute a warrant and seize additional property not described in the warrant, defense counsel can file a motion to suppress the additional evidence. Motions to suppress such additional evidence are filed relatively rarely because, if granted, they result only in the

suppression of the property not named in the warrant. See United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997).

On the other hand, defense counsel will often attempt to use the seizure of additional property as the basis for a motion to suppress all of the evidence obtained in a search. To be entitled to the extreme remedy of blanket suppression, the defendant must establish that the seizure of additional materials proves that the agents executed the warrant in "flagrant disregard" of its terms. See, e.g., United States v. Le, 173 F.3d 1258, 1269 (10th Cir. 1999); United States v. Matias, 836 F.2d 744, 747-48 (2d Cir. 1988) (citing cases). A search is executed in "flagrant disregard" of its terms when the officers so grossly exceed the scope of the warrant during execution that the authorized search appears to be merely a pretext for a "fishing expedition" through the target's private property. See, e.g., United States v. Liu, 239 F.3d 138 (2d Cir. 2000); United States v. Foster, 100 F.3d 846, 851 (10th Cir. 1996); United States v. Young, 877 F.2d 1099, 1105-06 (1st Cir. 1989).

Motions to suppress alleging "flagrant disregard" are common in computer searches because, for practical and technical reasons, agents executing computer searches frequently must seize hardware or files that are not described in the warrant. For example, as was just discussed, agents who have probable cause to believe that evidence of a defendant's fraud scheme is stored on the defendant's home computer may have to seize the entire computer and search it off-site. Defense lawyers often argue that by seizing more than the specific computer files named in the warrant, the agents "flagrantly disregarded" the seizure authority granted by the warrant. See, e.g., United States v. Henson, 848 F.2d 1374, 1383 (6th Cir. 1988); United States v. Hunter, 13 F. Supp. 2d 574, 585 (D. Vt. 1998); United States v. Gawryisiak, 972 F. Supp. 853, 865 (D.N.J. 1997), aff'd, 178 F.3d 1281 (3d Cir. 1999); United States v. Schwimmer, 692 F. Supp. 119, 127 (E.D.N.Y. 1988).

Prosecutors can best respond to "flagrant disregard" motions by showing that any seizure of property not named in the warrant resulted from a good faith response to inherent practical difficulties, rather than a wish to conduct a general search of the defendant's property under the guise of a narrow warrant. The courts have recognized the practical difficulties that agents face in conducting computer searches for specific files, and have approved off-site searches despite the incidental seizure of additional property. See, e.g., Davis v. Gracey, 111 F.3d 1472, 1280 (10th Cir. 1997) (noting "the obvious difficulties attendant in separating the contents of electronic storage [sought as evidence] from the computer hardware [seized] during the course of a search"); United States v. Schandl, 947 F.2d 462, 465-466 (11th Cir. 1991) (noting that an on-site search "might have been far more disruptive" than the off-site search conducted); Henson, 848 F.2d at 1383-84 ("We do not think it is reasonable to have required the officers to sift through the large mass of documents and computer files found in the [defendant's] office, in an effort to segregate those few papers that were outside the warrant."); United States v. Scott-Emuakpor, 2000 WL 288443, at *7 (W.D. Mich. Jan. 25, 2000) (noting "the specific problems associated with conducting a search for computerized records" that justify an off-site search); Gawrysiak, 972 F. Supp. at 866 ("The Fourth Amendment's mandate of reasonableness does not require the agent to spend days at the site viewing the computer screens to determine precisely which documents may be copied within the scope of the warrant."); United States v. Sissler, 1991 WL 239000, at *4 (W.D. Mich. Jan. 25, 1991) ("The police . . . were not obligated to inspect the computer and disks at the . . . residence because passwords and other security devices are often used to protect the information stored in them. Obviously, the police were permitted to remove them from the . . . residence so that a computer expert could attempt to 'crack' these security measures, a process that takes some time and effort. Like the seizure of documents, the seizure of the computer hardware and software was motivated by considerations of practicality. Therefore, the alleged carte blanche seizure of them was not a 'flagrant disregard' for the limitations of a search warrant."). See also United States v. Upham, 168 F.3d 532, 535

(1st Cir. 1999) ("It is no easy task to search a well-laden hard drive by going through all of the information it contains . . . . The record shows that the mechanics of the search for images later performed [off-site] could not readily have been done on the spot."); United States v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) ("[I]f some of the image files are stored on the internal hard drive of the computer, removing the computer to an FBI office or lab is likely to be the only practical way of examining its contents.").

The decisions permitting off-site computer searches are bolstered by analogous "physical-world" cases that have authorized agents to remove file cabinets and boxes of paper documents so that agents can review the contents off-site for the documents named in the warrant. See, e.g., United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (concluding that "wholesale seizure of file cabinets and miscellaneous papers" did not establish flagrant disregard because the seizure "was motivated by the impracticability of on-site sorting and the time constraints of executing a daytime search warrant"); Crooker v. Mulligan, 788 F.2d 809, 812 (1st Cir. 1986) (noting cases "upholding the seizure of documents, both incriminating and innocuous, which are not specified in a warrant but are intermingled, in a single unit, with relevant documents"); United States v. Tamura, 694 F.2d 591, 596 (9th Cir. 1982) (ruling that the district court properly denied suppression motion "where the Government's wholesale seizures were motivated by considerations of practicality rather than by a desire to engage in indiscriminate 'fishing'"); United States v. Hillyard, 677 F.2d 1336, 1340 (9th Cir. 1982) ("If commingling prevents on-site inspection, and no other practicable alternative exists, the entire property may be seizable, at least temporarily.").

Explaining the agent's search strategy and the practical considerations underlying the strategy in the affidavit may help ensure that the execution of the search will not be deemed in "flagrant disregard" of the warrant. Cf. United States v. Hay, 231 F.3d 630, 634 (9th Cir. 2000) (suggesting that a magistrate judge's authorization of a search supported by an affidavit that explained the need for an off-site search of a computer constituted "the magistrate judge's authorization" of the off-site search); United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000) (relying on the explanation of the search strategy contained in the affidavit to find that a computer search warrant was not overbroad). A careful explanation of the search strategy illustrates the agent's good faith and due care, articulates the practical concerns driving the search, and permits the judge to authorize the strategy described in the affidavit. A search that complies with the strategy explained in the supporting affidavit will not be in flagrant disregard of the warrant. See, e.g., United States v. Gawrysiak, 972 F. Supp. 853, 866 (D.N.J. 1997) (noting that agents' compliance with search plan included in affidavit evinced proper and reasonable care in executing authorized search).

Although explaining the search strategy has significant benefits, it is also important for agents not to be limited to an ineffective or excessively restrictive search strategy. For example, it is generally unwise to limit a search strategy solely to keyword searches. It is rare to know with certainty that the information sought will contain specified keywords and that the storage medium will be susceptible to keyword searches. Law and investment firms - not to mention individuals involved in criminal activity - often use code words to identify entities, individuals and specific business arrangements in documents and communications; sometimes the significance of such terms will not be apparent until after a careful file-by-file review has commenced. It should suffice to say that agents will engage "in search strategies such as keyword searches" to find the information described in the warrant. In addition, critical data on a computer may be in surprising nooks and crannies of the computer. For example, a robust search strategy should allow agents to search for deleted files in slack space. A search strategy should be sufficiently broad to ensure that agents will have no need to exceed the strategy to find the items identified in the warrant. Identifying a range of possible strategies is good practice.

When agents expect that the files described in the warrant will be commingled with innocent files outside of the warrant's scope, it is a good practice, if technically possible, to explain in the affidavit how the agents plan to search the computer for the targeted files.

When agents conduct a search for computer files and other electronic evidence stored in a hard drive or other storage device, the evidence may be commingled with data and files that have no relation to the crime under investigation. Figuring out how best to locate and retrieve the evidence amidst the unrelated data is more of an art than a science, and often requires significant technical expertise and careful attention to the facts. As a result, agents may or may not know at the time the warrant is obtained how the storage device should be searched, and, in beginning the search, may or may not know whether it will be possible to locate the evidence without conducting an extensive search through unrelated files. When agents have a factual basis for believing that they can locate the evidence using a specific set of techniques, the affidavit should explain the techniques that the agents plan to use to distinguish incriminating documents from commingled documents. Depending on the circumstances, it may be helpful to consult with experts in computer forensics to determine what kind of search can be conducted to locate the particular files described in the warrant. In some cases, a "key word" search or similar surgical approach may be possible. Notably, the Fourth Amendment does not generally require such an approach. See United States v. Habershaw, 2001 WL 1867803, at *7 (D. Mass. May 13, 2001) (rejecting argument that sector-by-sector search violates Fourth Amendment where key word search might have been used); United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) ("Computer records searches are no less constitutional than searches of physical records, where innocuous documents may be scanned to ascertain their relevancy."); United States v. Lloyd, 1998 WL 846822, at *3 (E.D.N.Y. Oct. 5, 1998). However, in extensive *dicta*, the Tenth Circuit has indicated that it favors such a narrow approach because it minimizes the possibility that the government will be able to use a narrow warrant to justify a broader search. See United States v. Carey, 172 F.3d 1268, 1275-76, 1275 n.8. (10th Cir. 1999) (citing Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J. L. &. Tech. 75, 108 (1994)); Campos, 221 F.3d at 1148. See also Gawrysiak, 972 F. Supp. at 866 (suggesting in *dicta* that agents executing a search for computer files "could have at the least checked the date on which each file was created, and avoided copying those files that were created before the time period covered by the warrant").

Of course, in many cases a narrow approach will be technically impossible. The targeted files may be mislabeled, hidden, oddly configured, written using code words to escape detection, encrypted, or otherwise impossible to find using a simple technique such as a "key word" search. Experience has shown that individuals engaged in various kinds of criminal conduct have used these techniques to obfuscate incriminating computer evidence. Because some judges may fail to appreciate such technical difficulties, it is a good practice as a matter of policy for agents to discuss these issues in the affidavit. In many cases, a more extensive search through innocent files will be necessary to determine which files fall within the scope of the warrant. Often, the only possible approach is to canvass the structure and sample some of the content of the seized storage device to tailor the best search techniques. In the course of this preliminary overview of the storage medium, unforeseeable technical difficulties may arise, and language in the affidavit should alert the magistrate judge of the need to allow for the development of flexible, changing search strategies. Explaining these practical needs in the affidavit can make clear at the outset why an extensive search will not be in "flagrant disregard" of the warrant, and why the extensive search complies fully with traditional Fourth Amendment principles. See Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."); United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) (noting

that records searches permit agents to search through many papers because "few people keep documents of their criminal transactions in a folder marked '[crime] records.'"); United States v. Gray, 78 F. Supp. 2d 524, 530 (E.D. Va. 1999) (noting that agents executing a search for computer files "are not required to accept as accurate any file name or suffix and [to] limit [their] search accordingly," because criminals may "intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories."); Hunter, 13 F. Supp. 2d at 584; United States v. Sissler, 1991 WL 239000, at *4 (W.D. Mich. Jan. 25, 1991) ("[T]he police were not obligated to give deference to the descriptive labels placed on the discs by [the defendant]. Otherwise, records of illicit activity could be shielded from seizure by simply placing an innocuous label on the computer disk containing them.").

When agents obtain a warrant to seize hardware that is itself evidence, contraband, or an instrumentality of crime, they should explain in the affidavit whether and how they plan to search the hardware following the seizure.

When agents have probable cause to seize hardware because it is evidence, contraband, or an instrumentality of crime, the warrant will ordinarily describe the property to be seized as the hardware itself. In many of these cases, however, the agents will plan to search the hardware after it is seized for electronic data stored inside the hardware that also constitute evidence or contraband. It is a good practice for agents to inform the magistrate of this plan in the supporting affidavit. Although the courts have upheld searches when agents did not explain this expectation in the affidavit, see, e.g., United States v. Simpson, 152 F.3d 1241, 1248 (10th Cir. 1998) (discussed below), the better practice is to inform the magistrate in the affidavit of the agents' plan to search the hardware following the seizure.

D. Post-Seizure Issues

In many cases, computer equipment that has been seized will be sent to a laboratory for forensic examination. The time that may elapse before a technical specialist completes the forensic examination varies widely, depending on the hardware itself, the evidence sought, and the urgency of the search. Often, however, the elapsed time is a matter of months. Several legal issues may arise during the post-seizure period that implicate the government's right to retain and search the computers in their custody.

1. Searching Computers Already in Law Enforcement Custody

In general, agents should obtain a second warrant to search a computer seized pursuant to a valid warrant if the property targeted by the proposed search is different from that underlying the first warrant. Agents often seize a computer pursuant to a warrant, and then ask whether they need a second warrant to search the computer. Whether a second warrant is needed depends on the purpose of the search. If agents plan to search the computer for the information that was the target of the original seizure, no second warrant is required. For example, in United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998), investigators obtained a warrant to seize the defendant's "computer diskettes . . . and the defendant's computer" based on probable cause to believe it contained child pornography. The investigators seized the computer and then searched it in police custody, finding child pornography images. On appeal following conviction, the defendant claimed that the investigators lacked the authority to *search* the computer because the warrant merely authorized the *seizure* of equipment. The Tenth Circuit rejected the argument, concluding that a warrant to seize computer equipment permitted agents to search the equipment. See id. at 1248. See also United States v. Gray, 78 F. Supp. 2d 524, 530-31 (E.D. Va. 1999) (holding that initial warrant authorizing search for evidence of computer hacking justified a subsequent search for such evidence, even though agents uncovered incriminating evidence beyond the scope of the warrant in the course of executing the search).

If investigators seize computer equipment for the evidence it contains and later decide to search the equipment for different evidence, however, it may be safe practice to obtain a second warrant. In United States v. Carey, 172 F.3d 1268 (10th Cir. 1999), detectives obtained a warrant to search the defendant's computer for records of narcotics sales. Searching the computer back at the police station, a detective discovered images of child pornography. At that point, the detective "abandoned the search for drug-related evidence" and instead searched the entire hard drive for evidence of child pornography. Id. at 1277-78. The Tenth Circuit suppressed the child pornography, holding that the subsequent search for child pornography exceeded the scope of the original warrant. See id. at 1276. Compare Carey with United States v. Walser, 275 F.3d 981, 986-87 (10th Cir. 2001) (upholding search where officer with warrant to search for electronic records of drug transactions discovered child pornography on computer, suspended search, and then returned to magistrate for second warrant to search for child pornography); Gray, 78 F. Supp. 2d at 530-31 (upholding search where agent discovered child pornography in the course of looking for evidence of computer hacking pursuant to a warrant, and then obtained a second warrant before searching the computer for child pornography).

Notably, Carey</SPAN'S style="TEXT-DECORATION: underline" See, e.g., Whren v. United States, 517 U.S. 806, 813 (1996); Horton v. California, 496 U.S. 128, 138 (1990). Relying on these precedents, several courts have indicated that an agent's subjective intent during the execution of a warrant no longer determines whether the search exceeded the scope of the warrant and violated the Fourth Amendment. See United States v. Van Dreel, 155 F.3d 902, 905 (7th Cir. 1998) ("[U]nder Whren, . . . once probable cause exists, and a valid warrant has been issued, the officer's subjective intent in conducting the search

is irrelevant."); United States v. Ewain, 88 F.3d 689, 694 (9th Cir. 1996) ("Using a subjective criterion would be inconsistent with Horton, and would make suppression depend too much on how the police tell their story, rather than on what they did."). According to these cases, the proper inquiry is whether, from an objective perspective, the search that the agents actually conducted was consistent with the warrant obtained. See Ewain, 88 F.3d at 694. The agent's subjective intent is either "irrelevant," Van Dreel, 155 F.3d at 905, or else merely one factor in the overall determination of "whether the police confined their search to what was permitted by the search warrant." Ewain, 88 F.3d at 694.

2. The Permissible Time Period For Examining Seized Computers

Neither Rule 41 nor the Fourth Amendment creates any specific time limits on the government's forensic examination of seized computers. However, some magistrate judges have begun imposing such limitations.

Despite the best efforts of the government to analyze seized computers quickly, the forensic examination of seized computers often takes months to complete because computers can store enormous amounts of data. As a result, suspects whose computers have been seized may be deprived of their computer hardware for an extended period of time. Neither Rule 41 nor the Fourth Amendment imposes any specific limitation on the time period of the government's forensic examination. The government ordinarily may retain the seized computer and examine its contents in a careful and deliberate manner without legal restrictions, subject only to Rule 41(e)'s authorization that a "person aggrieved" by the seizure of property may bring a motion for the return of the property (see "Rule 41(e) Motions for Return of Property," infra).[13]

A few magistrate judges have taken a different view, however. Several magistrate judges have refused to sign search warrants authorizing the seizure of computers unless the government conducts the forensic examination in a short period of time, such as thirty days. Some magistrate judges have imposed time limits as short as seven days, and several have imposed specific time limits when agents apply for a warrant to seize computers from operating businesses. In support of these limitations, a few magistrate judges have expressed their concern that it might be constitutionally "unreasonable" under the Fourth Amendment for the government to deprive individuals of their computers for more than a short period of time. Other magistrates have suggested that Rule 41's requirement that agents execute a "search" within 10 days of obtaining the warrant might apply to the forensic analysis of the computer as well as the initial search and seizure. See Fed. R. Crim. P. 41(c)(1).

The law does not expressly authorize magistrate judges to issue warrants that impose time limits on law enforcement's examination of seized evidence. Although the relevant case law is sparse, it suggests that magistrate judges lack the legal authority to refuse to issue search warrants on the ground that they believe that the agents may, in the future, execute the warrants in an unconstitutional fashion. See Abraham S. Goldstein, *The Search Warrant, the Magistrate, and Judicial Review*, 62 N.Y.U. L. Rev. 1173, 1196 (1987) ("The few cases on [whether a magistrate judge can refuse to issue a warrant on the ground that the search may be executed unconstitutionally] hold that a judge has a 'ministerial' duty to issue a warrant after 'probable cause' has been established."); In re Worksite Inspection of Quality Products, Inc., 592 F.2d 611, 613 (1st Cir. 1979) (noting the limited role of magistrate judges in issuing search warrants). As the Supreme Court suggested in one early case, the proper course is for the magistrate to issue the warrant so long as probable cause exists, and then to permit the parties to litigate the constitutional issues afterwards. See Ex Parte United States, 287 U.S. 241, 250 (1932) ("The refusal of the trial court to issue a warrant . . . is, in reality and effect, a refusal to permit the case to come to a

hearing upon either questions of law or fact, and falls little short of a refusal to permit the enforcement of the law.").

Prosecutors should also be prepared to explain to magistrate judges why a forensic search for files stored in a seized computer need not occur within 10 days of obtaining the warrant. Rule 41(c)(1) requires that the agents who obtain a warrant must "search, within a specified period of time not to exceed 10 days, the person or place named for the property or person specified." This rule directs agents to search the place named in the warrant and seize the property specified within 10 days so that the warrant does not become "stale" before it is executed. See United States v. Sanchez, 689 F.2d 508, 512 n.5 (5th Cir. 1982). This rule does not apply to the forensic analysis of evidence that has already been seized, however; even if such analysis involves a Fourth Amendment "search" in some cases, it plainly does not occur in "the place . . . named" in the warrant. See United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D.P.R. 2002) (stating that Rule 41 does not "provide[] 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"); United States v. Habershaw, 2001 WL 1867803, at *8 (D. Mass. May 13, 2001) (noting that "[f]urther forensic analysis of the seized hard drive image does not constitute a second execution of the warrant"). An analogy to paper documents may be helpful. A Rule 41 warrant that authorizes the seizure of a book requires that the book must be seized from the place described in the warrant within 10 days. However, neither the warrant nor Rule 41 requires law enforcement to examine the book and complete any forensic analysis of its pages within the same 10-day period. Cf. Commonwealth v. Ellis, 10 Mass. L. Rptr. 429, 1999 WL 815818, at *8-9 (Mass. Super. Aug. 27, 1999) (interpreting analogous state law provision and stating that "[t]he ongoing search of the computer's memory need not have been accomplished within the . . . period required for return of the warrant.").

Although the legal basis for imposing time limits on forensic analysis is unclear, a magistrate judge's refusal to issue a computer search warrant absent time limitations can create significant headaches for prosecutors. As a practical matter, prosecutors often have little choice but to go along with the magistrate judge's wishes. A judge's refusal to sign a search warrant generally is not an appealable final order, and the prosecutor's only recourse is to turn to another judge. See United States v. Savides, 658 F. Supp. 1399, 1404 (N.D. Ill. 1987) (noting that the second judge should be told that a first judge refused to sign the warrant), aff'd in relevant part sub nom. United States v. Pace, 898 F.2d 1218, 1230 (7th Cir. 1990). As a practical matter, then, prosecutors will often have little choice but to try to convince the judge not to impose a time limit, and if that fails, to request extensions when the time period proves impossible to follow.

At least one court has adopted the severe position that suppression is appropriate when the government fails to comply with court-imposed limits on the time period for reviewing seized computers. In United States v. Brunette, 76 F. Supp. 2d 30 (D. Me. 1999), a magistrate judge permitted agents to seize the computers of a child pornography suspect on the condition that the agents searched through the computers for evidence "within 30 days." The agents executed the search five days later, and seized several computers. A few days before the thirty-day period elapsed, the government applied for and obtained a thirty-day extension of the time for review. The agents then reviewed all but one of the seized computers within the thirty-day extension period, and found hundreds of images of child pornography. However, the agents did not begin reviewing the last of the computers until two days after the extension period had elapsed. The defendant moved for suppression of the child pornography images found in the last computer, on the ground that the search outside of the sixty-day period violated the terms of the warrant and subsequent extension order. The court agreed, stating that "because the Government failed to adhere to the requirements of the search warrant and subsequent order, any evidence gathered from the . . . computer is suppressed." Id. at 42.

The result in Brunette makes little sense either under Rule 41 or the Fourth Amendment. Even assuming that a magistrate judge has the authority to impose time constraints on forensic testing in the first place, it seems incongruous to impose suppression for violations of such conditions when analogous violations of Rule 41 itself would not result in suppression. Compare Brunette with United States v. Twenty-Two Thousand, Two Hundred Eighty Seven Dollars ($22,287.00), U.S. Currency, 709 F.2d 442, 448 (6th Cir. 1983) (rejecting suppression when agents began search "shortly after" 10 p.m., even though Rule 41 states that all searches must be conducted between 6:00 a.m. and 10 p.m.). This is especially true when the hardware to be searched is a container of contraband child pornography, and therefore is itself an instrumentality of crime not subject to return.

3. Rule 41(e) Motions for Return of Property

Rule 41(e) states that

> 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.

Fed. R. Crim. P. 41(e).

Rule 41(e) has particular importance in computer search cases because it permits owners of seized computer equipment to move for the return of the equipment before an indictment is filed. In some cases, defendants will file such motions because they believe that the seizure of their equipment violated the Fourth Amendment. If they are correct, the equipment must be returned. See, e.g., In re Grand Jury Investigation Concerning Solid States Devices, Inc., 130 F.3d 853, 855-56 (9th Cir. 1997). Rule 41(e) also permits owners to move for a return of their property when the seizure was lawful, but the movant is "aggrieved by the government's continued possession of the seized property." Id. at 856. The multi-functionality of computer equipment occasionally leads to Rule 41(e) motions on this basis. For example, a suspect under investigation for computer hacking may file a motion claiming that he must have his computer back to calculate his taxes or check his e-mail. Similarly, a business suspected of fraud may file a motion for the return of its equipment claiming that it needs the equipment returned or else the business will suffer.

Owners of properly seized computer equipment must overcome several formidable barriers before a court will order the government to return the equipment. First, the owner must convince the court that it should exercise equitable jurisdiction over the owner's claim. See Floyd v. United States, 860 F.2d 999, 1003 (10th Cir. 1988) ("Rule 41(e) jurisdiction should be exercised with caution and restraint."). Although the jurisdictional standards vary widely among different courts, most courts will assert jurisdiction over a Rule 41(e) motion only if the movant establishes: 1) that being deprived of possession of the property causes "irreparable injury," and 2) that the movant is otherwise without a remedy at law. See In re the Matter of the Search of Kitty's East, 905 F.2d 1367, 1370-71 (10th Cir. 1990). Cf. Ramsden v. United States, 2 F.3d 322, 325 (9th Cir. 1993) (articulating four-factor jurisdictional test from pre-1989 version of Rule 41(e)). If the movant established these elements, the court will move to the merits of the claim. On the merits, seized property will be returned only if the government's continued

possession is unreasonable. See Ramsden, 2 F.3d at 326. This test requires the court to weigh the government's interest in continued possession of the property with the owner's interest in the property's return. See United States v. Premises Known as 608 Taylor Ave., 584 F.2d 1297, 1304 (3d Cir. 1978). In particular,

> If the United States has a need for the property in an investigation or prosecution, its retention of the property generally is reasonable. But, if the United States' legitimate interests can be satisfied even if the property is returned, continued retention of the property would be unreasonable.

Advisory Committee Notes to the 1989 Amendment of Rule 41(e) (quoted in Ramsden, 2 F.3d at 326). Rule 41(e) motions requesting the return of properly seized computer equipment succeed only rarely. First, courts will usually decline to exercise jurisdiction over the motion if the government has offered the property owner an electronic copy of the seized computer files. See In re Search Warrant Executed February 1, 1995, 1995 WL 406276, at *2 (S.D.N.Y. Jul. 7, 1995) (concluding that owner of seized laptop computer did not show irreparable harm where government offered to allow owner to copy files it contained); United States v. East Side Ophthalmology, 1996 WL 384891, at *4 (S.D.N.Y. Jul. 9, 1996). See also Standard Drywall, Inc. v. United States, 668 F.2d 156, 157 n.2. (2d Cir. 1982) ("We seriously question whether, in the absence of seizure of some unique property or privileged documents, a party could ever demonstrate irreparable harm [justifying jurisdiction] when the Government either provides the party with copies of the items seized or returns the originals to the party and presents the copies to the jury.").

Second, courts that reach the merits generally find that the government's interest in the computer equipment outweighs the defendant's so long as a criminal prosecution or forfeiture proceeding is in the works. See United States v. Stowe, 1996 WL 467238, at *1-3 (N.D. Ill. Aug. 15, 1996) (continued retention of computer equipment is reasonable after 18 months where government claimed that investigation was ongoing and defendant failed to articulate convincing reason for the equipment's return); In the Matter of Search Warrant for K-Sports Imports, Inc., 163 F.R.D. 594, 597 (C.D. Cal. 1995) (denying motion for return of computer records relating to pending forfeiture proceedings); see also Johnson v. United States, 971 F. Supp. 862, 868 (D.N.J. 1997) (denying Rule 41(e) motion to return bank's computer tapes because bank was no longer an operating business). If the government does not plan to use the computers in further proceedings, however, the computer equipment must be returned. See United States v. Moore, 188 F.3d 516, 1999 WL 650568, at *6 (9th Cir. Jul. 15, 1999) (unpublished) (ordering return of computer where "the government's need for retention of the computer for use in another proceeding now appears . . . remote") ; K-Sports Imports, Inc., 163 F.R.D. at 597. Further, a court may grant a Rule 41(e) motion if the defendant cannot operate his business without the seized computer equipment and the government can work equally well from a copy of the seized files. See United States v. Bryant, 1995 WL 555700, at *3 (S.D.N.Y. Sept. 18, 1995) (referring to magistrate judge's prior unpublished ruling ordering the return of computer equipment, and stating that "the Magistrate Judge found that defendant needed this machinery to operate his business").

III. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

A. Introduction

ECPA regulates how the government can obtain stored account information from network service providers such as ISPs. Whenever agents or prosecutors seek stored e-mail, account records, or subscriber information from a network service provider, they must comply with ECPA. ECPA's classifications can be understood most easily using the chart that appears in Part F of this chapter

The stored communication portion of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2701-2712, creates statutory privacy rights for customers and subscribers of computer network service providers.

In a broad sense, ECPA "fills in the gaps" left by the uncertain application of Fourth Amendment protections to cyberspace. To understand these gaps, consider the legal protections we have in our homes. The Fourth Amendment clearly protects our homes in the physical world: absent special circumstances, the government must first obtain a warrant before it searches there. When we use a computer network such as the Internet, however, we do not have a physical "home." Instead, we typically have a network account consisting of a block of computer storage that is owned by a network service provider such as America Online. If law enforcement investigators want to obtain the contents of a network account or information about its use, they do not need to go to the user to get that information. Instead, the government can obtain the information directly from the provider.

Although the Fourth Amendment generally requires the government to obtain a warrant to search a home, it does not require the government to obtain a warrant to obtain the stored contents of a network account. Instead, the Fourth Amendment generally permits the government to issue a subpoena to a network provider ordering the provider to divulge the contents of an account.[14] ECPA addresses this imbalance by offering network account holders a range of statutory privacy rights against access to stored account information held by network service providers.

Because ECPA is an unusually complicated statute, it is helpful when approaching the statute to understand the intent of its drafters. The structure of ECPA reflects a series of classifications that indicate the drafters' judgments about what kinds of information implicate greater or lesser privacy interests. For example, the drafters saw greater privacy interests in stored e-mails than in subscriber account information. Similarly, the drafters believed that computing services available "to the public" required more strict regulation than services not available to the public. (Perhaps this judgment reflects the view that providers available to the public are not likely to have close relationships with their customers, and therefore might have less incentive to protect their customers' privacy.) To protect the array of privacy interests identified by its drafters, ECPA offers varying degrees of legal protection depending on the perceived importance of the privacy interest involved. Some information can be obtained from providers with a mere subpoena; other information requires a special court order; and still other information requires a search warrant. In general, the greater the privacy interest, the greater the privacy protection.

Agents and prosecutors must apply the various classifications devised by ECPA's drafters to the facts of each case to figure out the proper procedure for obtaining the information sought. First, they must classify the network services provider (e.g., does the provider provide "electronic communication service," "remote computing service," or neither). Next, they must classify the information sought (e.g., is the information content "in electronic storage," content held by a remote computing service, "a record

. . . pertaining to a subscriber," or other information enumerated by ECPA). Third, they must consider whether they are seeking to compel disclosure, or seeking to accept information disclosed voluntarily by the provider. If they seek compelled disclosure, they need to determine whether they need a search warrant, a 2703(d) court order, or a subpoena to compel the disclosure. If they are seeking to accept information voluntarily disclosed, they must determine whether the statute permits the disclosure. The chart contained in Part F of this chapter provides a useful way to apply these distinctions in practice.

The organization of this chapter will follow ECPA's various classifications. Part B explains ECPA's classification structure which distinguishes between providers of "electronic communication service" and providers of "remote computing service." Part C explains the different kinds of information that providers can divulge, such as content "in electronic storage" and "records . . . pertaining to a subscriber." Part D explains the legal process that agents and prosecutors must follow to compel a provider to disclose information. Part E looks at the flip side of this problem, and explains when providers may voluntarily disclose account information. A summary chart appears in Part F. The chapter ends with two additional sections. Part G discusses three important issues that may arise when agents obtain records from network providers: steps to preserve evidence, steps to prevent disclosure to subjects, and Cable Act issues. Finally, Part H discusses the remedies that courts may impose following violations of ECPA.

This chapter includes amendments to ECPA specified by the USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (the "PATRIOT Act"). The PATRIOT Act clarified and updated ECPA in light of modern technologies, and in several respects it eased restrictions on law enforcement access to stored communications. Some of these amendments, noted herein, are currently scheduled to sunset on December 31, 2005. See PATRIOT Act § 224, 115 Stat. 272, 295. Law enforcement personnel who use statutory provisions which are scheduled to sunset are strongly encouraged to report their experiences to the Computer Crime and Intellectual Property Section at (202) 514-1026. CCIPS can convey such information to Congress, who will decide whether the changes effected by the PATRIOT Act should be made permanent.

B. Providers of Electronic Communication Service vs. Remote Computing Service

ECPA divides providers covered by the statute into "provider[s] of electronic communication service" and "provider[s] of remote computing service." To understand these terms, it helps to recall the era in which ECPA, a 1986 statute, was drafted. At that time, network account holders generally used third-party network service providers for two reasons. First, account holders used their accounts to send and receive communications such as e-mail. The use of computer networks to communicate prompted privacy concerns because in the course of sending and retrieving messages, it was common for several computers to copy the messages and store them temporarily. Copies created by these providers of "electronic communication service" and placed in temporary "electronic storage" in the course of transmission sometimes stayed on a provider's computer for several months. See H.R. Rep. No. 99-647, at 22 (1986).

The second reason account holders used network service providers was to outsource computing tasks. For example, users paid to have remote computers store extra files, or process large amounts of data. When users hired such commercial "remote computing services" to perform tasks for them, they would send a copy of their private information to a third-party computing service, which retained the data for later reference. Remote computing services raised privacy concerns because the service providers often retained copies of their customers' files. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557.

ECPA protects communications held by providers of electronic communication service when those communications are in "electronic storage," as well as communications held by providers of remote computing service. To that end, the statute defines "electronic communication service," "electronic storage," and "remote computing service" in the following way:

"Electronic communication service"

An electronic communication service ("ECS") is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). (For a discussion of the definitions of wire and electronic communications, see Chapter 4.C.2, infra.) For example, "telephone companies and electronic mail companies" generally act as providers of electronic communication services. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568; see also FTC v. Netscape Communications Corp., 196 F.R.D. 559, 560 (N.D. Cal. 2000) (noting that Netscape, a provider of e-mail accounts through netscape.net, is a provider of ECS).

The legislative history and case law indicate that the key issue in determining whether a company provides ECS is that company's role in providing the ability to send or receive the precise communication at issue, regardless of the company's primary business. See H.R. Rep. No. 99-647, at 65 (1986). Any company or government entity that provides others with means of communicating electronically can be a "provider of electronic communication service" relating to the communications it provides, even if providing communications service is merely incidental to the provider's primary function. See Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (city that provided pager service to its police officers can be a provider of electronic communication service); United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993) (airline that provides travel agents with computerized travel reservation system accessed through separate computer terminals can be a provider of electronic communication service).

Conversely, a service cannot provide ECS with respect to a communication if the service did not provide the ability to send or receive that communication. See Sega Enterprises Ltd. v. MAPHIA, 948 F. Supp. 923, 930-31 (N.D. Cal. 1996) (video game manufacturer that accessed private e-mail stored on another company's bulletin board service in order to expose copyright infringement was not a provider of

electronic communication service); State Wide Photocopy v. Tokai Fin. Servs. Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995) (financing company that used fax machines and computers but did not provide the ability to send or receive communications was not provider of electronic communication service). Significantly, a mere user of ECS provided by another is not an ECS. For example, a web site is not a provider of electronic communication service, even though it may send and receive electronic communications from customers. In Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001), the plaintiff argued that Amazon.com (to whom plaintiff sent his name, credit card number, and other identification information) was an electronic communications service provider because "without recipients such as Amazon.com, users would have no ability to send electronic information." The court rejected this argument, holding that Amazon was properly characterized as a user rather than a provider of ECS. See id.

"Electronic storage"

18 U.S.C. § 2510(17) defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," or in the alternative as "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The mismatch between the everyday meaning of "electronic storage" and its narrow statutory definition has been a source of considerable confusion. It is crucial to remember that "electronic storage" refers only to temporary storage, made in the course of transmission, by a provider of electronic communication service. For example, the court in In re Doubleclick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001), held that cookies, which are information stored on a user's computer by a web site and sent back to the web site when the user accesses the web site, fall outside of the definition of "electronic storage" and hence outside of ECPA because of their "long-term residence on plaintiffs' hard drives."

To determine whether a communication is in "electronic storage," it helps to identify the communication's final destination. A copy of a communication is in "electronic storage" only if it is a copy of a communication created at an intermediate point that is designed to be sent on to its final destination. For example, e-mail that has been received by a recipient's service provider but has not yet been accessed by the recipient is in "electronic storage." See Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 461 (5th Cir. 1994). At that stage, the copy of the stored communication exists only as a temporary and intermediate measure, pending the recipient's retrieval of the communication from the service provider. Once the recipient retrieves the e-mail, however, the communication reaches its final destination. If a recipient then chooses to retain a copy of the accessed communication on the provider's system, the copy stored on the network is no longer in "electronic storage" because the retained copy is no longer in "temporary, intermediate storage . . . incidental to . . . electronic transmission." 18 U.S.C. § 2510(17). Rather, because the process of transmission to the intended recipient has been completed, the copy is simply a remotely stored file. See Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 635-38 (E.D. Pa. 2001) (holding that because an e-mail was acquired from post-transmission storage, it was not in "electronic storage" and its acquisition was not prohibited under ECPA); H.R. Rep. No. 99-647, at 64-65 (1986) (noting Congressional intent that opened e-mail and voicemail left on a provider's system be covered by provisions relating to remote computing services, rather than provisions relating to services holding communications in "electronic storage").

As a practical matter, whether a communication is held in "electronic storage" by a provider governs whether that service provides ECS with respect to the communication. The two concepts are coextensive: a service provides ECS with respect to a communication if and only if the service holds the communication in electronic storage. Thus, it follows that if a communication is not in temporary,

intermediate storage incidental to its electronic transmission, the service cannot provide ECS for that communication. Instead, the service must provide either "remote computing service" (also known as "RCS,"discussed below), or else neither ECS nor RCS. See discussion infra.

"Remote computing service"

The term "remote computing service" ("RCS") is defined by 18 U.S.C. § 2711(2) as "provision to the public of computer storage or processing services by means of an electronic communications system." An "electronic communications system" is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).

Roughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a customer. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3564-65. For example, a service provider that processes data in a time-sharing arrangement provides an RCS. See H.R. Rep. No. 99-647, at 23 (1986). A mainframe computer that stores data for future retrieval also provides an RCS. See Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432, 443 (W.D. Tex. 1993) (holding that provider of bulletin board services was a remote computing service). In contrast with a provider of ECS, a provider of RCS does not hold customer files on their way to a third intended destination; instead, they are stored or processed by the provider for the convenience of the account holder. Accordingly, files held by a provider acting as an RCS cannot be in "electronic storage" according to § 2510(17).

Under the definition provided by § 2711(2), a service can only be a "remote computing service" if it is available "to the public." Services are available to the public if they are available to any member of the general population who complies with the requisite procedures and pays any requisite fees. For example, America Online is a provider to the public: anyone can obtain an AOL account. (It may seem odd at first that a service can charge a fee but still be considered available "to the public," but this mirrors commercial relationships in the physical world. For example, movie theaters are open "to the public" because anyone can buy a ticket and see a show, even though tickets are not free.) In contrast, providers whose services are open only to those with a special relationship with the provider are not available to the public. For example, employers may offer network accounts only to employees. See Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (interpreting the "providing . . . to the public" clause in § 2702(a) to exclude an internal e-mail system that was made available to a hired contractor but was not available to "any member of the community at large"). Such providers cannot provide remote computing service because their network services are not available to the public.

Whether an entity is a provider of "electronic communication service," a provider of "remote computing service," or neither depends on the nature of the particular communication sought. For example, a single provider can simultaneously provide "electronic communication service" with respect to one communication and "remote computing service" with respect to another communication.

An example can illustrate how these principles work in practice. Imagine that Joe sends an e-mail from his account at work ("joe@goodcompany.com") to the personal account of his friend Jane ("jane@localisp.com"). The e-mail will stream across the Internet until it reaches the servers of Jane's Internet service provider, here the fictional LocalISP. When the message first arrives at LocalISP, LocalISP is a provider of ECS with respect to that message. Before Jane accesses LocalISP and retrieves the message, Joe's e-mail is in "electronic storage." See Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 461 (5th Cir. 1994). Once Jane retrieves Joe's e-mail, she can either delete the message from LocalISP's server, or else leave the message stored there. If Jane chooses to store the e-mail with LocalISP, LocalISP is now a provider of RCS (and not ECS) with respect to the e-mail sent

by Joe. The role of LocalISP has changed from a transmitter of Joe's e-mail to a storage facility for a file stored remotely for Jane by a provider of RCS. See H.R. Rep. No. 99-647, at 64-65 (1986) (noting Congressional intent to treat opened e-mail stored on a server under provisions relating to remote computing services, rather than services holding communications in "electronic storage").

Next imagine that Jane responds to Joe's e-mail. Jane's return e-mail to Joe will stream across the Internet to the servers of Joe's employer, Good Company. Before Joe retrieves the e-mail from Good Company's servers, Good Company is a provider of ECS with respect to Jane's e-mail (just like LocalISP was with respect to Joe's original e-mail before Jane accessed it). When Joe accesses Jane's e-mail message and the communication reaches its destination (Joe), Good Company ceases to be a provider of ECS with respect to that e-mail (just as LocalISP ceased to be a provider of ECS with respect to Joe's original e-mail when Jane accessed it). Unlike LocalISP, however, Good Company does not become a provider of RCS if Joe decides to store the opened e-mail on Good Company's server. Rather, for purposes of this specific message, Good Company is a provider of neither ECS nor RCS. Good Company does not provide RCS because it does not provide services to the public. See 18 U.S.C. § 2711(2) ("[T]he term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.") (emphasis added); Andersen Consulting, 991 F. Supp. at 1043. Because Good Company provides neither ECS nor RCS with respect to the opened e-mail in Joe's account, ECPA no longer regulates access to this e-mail, and such access is governed solely by the Fourth Amendment. Functionally speaking, the opened e-mail in Joe's account drops out of ECPA.

Finally, consider the status of the other copies in this scenario: Jane has downloaded a copy of Joe's e-mail from LocalISP's server to her personal computer at home, and Joe has downloaded a copy of Jane's e-mail from Good Company's server to his office desktop computer at work. ECPA governs neither. Although these computers contain copies of e-mails, these copies are not stored on the server of a third-party provider of RCS or ECS, and therefore ECPA does not apply. Access to the copies of the communications stored in Jane's personal computer at home and Joe's office computer at work is governed solely by the Fourth Amendment. See generally Chapters 1 and 2.

As this example indicates, a single provider can simultaneously provide ECS with regard to some communications and RCS with regard to others, or ECS with regard to some communications and neither ECS nor RCS with regard to others. As a practical matter, however, agents do not need to grapple with these difficult issues in most cases. Instead, agents can simply draft the appropriate order based on the information they seek. For example, if the police suspect that Jane and Joe have conspired to commit a crime, the police might seek an order or subpoena compelling LocalISP to divulge all files in Jane's account except for those in "electronic storage." In plain English, this is equivalent to asking for all of Jane's opened e-mails and stored files. Alternatively, the police might seek an order compelling Good Company to disclose files in "electronic storage" in Joe's account. This is equivalent to asking for unopened e-mails in Joe's account. A helpful chart appears in Part F of this chapter. Sample language that may be used appears in Appendices B, E, and F.

C. Classifying Types of Information Held by Service Providers

Network service providers can store different kinds of information relating to an individual customer or subscriber. Consider the case of the e-mail exchange between Joe and Jane discussed above. Jane's service provider, LocalISP, probably has access to a range of information about Jane and her account. For example, LocalISP may have opened and unopened e-mails; account logs that reveal when Jane logged on and off LocalISP; Jane's credit card information for billing purposes; and Jane's name and address. When agents and prosecutors wish to obtain such records, they must be able to classify these types of information using the language of ECPA. ECPA breaks the information down into three categories: basic subscriber information listed in 18 U.S.C. § 2703(c)(2); "record[s] or other information pertaining to a subscriber to or customer of [the] service"; and "contents." See 18 U.S.C. §§ 2510(8), 2703(c)(1).

1. Basic Subscriber Information Listed in 18 U.S.C. § 2703(c)(2)

18 U.S.C. § 2703(c)(2) lists the categories of basic subscriber information:
(A) name; (B) address; (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)[.]
In general, the items in this list relate to the identity of a subscriber, his relationship with his service provider, and his basic session connection records. This list does not include other, more extensive transaction-related records, such as logging information revealing the e-mail addresses of persons with whom a customer corresponded during a prior session. The PATRIOT Act enhanced the categories of basic subscriber information in three respects. See PATRIOT Act § 210, 115 Stat. 272, 283 (2001). It added "records of session times and durations," as well as "any temporarily assigned network address" to 18 U.S.C. § 2703(c)(2). In the Internet context, these records include the IP address assigned by an Internet service provider to a customer for a particular session. They also include other information relating to account access, such as the originating telephone number for dial-up Internet access or the IP address of a user accessing an account over the Internet. In addition, the PATRIOT Act added to this list of subscriber information the "means and source of payment" that a customer uses to pay for an account, "including any credit card or bank account number."

2. Records or Other Information Pertaining to a Customer or Subscriber

18 U.S.C. § 2703(c)(1) covers a second type of information: "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." This is a catch-all category that includes all records that are not contents, including basic subscriber information. Common examples of "record[s] . . . pertaining to a subscriber" include transactional records, such as account logs that record account usage; cell-site data for cellular telephone calls; and e-mail addresses of other individuals with whom the account holder has corresponded. See H.R. Rep. No. 103-827, at 10, 17, 31 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3490, 3497, 3511; United States v. Allen, 53 M.J. 402, 409 (C.A.A.F. 2000) (concluding that "a log identifying the date, time, user, and detailed internet address of sites accessed" by a user constituted "a record or other information pertaining to a subscriber or customer of such service" under ECPA). See also Hill v. MCI Worldcom, 120 F. Supp. 2d 1194, 1195-96 (S.D. Iowa 2000) (concluding that the "names, addresses, and phone numbers of parties . . . called" constituted "a record or other information pertaining to a subscriber or customer of such service" for a telephone account). According to the legislative history of the 1994 amendments to § 2703(c), the purpose of separating the basic subscriber information from other non-content records was to distinguish basic subscriber information from more revealing transactional information that could contain a "person's entire on-line profile." H.R. Rep. No. 103-827 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3497, 3511.

3. Contents

The contents of a network account are the actual files stored in the account. See 18 U.S.C. § 2510(8) ("'contents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication"). For example, stored e-mails or voice mails are "contents," as are word processing files stored in employee network accounts. The subject headers of e-mails are also contents. Cf. Brown v. Waddell, 50 F.3d 285, 292 (4th Cir. 1995) (noting that numerical pager messages provide "an unlimited range of number-coded substantive messages" in the course of holding that the interception of pager messages requires compliance with Title III).

Contents can be further divided into three subcategories: contents stored "in electronic storage" by providers of electronic communication service; contents stored by providers of remote computing services; and contents held by neither. The distinctions among these types of content are discussed in Part B, supra.

D. Compelled Disclosure Under ECPA

18 U.S.C. § 2703 articulates the steps that the government must take to compel providers to disclose the contents of stored wire or electronic communications (including e-mail and voice mail) and other information such as account records and basic subscriber information.
Section 2703 offers five mechanisms that a "government entity" can use to compel a provider to disclose certain kinds of information. The five mechanisms, in ascending order of required threshold showing, are as follows:

1) Subpoena;
2) Subpoena with prior notice to the subscriber or customer;
3) § 2703(d) court order;
4) § 2703(d) court order with prior notice to the subscriber or customer; and
5) Search warrant.

One feature of the compelled disclosure provisions of ECPA is that greater process generally includes access to information that can be obtained with lesser process. Thus, a § 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a § 2703(d) order can compel (and then some). As a result, the additional work required to satisfy a higher threshold will often be justified, both because it can authorize a broader disclosure and because pursuing a higher threshold provides extra insurance that the process complies fully with the statute. Note, however, the notice requirement must be considered as a separate burden under this analysis: a subpoena with notice to the subscriber can be used to compel information not available using a § 2703(d) order without subscriber notice. (One small category of information can be compelled under ECPA without a subpoena. When investigating telemarketing fraud, law enforcement may submit a written request to a service provider for the name, address, and place of business of a subscriber or customer engaged in telemarketing. See 18 U.S.C. § 2703(c)(1)(D).)

1. Subpoena

Investigators can subpoena basic subscriber information.
ECPA permits the government to compel two kinds of information using a subpoena. First, the government may compel the disclosure of the basic subscriber information (discussed above in section C.1) listed in 18 U.S.C. § 2703(c)(2):

> (A) name; (B) address; (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)[.]

18 U.S.C. § 2703(c)(2).
Agents can also use a subpoena to obtain information that is outside the scope of ECPA. The hypothetical e-mail exchange between Jane and Joe discussed in Part B of this chapter provides a useful example: Good Company provided neither "remote computing service" nor "electronic communication service" with respect to the opened e-mail on Good Company's server. See Part B, supra. Accordingly, § 2703 does not impose any requirements on its disclosure, and investigators can issue a subpoena compelling Good Company to divulge the communication just as they would if ECPA did not exist. Similarly, information relating or belonging to a person who is neither a "customer" nor a "subscriber" is

not protected by ECPA, and may be obtained using a subpoena according to the same rationale. Cf. Organizacion JD Ltda. v. United States Department of Justice, 124 F.3d 354, 359-61 (2d Cir. 1997) (discussing the scope of the word "customer" as used in ECPA).

The legal threshold for issuing a subpoena is low. See United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950). Of course, evidence obtained in response to a federal grand jury subpoena must be protected from disclosure pursuant to Fed. R. Crim. P. 6(e). Types of subpoenas other than federal grand jury subpoenas may be used to obtain disclosure pursuant to 18 U.S.C. § 2703(c)(2): any federal or state grand jury or trial subpoena will suffice, as will an administrative subpoena authorized by a federal or state statute. See 18 U.S.C. § 2703(c)(2). For example, subpoenas authorized by § 6(a)(4) of the Inspector General Act may be used. See 5 U.S.C. app. However, at least one court has held that a pre-trial discovery subpoena issued in a civil case pursuant to Fed. R. Civ. P. 45 is inadequate. See FTC v. Netscape Communications Corp., 196 F.R.D. 559 (N.D. Cal. 2000) (holding that pre-trial discovery subpoena did not fall within the meaning of "trial subpoena"). Sample subpoena language appears in Appendix E.

2. Subpoena with Prior Notice to the Subscriber or Customer

Investigators can subpoena opened e-mail from a provider if they comply with the notice provisions of §§ 2703(b)(1)(B) and 2705.

Agents who obtain a subpoena, and either give prior notice to the subscriber or comply with the delayed notice provisions of § 2705(a), may obtain:

1) everything that can be obtained using a subpoena without notice;

2) "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." 18 U.S.C. § 2703(b)(1)(B)(i), § 2703(b)(2); and

3) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a).

As a practical matter, this means that agents can obtain opened e-mail (and other stored electronic or wire[15] communications in "electronic storage" more than 180 days) using a subpoena, so long as they comply with ECPA's notice provisions. See H.R. Rep. No. 99-647, at 64-65 (1986).

The notice provisions can be satisfied by giving the customer or subscriber "prior notice" of the disclosure. See 18 U.S.C. § 2703(b)(1)(B). However, 18 U.S.C. § 2705(a)(1)(B) and § 2705(a)(4) permit notice to be delayed for ninety days "upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result." 18 U.S.C. § 2705(a)(1)(B). Both "supervisory official" and "adverse result" are specifically defined terms for the purpose of delaying notice. See § 2705(a)(2) (defining "adverse result"); § 2705(a)(6) (defining "supervisory official"). This provision of ECPA provides a permissible way for agents to delay notice when notice would jeopardize a pending investigation or endanger the life or physical safety of an individual. Upon expiration of the delayed notice period,[16] the statute requires the government to send a copy of the request or process along with a letter explaining the delayed notice to the customer or subscriber. See 18 U.S.C. § 2705(a)(5).

ECPA's provision allowing for obtaining opened e-mail using a subpoena combined with prior notice to the subscriber appears to derive from Supreme Court case law interpreting the Fourth and Fifth Amendments. See Clifford S. Fishman & Anne T. McKenna, Wiretapping and Eavesdropping § 26:9, at 26-12 (2d ed. 1995). When an individual gives paper documents to a third-party such as an accountant, the government may subpoena the paper documents from the third party without running afoul of either

the Fourth or Fifth Amendment. See generally United States v. Couch, 409 U.S. 322 (1973) (rejecting Fourth and Fifth Amendment challenges to subpoena served on defendant's accountant for the accountant's business records stored with the accountant). In allowing the government to subpoena opened e-mail, "Congress seems to have concluded that by 'renting' computer storage space with a remote computing service, a customer places himself in the same situation as one who gives business records to an accountant or attorney." Fishman & McKenna, §26:9, at 26-13.

3. Section 2703(d) Order

Agents need a § 2703(d) court order to obtain most account logs and most transactional records. Agents who obtain a court order under 18 U.S.C. § 2703(d) may obtain:

- 1) anything that can be obtained using a subpoena without notice; and
- 2) all "record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])." 18 U.S.C. § 2703(c)(1).

A court order authorized by 18 U.S.C. § 2703(d) may be issued by any federal magistrate, district court or equivalent state court judge. See 18 U.S.C. §§ 2703(d), 2711(3). To obtain such an order, known as an "articulable facts" court order or simply a "d" order,

> the governmental entity [must] offer[] 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.

Id.

This standard does not permit law enforcement merely to certify that it has specific and articulable facts that would satisfy such a showing. Rather, the government must actually offer those facts to the court in the application for the order. See United States v. Kennedy, 81 F. Supp. 2d 1103, 1109-11 (D. Kan. 2000) (concluding that a conclusory application for a § 2703(d) order "did not meet the requirements of the statute."). The House Report accompanying the 1994 amendment to § 2703(d) included the following analysis:

This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation.

H.R. Rep. No. 102-827, at 31 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3511 (quoted in full in Kennedy, 81 F. Supp. 2d at 1109 n.8). As a practical matter, a short factual summary of the investigation and the role that the records will serve in advancing the investigation should satisfy this criterion. A more in-depth explanation may be necessary in particularly complex cases. A sample § 2703(d) application and order appears in Appendix B.

Section 2703(d) orders issued by federal courts have effect outside the district of the issuing court. ECPA permits a judge to enter § 2703(d) orders compelling providers to disclose information even if the judge does not sit in the district in which the information is stored. See 18 U.S.C. § 2703(d) (stating that "any court that is a court of competent jurisdiction" may issue a § 2703(d) order) (emphasis added); 18 U.S.C. § 2711(3) (stating that "'court of competent jurisdiction' has the meaning assigned by section

3127, and includes any Federal court within that definition, without geographical limitation")[17]; 18 U.S.C. § 3127(2) (defining "court of competent jurisdiction").
Section 2703(d) orders may also be issued by state courts. See 18 U.S.C. §§ 2711(3), 3127(2)(B) (defining "court of competent jurisdiction" to include "a court of general criminal jurisdiction of a State authorized by the law of the State to enter orders authorizing the use of a pen register or trap and trace device"). However, the statute does not confer extraterritorial effect on § 2703(d) orders issued by state courts. See 18 U.S.C. §§ 2711(3).

4. § 2703(d) Order with Prior Notice to the Subscriber or Customer

Investigators can obtain everything in an account except for unopened e-mail or voicemail stored with a provider for 180 days or less using a § 2703(d) court order that complies with the notice provisions of § 2705.
Agents who obtain a court order under 18 U.S.C. § 2703(d), and either give prior notice to the subscriber or else comply with the delayed notice provisions of § 2705(a), may obtain:

- 1) everything that can be obtained using a § 2703(d) court order without notice;
- 2) "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service," 18 U.S.C. § 2703(b)(1)(B)(ii), § 2703(b)(2); and
- 3) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a).

As a practical matter, this means that the government can obtain the full contents of a subscriber's account except unopened e-mail and voicemail (which has been in "electronic storage" 180 days or less) using a § 2703(d) order that complies with the prior notice provisions of § 2703(b)(1)(B).[18]
As an alternative to giving prior notice, agents can obtain an order delaying notice for up to ninety days when notice would seriously jeopardize the investigation. See 18 U.S.C. § 2705(a). In such cases, agents generally will obtain this order by including an appropriate request in the agents' 2703(d) application and proposed order; sample language appears in Appendix B. Agents may also apply to the court for extensions of the delay. See 18 U.S.C. § 2705(a)(1)(A), § 2705(a)(4). The legal standards for obtaining a court order delaying notice mirror the standards for certified delayed notice by a supervisory official. See Part D.2., supra. The applicant must satisfy the court that "there is reason to believe that notification of the existence of the court order may . . . endanger[] the life or physical safety of an individual; [lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or . . . otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. § 2705(a)(1)(A), § 2705(a)(2). Importantly, the applicant must satisfy this standard anew every time the applicant seeks an extension of the delayed notice.

5. Search Warrant

Investigators can obtain the full contents of an account with a search warrant. ECPA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant.

Agents who obtain a search warrant under Rule 41 of the Federal Rules of Criminal Procedure or an equivalent state warrant may obtain:

- 1) everything that can be obtained using a § 2703(d) court order with notice; and
- 2) "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less." 18 U.S.C. § 2703(a).
- In other words, agents can obtain every record and all of the contents of an account by obtaining a search warrant based on probable cause pursuant to Fed. R. Crim. P. 41.[21] The search warrant can then be served on the service provider and compels the provider to divulge to law enforcement the information described in the search warrant. Notably, obtaining a search warrant obviates the need to give notice to the subscriber. See 18 U.S.C. § 2703(b)(1)(A). Moreover, because the warrant is issued by a neutral magistrate based on probable cause, obtaining a search warrant effectively insulates the process from challenge under the Fourth Amendment.

Although most search warrants obtained under Rule 41 are limited to "a search of property . . . within the district" of the authorizing magistrate judge, search warrants under § 2703(a) may be issued by a federal "court with jurisdiction over the offense under investigation," even for records held in another district.[22] 18 U.S.C. § 2703(a). (State courts may also issue warrants under § 2703(a), but the statute does not give these warrants effect outside the limits of the courts' territorial jurisdiction. See id.) Otherwise, as a practical matter, § 2703(a) search warrants are obtained just like Rule 41 search warrants. As with a typical Rule 41 warrant, investigators must draft an affidavit and a proposed warrant that complies with Rule 41. See 18 U.S.C. § 2703(a). Once a magistrate judge signs the warrant, however, investigators ordinarily do not themselves search through the provider's computers in search of the materials described in the warrant. Instead, investigators serve the warrant on the provider as they would a subpoena, and the provider produces the material described in the warrant.

One district court recently held unconstitutional the practice of having service providers produce the materials specified in a search warrant. See United States v. Bach, 2001 WL 1690055 (D. Minn. Dec. 14, 2001). In Bach, state law enforcement officials obtained a search warrant under state law for information regarding a Yahoo email account and faxed the warrant to Yahoo, which produced the appropriate documents. The district court suppressed the results of the search as a Fourth Amendment violation. The court held that the Fourth Amendment mandates the protections codified in 18 U.S.C. § 3105, which requires that a law enforcement officer be present and act in the execution of a search warrant. According to the court, "section 2703 is not an exception to and does not provide an alternative mode of execution from section 3105," so federal law enforcement officials are mandated by statute to comply with § 3105 when executing a search warrant under 2703(a). The court held that even in the absence of a statutory mandate, the Fourth Amendment requires a law enforcement officer to be present and act in the execution of any search warrant, including a warrant issued under 2703(a).

The government has appealed the Bach decision. The government's brief points out that, leaving aside Bach's questionable Fourth Amendment jurisprudence and the inappropriateness of the suppression remedy, ECPA makes clear Congress's intent to authorize the use of § 2703 search warrants for subscriber content as a form of compulsory process directed to third-party network providers - not as a

traditional search warrant. See, e.g., 18 U.S.C. §§ 2702(b)(2), (c)(1) (stating explicitly that a provider may disclose customer records in response to § 2703 process). Furthermore, even if 18 U.S.C. § 3105 were applicable to warrants served pursuant to ECPA, § 3105 does not require the presence of law enforcement when service providers collect and produce information pursuant to a search warrant because the problems associated with private exercise of search and seizure powers are not implicated when service providers collect and produce information in response to a warrant. See In re Application of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities, 616 F.2d 1122, 1130 (9th Cir. 1980); In re Application of the United States for an Order Authorizing the Installation of a Pen Register or Touch-Tone Decoder and Terminating Trap, 610 F.2d 1148, 1154 (3rd Cir. 1979). Moreover, practically speaking, requiring the presence of law enforcement at the execution of these search warrants would prove extremely burdensome, as searches can prove time consuming, and ISPs maintain account information in a variety of locations. Also, it is difficult to imagine how a law enforcement officer could play a useful role in a service provider's actual retrieval of the specified records.

Nevertheless, in the interest of caution, until the issues raised in Bach are ultimately resolved, law enforcement officials preparing a warrant pursuant to § 2703 are advised to request in the search warrant application that the magistrate expressly permit faxing the warrant to the ISP and executing the warrant without the officer present. For draft language or other information and guidance regarding Bach, contact the Computer Crime and Intellectual Property Section at (202) 514-1026.

E. Voluntary Disclosure

Providers of services not available "to the public" may freely disclose both contents and other records relating to stored communications. ECPA imposes restrictions on voluntary disclosures by providers of services to the public, but it also includes exceptions to those restrictions.

The voluntary disclosure provisions of ECPA appear in 18 U.S.C. § 2702. These provisions govern when a provider of RCS or ECS can disclose contents and other information voluntarily, both to the government and non-government entities. If the provider may disclose the information to the government and is willing to do so voluntarily, law enforcement does not need to obtain a legal order to compel the disclosure. If the provider either may not or will not disclose the information, agents must rely on compelled disclosure provisions and obtain the appropriate legal orders.

When considering whether a provider of RCS or ECS can disclose contents or records, the first question agents must ask is whether the relevant service offered by the provider is available "to the public." If the provider does not provide the applicable service "to the public," then ECPA does not place any restrictions on disclosure. See 18 U.S.C. § 2702(a). For example, in Andersen Consulting v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998), the petroleum company UOP hired the consulting firm Andersen Consulting and gave Andersen employees accounts on UOP's computer network. After the relationship between UOP and Andersen soured, UOP disclosed to the *Wall Street Journal* e-mails that Andersen employees had left on the UOP network. Andersen sued, claiming that the disclosure of its contents by the provider UOP had violated ECPA. The district court rejected the suit on the ground that UOP did not provide an electronic communication service to the public:

> [G]iving Andersen access to [UOP's] e-mail system is not equivalent to providing e-mail to the public. Andersen was hired by UOP to do a project and as such, was given access to UOP's e-

> mail system similar to UOP employees. Andersen was not any member of the community at large, but a hired contractor.

Id. at 1043. Because UOP did not provide services to the public, ECPA did not prohibit disclosure of contents belonging to UOP's "subscribers."

If the services offered by the provider *are* available to the public, then ECPA forbids both the disclosure of contents to any third party and the disclosure of other records *to any governmental entity*, unless a statutory exception applies.[21] Section 2702(b) contains exceptions for disclosure of contents, and § 2702(c) contains exceptions for disclosure of other customer records.

ECPA provides for the voluntary disclosure of contents when:

1) the disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," § 2702(b)(5);

2) the disclosure is made "to a law enforcement agency . . . if the contents . . . were inadvertently obtained by the service provider . . .[and] appear to pertain to the commission of a crime," § 2702(b)(6)(A);

3) the provider "reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay," § 2702(b)(6)(C);

4) the Child Protection and Sexual Predator Punishment Act of 1998, 42 U.S.C. § 13032, mandates the disclosure, 18 U.S.C. § 2702(b)(6)(B); or

5) the disclosure is made to the intended recipient of the communication, with the consent of the intended recipient or sender, to a forwarding address, or pursuant to a court order or legal process. § 2702(b)(1)-(4).

ECPA provides for the voluntary disclosure of non-content customer records by a provider to a governmental entity when:[22]

1) the disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," § 2702(c)(3);

2) the provider "reasonably believes that an emergency involving immediate danger of death of serious physical injury to any person" justifies disclosure, § 2702(c)(4); or

3) the disclosure is made with the consent of the intended recipient, or pursuant to a court order or legal process § 2702(c)(1)-(2).

In general, these exceptions permit disclosure by a provider to the public when the needs of public safety and service providers outweigh privacy concerns of customers, or else when disclosure is unlikely to pose a serious threat to privacy interests.

F. Quick Reference Guide

Voluntary Disclosure Allowed?		**Mechanisms to Compel Disclosure**	
Public Provider	Non-Public Provider	Public Provider	Non-Public Provider
	Not to government,	Yes	Subpoena; 2703(d) order; or search	Subpoena; 2703(d) order;

Basic subscriber, session, and billing information	unless § 2702(c) exception applies [§ 2702(a)(3)]	[§ 2702 (a)(3)]	warrant [§ 2703(c)(2)]	or search warrant [§ 2703(c)(2)]
Other transactional and account records	Not to government, unless § 2702(c) exception applies [§ 2702(a)(3)]	Yes [§ 2702 (a)(3)]	2703(d) order or search warrant [§ 2703(c)(1)]	2703(d) order or search warrant [§ 2703(c)(1)]
Accessed communications (opened e-mail and voice mail) left with provider and other stored files	No, unless § 2702(b) exception applies [§ 2702(a)(2)]	Yes [§ 2702 (a)(2)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(b)]	Subpoena; ECPA doesn't apply [§ 2711(2)]
Unretrieved communication, including e-mail and voice mail (in electronic storagemore than 180 days)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702 (a)(1)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a,b)]	Subpoena with notice; 2703(d) order with notice; or search warrant [§ 2703(a,b)]
Unretrieved communication, including e-mail and voice mail (in electronic storage 180 days or less)	No, unless § 2702(b) exception applies [§ 2702(a)(1)]	Yes [§ 2702 (a)(1)]	Search warrant [§ 2703(a)]	Search warrant [§ 2703(a)]

G. Working with Network Providers: Preservation of Evidence, Preventing Disclosure to Subjects, and Cable Act Issues

In general, investigators should communicate with network service providers before issuing subpoenas or obtaining court orders that compel the providers to disclose information.

Law enforcement officials who procure records under ECPA quickly learn the importance of communicating with network service providers. This is true because every network provider works differently. Some providers retain very complete records for a long period of time; others retain few records, or even none. Some providers can comply easily with law enforcement requests for information; others struggle to comply with even simple requests. These differences result from varied philosophies, resources, hardware and software among network service providers. Because of these differences, agents often will want to communicate with network providers to learn how the provider operates *before* obtaining a legal order that compels the provider to act.

ECPA contains two provisions designed to aid law enforcement officials working with network service providers. When used properly, these provisions help ensure that providers will not delete needed records or notify others about the investigation.

1. Preservation of Evidence under 18 U.S.C. § 2703(f)

Agents may direct providers to preserve existing records pending the issuance of compulsory legal process. Such requests have no prospective effect, however.

In general, no law regulates how long network service providers must retain account records in the United States. Some providers retain records for months, others for hours, and others not at all. As a practical matter, this means that evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. For example, agents may learn of a child pornography case on Day 1, begin work on a search warrant on Day 2, obtain the warrant on Day 5, and then learn that the network service provider deleted the records in the ordinary course of business on Day 3. To minimize this risk, ECPA permits the government to direct providers to "freeze" stored records and communications pursuant to 18 U.S.C. § 2703(f). Specifically, § 2703(f)(1) states:

A provider of wire or electronic communication service or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

There is no legally prescribed format for § 2703(f) requests. While a simple phone call should therefore be adequate, a fax or an e-mail is better practice because it both provides a paper record and guards against miscommunication. Upon receipt of the government's request, the provider must retain the records for 90 days, renewable for another 90-day period upon a government request. See 18 U.S.C. § 2703(f)(2). A sample § 2703(f) letter appears in Appendix C.

Agents who send § 2703(f) letters to network service providers should be aware of two limitations. First, the authority to direct providers to preserve records and other evidence is not prospective. That is, § 2703(f) letters can order a provider to preserve records that have already been created, but cannot order providers to preserve records not yet made. If agents want providers to record information about future electronic communications, they must comply with the electronic surveillance statutes discussed in Chapter 4.

A second limitation of § 2703(f) is that some providers may be unable to comply effectively with § 2703(f) requests. As of the time of this writing, for example, the software used by America Online generally requires AOL to reset the password of an account when it attempts to comply with a § 2703(f) request to preserve stored e-mail. A reset password may well tip off the suspect. As a result, agents may or may not want to issue § 2703(f) letters to AOL or other providers who use similar software, depending on the facts. The key here is effective communication: agents should communicate with the network provider before ordering the provider to take steps that may have unintended adverse effects. Agents simply cannot make informed investigative choices without knowing the provider's particular practices, strengths, and limitations.

2. Orders Not to Disclose the Existence of a Warrant, Subpoena, or Court Order

18 U.S.C. § 2705(b) states:
A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications
service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in--
(1) endangering the life or physical safety of an individual;
(2) flight from prosecution;
(3) destruction of or tampering with evidence;
(4) intimidation of potential witnesses; or
(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.
18 U.S.C. § 2705(b).
This language permits agents to apply for a court order directing network service providers not to disclose the existence of compelled process whenever the government itself has no legal duty to notify the customer or subscriber of the process. If the relevant process is a § 2703(d) order or § 2703(a) warrant, agents can simply include appropriate language in the application and proposed order or warrant. If agents instead seek to compel information using a subpoena, they must apply separately for this order.

3. The Cable Act, 47 U.S.C. § 551

The Cable Act restricts government access to cable operator records only when the records relate to ordinary cable services. It does not restrict government access to records relating to Internet access or telephone service provided by a cable operator.
In 1984, Congress passed the Cable Communications Policy Act ("the Cable Act"), 47 U.S.C. § 551, setting forth a restrictive system of rules governing law enforcement access to records possessed by a cable company. Under these rules, even a search warrant was insufficient to gain access to cable company records. The government could obtain "personally identifiable information concerning a cable subscriber" only by overcoming a heavy burden of proof at an in-court adversary proceeding, as specified in 47 U.S.C. § 551(h).
Subsequent to the 1984 passage of the Cable Act, cable companies began to provide Internet access and telephone service. Some cable companies asserted that the stringent disclosure restrictions of the Cable Act governed not only their provision of traditional cable programming services, but also their provision of Internet and telephone services. Congress responded in the 2001 USA PATRIOT Act by amending the Cable Act to specify that its disclosure restrictions apply only to records revealing what ordinary cable television programming a customer purchases, such as particular premium channels or "pay per view" shows. See PATRIOT Act § 211, 115 Stat. 272, 283-84 (2001). In particular, cable operators may disclose subscriber information to the government pursuant to ECPA, Title III, and the Pen Register/Trap and Trace statute, except for "records revealing cable subscriber selection of video programming." 47 U.S.C. § 551(c)(2)(D). Records revealing subscriber selection of video programming remain subject to the restrictions of 47 U.S.C. § 551(h).

H. Remedies

1. Suppression

ECPA does not provide a suppression remedy. See 18 U.S.C. § 2708 ("The [damages] remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."). Accordingly, nonconstitutional violations of ECPA do not result in suppression of the evidence. See United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998) ("[T]he Stored Communications Act expressly rules out exclusion as a remedy"); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("[S]uppression is not a remedy contemplated under the ECPA."); United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) ("Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act."), aff'd, 225 F.3d 656, 2000 WL 1062039 (4th Cir. 2000); United States v. Charles, 1998 WL 204696, at *21 (D. Mass. 1998) ("ECPA provides only a civil remedy for a violation of § 2703"); United States v. Reyes, 922 F. Supp. 818, 837-38 (S.D.N.Y. 1996) ("Exclusion of the evidence is not an available remedy for this violation of the ECPA. . . . The remedy for violation of [18 U.S.C. § 2701-11] lies in a civil action.").[(23)]

Defense counsel seeking suppression of evidence obtained in violation of ECPA are likely to rely on McVeigh v. Cohen, 983 F. Supp. 215 (D.D.C. 1998). In this unusual case, Judge Sporkin enjoined the United States Navy from dismissing 17-year Navy veteran Timothy R. McVeigh after the Navy learned that McVeigh was gay. The Navy learned of McVeigh's sexual orientation after McVeigh sent an e-mail signed "Tim" from his AOL account "boysrch" to the AOL account of a civilian Navy volunteer. When the volunteer examined AOL's "member profile directory," she learned that "boysrch" belonged to a man in the military stationed in Honolulu who listed his marital status as "gay." Suspecting that the message was from McVeigh, the volunteer forwarded the e-mail and directory profile to officers aboard McVeigh's submarine. The officers then began investigating McVeigh's sexual orientation. To confirm McVeigh's identity, a Navy paralegal telephoned AOL and offered a false story for why he needed the real name of "boysrch." The paralegal did not disclose that he was a Naval serviceman. After the AOL representative confirmed that "boysrch" belonged to McVeigh's account, the Navy began a discharge proceeding against McVeigh. Shortly before McVeigh's discharge was to occur, McVeigh filed suit and asked for a preliminary injunction blocking the discharge. Judge Sporkin granted McVeigh's motion the day before the discharge.

Judge Sporkin's opinion reflects both the case's highly charged political atmosphere and the press of events surrounding the issuance of the opinion.[(24)]

In the course of criticizing the Navy for substituting subterfuge for ECPA's legal process to obtain McVeigh's basic subscriber information from AOL, Judge Sporkin made statements that could be interpreted as reading a suppression remedy into ECPA for flagrant violations of the statute:

[I]t is elementary that information obtained improperly can be suppressed where an individual's rights have been violated. In these days of 'big brother,' where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed.

Id. at 220. While ECPA should be strictly observed, the statement that suppression is appropriate when information is obtained in violation of "an individual's rights" is somewhat perplexing. Both the case law

and the text of ECPA itself make clear that ECPA does not offer a suppression remedy for nonconstitutional violations. Accordingly, this statement must be construed to refer only to *constitutional* rights.

2. Civil Actions and Disclosures

Although ECPA does not provide a suppression remedy for statutory violations, it does provide for civil damages (including, in some cases, punitive damages), as well as the prospect of disciplinary actions against officers and employees of the United States who have engaged in willful violations of the statute. Liability and discipline can result not only from violations of the rules already described in this chapter, but also from the improper disclosure of some kinds of ECPA-related information. Information that is obtained through process (subpoena, order, or search warrant) under ECPA and that qualifies as a "record" under the Privacy Act, 5 U.S.C. § 552a(a), cannot willfully be disclosed by an officer or governmental entity without violating ECPA. See 18 U.S.C. § 2707(g). However, it is not a violation to make a disclosure "in the proper performance of the official functions of the officer or governmental agency making the disclosure," nor is it unlawful to disclose information that has been previously and lawfully disclosed to the public. Id. Section 2707(g), unless extended, will sunset on December 31, 2005. See PATRIOT Act §§ 223, 224, 115 Stat. 272, 293-95 (2001).

ECPA includes separate provisions for suits against the United States and suits against any other person or entity. 18 U.S.C. § 2707 permits a "person aggrieved" by an ECPA violation to bring a civil action against the "person or entity, other than the United States, which engaged in that violation." 18 U.S.C. § 2707(a). Relief can include money damages no less than $1,000 per person, equitable or declaratory relief, and a reasonable attorney's fee plus other reasonable litigation costs. Willful or intentional violations can also result in punitive damages, see § 2707(b)-(c), and employees of the United States may be subject to disciplinary action for willful or intentional violations. See § 2707(d). A good faith reliance on a court order or warrant, grand jury subpoena, legislative authorization, or statutory authorization provides a complete defense to any ECPA civil or criminal action. See § 2707(e). Qualified immunity may also be available. See Chapter 4.D.2.

Suits against the United States may be brought under 18 U.S.C. § 2712 for willful violations of ECPA, Title III, or specified sections of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801. This section authorizes courts to award actual damages or $10,000, whichever is greater, and reasonable litigation costs. Section 2712 also defines procedures for suits against the United States and a process for staying proceedings when civil litigation would interfere with a related investigation or criminal prosecution. See 18 U.S.C. § 2712 (b), (e). Unless extended, § 2712 will sunset on December 31, 2005. See PATRIOT Act §§ 223, 224, 115 Stat. 272, 293-95 (2001).

\

IV. ELECTRONIC SURVEILLANCE IN COMMUNICATIONS NETWORKS

A. Introduction

Criminal investigations often involve electronic surveillance. In computer crime cases, agents may want to monitor a hacker as he breaks into a victim computer system, or set up a "cloned" e-mail box to monitor a suspect sending or receiving child pornography over the Internet. In a more traditional context, agents may wish to wiretap a suspect's telephone, or learn whom the suspect has called, and when. This chapter explains how the electronic surveillance statutes work in criminal investigations involving computers.

Two federal statutes govern real-time electronic surveillance in federal criminal investigations. The first and most important is the wiretap statute, 18 U.S.C. §§ 2510-2522, first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (and generally known as "Title III"). The second statute is the Pen Registers and Trap and Trace Devices chapter of Title 18 ("the Pen/Trap statute"), 18 U.S.C. §§ 3121-3127, which governs pen registers and trap and trace devices. Failure to comply with these statutes may result in civil and criminal liability, and in the case of Title III, may also result in suppression of evidence.

B. Content vs. Addressing Information

In general, the Pen/Trap statute regulates the collection of addressing and other non-content information for wire and electronic communications. Title III regulates the collection of actual content of wire and electronic communications.

Title III and the Pen/Trap statute coexist because they regulate access to different types of information. Title III permits the government to obtain the contents of wire and electronic communications in transmission. In contrast, the Pen/Trap statute concerns the real-time collection of addressing and other non-content information relating to those communications. See 18 U.S.C. § 2511(h)(i) (stating that it is not a violation of Title III to use a pen register or trap and trace device); United States Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000); Brown v. Waddell, 50 F.3d 285, 289-94 (4th Cir. 1995) (distinguishing pen registers from Title III intercept devices).

The difference between addressing information and content is clear in the case of traditional communications such as telephone calls. The addressing information for a telephone call is the phone number dialed for an outgoing call, and the originating number (the caller ID information) for an incoming call. In contrast, the content of the communication is the actual conversation between the parties to the call.

The distinction between addressing information and content also applies to Internet communications. For example, when computers attached to the Internet communicate with each other, they break down messages into discrete chunks known as "packets," and then send each packet out to its intended destination. Every packet contains addressing information in the "header" of the packet (much like the "to" and "from" addresses on an envelope), followed by the content of the message (much like a letter inside an envelope). The Pen/Trap statute permits law enforcement to obtain the addressing information

of Internet communications much as it would addressing information for traditional phone calls. However, reading the entire packet ordinarily implicates Title III. The primary difference between an Internet pen/trap device and an Internet Title III intercept device (sometimes known as a "sniffer") is that the former is programmed to capture and retain only addressing information, while the latter is programmed to capture and retain the entire packet.

The same distinction applies to Internet e-mail. Every Internet e-mail message consists of a set of headers that contain addressing and routing information generated by the mail program, followed by the actual contents of the message authored by the sender. The addressing and routing information includes the e-mail address of the sender and recipient, as well as information about when and where the message was sent on its way (roughly analogous to the postmark on a letter). The Pen/Trap statute permits law enforcement to obtain the addressing information of Internet e-mails (minus the subject line, which can contain content) using a court order, just like it permits law enforcement to obtain addressing information for phone calls and individual Internet "packets" using a court order. Conversely, the interception of e-mail contents, including the subject line, requires careful compliance with the strict dictates of Title III.

In some circumstances, there can be debate about the distinction between addressing information and content. Prosecutors or agents who encounter such issues should contact the Computer Crime and Intellectual Property Section at (202) 514-1026 or their local CTC (see Introduction, p. ix).

C. The Pen/Trap Statute, 18 U.S.C. §§ 3121-3127

The Pen/Trap statute authorizes a government attorney to apply to a court for an order authorizing the installation of a pen register and/or trap and trace device so long as "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2). In rough terms, a pen register records outgoing addressing information (such as a number dialed from a monitored telephone), and a trap and trace device records incoming addressing information (such as caller ID information). Although the Pen/Trap statute previously included language which specifically referenced telephone communications, numerous courts had applied the statute to computer network communications. In 2001, the USA PATRIOT Act confirmed that the Pen/Trap statute applies to a wide range of communication technologies. See PATRIOT Act § 216, 115 Stat. 272, 288-90 (2001).

1. Definition of pen register and trap and trace device

The Pen/Trap statute defines pen registers and trap and trace devices broadly. As defined in 18 U.S.C. § 3127(3), a "pen register" 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, provided, however, that such information shall not include the contents of any communication . . . .

The definition of pen register further excludes devices or processes used for billing or cost accounting. See 18 U.S.C. § 3127(3). The statute defines a "trap and trace device" as

> a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, or 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.

18 U.S.C. § 3127(4). Because Internet headers contain both "to" and "from" information, a device that reads the entire header (minus the subject line in the case of e-mail headers) is known simply as a pen/trap device.

The breadth of these definitions results from the scope of their components. First, "an instrument or facility from which a wire or electronic communication is transmitted" encompasses a wide variety of communications technologies, including a telephone, a cellular telephone, an Internet user account, an e-mail account, or an IP address. Second, the definitions' inclusion of all "dialing, routing, addressing, or signaling information" encompasses almost all non-content information in a communication. Third, because the definitions of a pen register and a trap and trace device include both a "device" and a "process," the statute covers software routines as well as physical devices. Because the definitions are written in broad, technology-neutral language, prosecutors or agents may have questions about whether particular devices constitute pen registers or trap and trace devices, and they should direct any such questions to the Computer Crime and Intellectual Property Section at (202) 514-1026, the Office of Enforcement Operations at (202) 514-6809, or their local CTC (see Introduction, p. ix).

2. Pen/Trap Orders: Application, Issuance, Service, and Reporting

To obtain a pen/trap order, applicants must identify themselves, identify the law enforcement agency conducting the investigation, and then certify their belief that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency. See 18 U.S.C. § 3122(b)(1)-(2). The issuing court must also have jurisdiction over the offense being investigated. See 18 U.S.C. § 3127(2)(a). So long as the application contains these elements, the court will authorize the installation and use of a pen/trap device anywhere in the United States. See 18 U.S.C. § 3123(a)(1). The court will not conduct an "independent judicial inquiry into the veracity of the attested facts." In re Application of the United States, 846 F. Supp. 1555, 1558-59 (M.D. Fla. 1994). See also United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) ("The judicial role in approving use of trap and trace devices is ministerial in nature.").

A federal pen/trap order may have effect outside the district of the issuing court. In the case of a federal applicant, the order "appl[ies] to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order." 18 U.S.C. § 3123(a)(1). For example, a federal prosecutor may obtain an order to trace telephone calls made to a particular telephone. The order applies not only to the local carrier serving that line, but also to other providers (such as long-distance carriers and regional carriers in other parts of the country) through whom calls are placed to the target telephone. Similarly, in the Internet context, a federal prosecutor may obtain an order to trace communications to a particular victim computer or IP address. If a hacker is routing communications through a chain of intermediate pass-through computers, the order would apply to each computer in the chain from the victim to the source of the communications.

The Pen/Trap statute does not require the pen/trap application or order to specify all of the providers subject to the order, although the order must specify the initial provider. See 18 U.S.C. § 3123(b)(1)(A). To receive a provider's assistance, an investigator simply needs to serve the provider with the order. Upon the provider's request, law enforcement must also provide "written or electronic certification" that the order applies to the provider. See 18 U.S.C. § 3123(a)(1). There are strong practical motivations for this relatively informal process. When prosecutors apply for a pen/trap order, they usually will not know the identity of upstream providers in the chain of communications covered by the order. If law enforcement personnel were required to return to court each time they discovered the identity of a new provider, investigations would be delayed significantly.

A pen/trap order may authorize use of a pen/trap device for up to sixty days, and may be extended for additional sixty-day periods. See 18 U.S.C. § 3123(c). The court order also directs the provider not to disclose the existence of the pen/trap "to any . . . person, unless or until otherwise ordered by the court," 18 U.S.C. § 3123(d)(2), and may order providers of wire or electronic communications service, landlords, custodians, or other persons to "furnish . . . forthwith all information, facilities, and technical assistance necessary" to install pen/trap devices. See 18 U.S.C. § 3124(a), (b). Providers who are ordered to assist with the installation of pen/trap devices under § 3124 can receive reasonable compensation for reasonable expenses incurred in providing facilities or technical assistance to law enforcement. See 18 U.S.C. § 3124(c). A provider's good faith reliance on a court order provides a complete defense to any civil or criminal action arising from its assistance in accordance with the order. See 18 U.S.C. § 3124(d), (e).

The Pen/Trap statute contains a reporting requirement for the narrow class of cases in which law enforcement officers install their own pen/trap device on a packet-switched network of a provider of electronic communications service. See 18 U.S.C. § 3123(a)(3)(A). Usually, when law enforcement serves a pen/trap order on a provider, the provider itself will collect the specified information and provide it to law enforcement. In cases where a provider cannot or will not do so, or in other rare instances, the government may install its own pen/trap device, such as the FBI's DCS 1000. In these cases, the government must provide the following information to the court under seal within thirty days after termination of the order: (1) the identity of the officers who installed or accessed the device; (2) the date and time the device was installed, accessed, and uninstalled; (3) the configuration of the device at installation and any subsequent modifications of that configuration; and (4) the information collected by the device. See 18 U.S.C. § 3123(a)(3). When the government installs a pen/trap device, it must use "technology reasonably available to it" in order to avoid recording or decoding the contents of a wire or electronic communication. See 18 U.S.C. § 3121(c).

Importantly, the limited judicial review of pen/trap orders coexists with a strong enforcement mechanism for violations of the statute. See 18 U.S.C. § 3121(d) (providing criminal penalties for violations of the pen/trap statute). As one court has explained,

> [t]he salient purpose of requiring the application to the court for an order is to affix personal responsibility for the veracity of the application (i.e., to ensure that the attesting United States Attorney is readily identifiable and legally qualified) and to confirm that the United States Attorney has sworn that the required investigation is in progress. . . . As a form of deterrence and as a guarantee of compliance, the statute provides . . . for a term of imprisonment and a fine as punishment for a violation [of the statute].

In re Application of the United States, 846 F. Supp. at 1559.

The Pen/Trap statute also grants providers of electronic or wire communication service broad authority to use pen/trap devices on their own networks without a court order. 18 U.S.C. § 3121(b) states that providers may use pen/trap devices without a court order

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or

(3) where the consent of the user of that service has been obtained.

18 U.S.C. § 3121(b).

D. The Wiretap Statute ("Title III"), 18 U.S.C. §§ 2510-2522

1. Introduction: The General Prohibition

Since its enactment in 1968 and amendment in 1986, Title III has provided the statutory framework that governs real-time electronic surveillance of the contents of communications. When agents want to wiretap a suspect's phone, "keystroke" a hacker breaking into a computer system, or accept the fruits of wiretapping by a private citizen who has discovered evidence of a crime, the agents first must consider the implications of Title III.

The structure of Title III is surprisingly simple. The statute's drafters assumed that every private communication could be modeled as a two-way connection between two participating parties, such as a telephone call between A and B. At a fundamental level, the statute prohibits a third party (such as the government) who is not a participating party to the communication from intercepting private communications between the parties using an "electronic, mechanical, or other device," unless one of several statutory exceptions applies. See 18 U.S.C. § 2511(1). Importantly, this prohibition is quite broad. Unlike some privacy laws that regulate only certain cases or specific places, Title III expansively prohibits eavesdropping (subject to certain exceptions and interstate requirements) essentially everywhere by anyone in the United States. Whether investigators want to conduct surveillance at home, at work, in government offices, in prison, or on the Internet, they must make sure that the monitoring complies with Title III's prohibitions.

The questions that agents and prosecutors must ask to ensure compliance with Title III are straightforward, at least in form: 1) Is the communication to be monitored one of the protected communications defined in 18 U.S.C. § 2510? 2) Will the proposed surveillance lead to an "interception" of the communications? 3) If the answer to the first two questions is "yes," does a statutory exception apply that permits the interception?

2. Key Phrases

Title III broadly prohibits the "interception" of "oral communications," "wire communications," and "electronic communications." These phrases are defined by the statute. See generally 18 U.S.C. § 2510. In computer crime cases, agents and prosecutors planning electronic surveillance must understand the definition of "wire communication," "electronic communication," and "intercept." (Surveillance of oral communications rarely arises in computer crime cases, and will not be addressed directly here. Agents and prosecutors requiring assistance in cases involving oral communications should contact the Justice Department's Office of Enforcement Operations at (202) 514-6809.)

"Wire communication"

In general, telephone conversations are wire communications.

According to § 2510(1), "wire communication" means

> any aural transfer made in whole or in part though the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.

Within this complicated definition, the most important requirement is that the content of the communication must include the human voice. See § 2510(18) (defining "aural transfer" as "a transfer containing the human voice at any point between and including the point of origin and point of reception"). If a communication does not contain a genuine human voice, either alone or in a group conversation, then it cannot be a wire communication. See S. Rep. No. 99-541, at 12 (1986), reprinted in 1986 U.S.C.C.A.N. 3555; United States v. Torres, 751 F.2d 875, 885-86 (7th Cir. 1984) (concluding that "silent television surveillance" cannot lead to an interception of wire communications under Title III because no aural acquisition occurs).

The additional requirement that wire communications must be sent "in whole or in part . . . by the aid of wire, cable, or other like connection . . ." presents a fairly low hurdle. So long as the signal travels through wire at some point along its route between the point of origin and the point of reception, the requirement is satisfied. For example, all voice telephone transmissions, including those from satellite signals and cellular phones, qualify as wire communications. See H.R. Rep. No. 99-647, at 35 (1986). Because such transmissions are carried by wire within switching stations, they are expressly included in the definition of wire communication. Importantly, the presence of wire inside equipment at the sending or receiving end of a communication (such as an individual cellular phone) does not satisfy the requirement that a communication be sent "in part" by wire. The wire must transmit the communication "to a significant extent" along the path of transmission, outside of the equipment that sends or receives the communication. Id.

It should be noted that prior to the passage of the USA PATRIOT Act of 2001, the definition of "wire communication" explicitly included "any electronic storage of such communication." The USA PATRIOT Act deleted this phrase and amended § 2703 of ECPA to ensure that stored wire communications (e.g. voice mails) are covered not under Title III, but instead under the ECPA provisions that also apply to stored electronic communication, or e-mails. See PATRIOT Act § 209, 115 Stat. 272, 283 (2001). The practical effect of this change is that government access to stored voice mail is no longer controlled by Title III. Instead, voice mail is now covered by ECPA, and disclosure rules for

voice mail are now identical to the rules for e-mail. This change will sunset December 31, 2005, unless extended by Congress. See Chapter 3.A, supra.

"Electronic communication"

Most Internet communications (including e-mail) are electronic communications.

18 U.S.C. § 2510(12) defines "electronic communication" as

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device . . . ; or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

As the definition suggests, electronic communication is a broad, catch-all category. See United States v. Herring, 993 F.2d 784, 787 (11th Cir. 1993). "As a rule, a communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice (carried in part by wire)." H.R. Rep. No. 99-647, at 35 (1986). Most electric or electronic signals that do not fit the definition of wire communications qualify as electronic communications. For example, almost all Internet communications (including e-mail) qualify as electronic communications.

"Intercept"

The structure and language of ECPA and Title III require that the term "intercept" be applied only to communications acquired contemporaneously with their transmission, and not to the acquisition of stored wire or electronic communications. Most courts have adopted this approach, but this issue is unresolved in the Ninth Circuit.

Section 2510(4) defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." The word "acquisition" is ambiguous in this definition. For example, when law enforcement surveillance equipment records the contents of a communication, the communication might be "acquired" at three distinct points: first, when the equipment records the communication; second, when law enforcement later obtains the recording; or third, when law enforcement plays the recording and either hears or sees the contents of the communication. The text of § 2510(4) does not specify which of these events constitutes an "acquisition" for the purposes of Title III. See United States v. Turk, 526 F.2d 654, 657-58 (5th Cir. 1976).

Moreover, the definition of "intercept" does not explicitly address whether the acquisition must be contemporaneous with the transmission. However, the relationship between Title III and ECPA requires that the meaning of "intercept" be restricted to acquisitions of communications contemporaneous with their transmission. For example, an e-mail or voice mail may spend time in electronic storage before it is ultimately retrieved by its recipient. If law enforcement obtains such a communication from electronic storage, it has not intercepted the communication within the meaning of Title III, because acquisition of the contents of stored electronic or wire communications is governed by § 2703(a) of ECPA, not by Title III.

Most courts have adopted this interpretation and held that both wire and electronic communications are intercepted only when they are acquired contemporaneously with their transmission. In other words, interception of the communications refers only to their real-time acquisition at the time of transmission between the parties to the communication. An investigator who subsequently obtains access to a stored copy of the communication does not "intercept" the communication. See, e.g., Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 460-63 (5th Cir. 1994) (access to stored e-mail communications) ; Wesley College v. Pitts, 974 F. Supp. 375, 384-90 (D. Del. 1997) (same); United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990) (access to stored pager communications); United States v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996) (same); Bohach v. City of Reno, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996) (same); United States v. Moriarty, 962 F. Supp. 217, 220-21 (D. Mass. 1997) (access to stored wire communications) ; In re State Police Litigation, 888 F. Supp 1235, 1264 (D. Conn. 1995) (same); Payne v. Norwest Corp., 911 F. Supp. 1299, 1303 (D. Mont. 1995), aff'd in part and rev'd in part, 113 F.3d 1079 (9th Cir. 1997) (same). In addition, because communications are intercepted only if acquired contemporaneously with transmission, a key logger device on a personal computer will not intercept communications if it is configured such that keystrokes are not recorded when the computer's modem is in use. See United States v. Scarfo, 180 F. Supp. 2d 572, 582 (D.N.J. 2001).

In the Ninth Circuit, the question of whether the definition of "intercept" is limited to real-time acquisitions remains for now less certain, for reasons that require some historical explanation. Prior to passage of the USA PATRIOT Act, the definition of "wire communication" in § 2510(1), unlike the definition of "electronic communication" in § 2510(12), explicitly included "any electronic storage of such communication." In United States v. Smith, 155 F.3d 1051, 1058-59 (9th Cir. 1998), the Ninth Circuit held that a party can intercept a wire communication by obtaining a copy of the communication in "electronic storage," as defined in § 2510(17). The court reasoned that wire communications should be treated differently than electronic communications because the definition of wire communication expressly included the phrase "any electronic storage of such communication," and because limiting interceptions of wire communications to contemporaneous acquisitions would have rendered that phrase meaningless, as wire communications in electronic storage could never be intercepted. See id. at 1057-58.[(25)] The court went on to define "intercept" under Title III in relation to "access" under § 2701 of ECPA, with an interception "entail[ing] actually acquiring the contents of a communication, whereas the word 'access' merely involves being in a position to acquire the contents of a communication." Id. at 1058.

Now, however, the USA PATRIOT Act has eliminated the statutory basis for the Ninth Circuit's decision in Smith by deleting the phrase "any electronic storage of such communication" from the definition of wire communication and by explicitly including stored wire communications in § 2703 of ECPA. There is now a clear and uniform statutory distinction between stored electronic and wire communications, which are subject to ECPA, and contemporaneous interceptions of electronic and wire communications, which are subject to Title III.

3. Exceptions to Title III

Title III broadly prohibits the intentional interception, use, or disclosure[(26)] of wire and electronic communications unless a statutory exception applies. See 18 U.S.C. § 2511(1). In general, this prohibitions bars third parties (including the government) from wiretapping telephones and installing electronic "sniffers" that read Internet traffic.

The breadth of Title III's prohibition means that the legality of most surveillance techniques under Title III depends upon whether a statutory exception to the rule applies. Title III contains dozens of exceptions, which may or may not apply in hundreds of different situations. In computer crime cases, however, seven exceptions apply most often:
A) interception pursuant to a § 2518 court order;
B) the 'consent' exception, § 2511(2)(c)-(d);
C) the 'provider' exception, § 2511(2)(a)(i);
D) the 'computer trespasser' exception, § 2511(2)(i);
E) the 'extension telephone' exception, § 2510(5)(a);
F) the 'inadvertently obtained criminal evidence' exception, § 2511(3)(b)(iv); and
G) the 'accessible to the public' exception, § 2511(2)(g)(i).
Prosecutors and agents need to understand the scope of these seven exceptions in order to determine whether different surveillance strategies will comply with Title III.

a) Interception Authorized by a Title III Order, 18 U.S.C. § 2518.

Title III permits law enforcement to intercept wire and electronic communications pursuant to a court order under 18 U.S.C. § 2518 (a "Title III order"). High-level Justice Department approval is required for federal Title III applications, by statute in the case of wire communications, and by Justice Department policy in the case of electronic communications (except for numeric pagers). When authorized by the Justice Department and signed by a United States District Court or Court of Appeals judge, a Title III order permits law enforcement to intercept communications for up to thirty days. See § 2518.
18 U.S.C. §§ 2516-2518 imposes several formidable requirements that must be satisfied before investigators can obtain a Title III order. Most importantly, the application for the order must show probable cause to believe that the interception will reveal evidence of a predicate felony offense listed in § 2516. See § 2518(3)(a)-(b). For federal agents, the predicate felony offense must be one of the crimes specifically enumerated in § 2516(1)(a)-(r) to intercept wire communications, or any federal felony to intercept electronic communications. See 18 U.S.C. § 2516(3). The predicate crimes for state investigations are listed in 18 U.S.C. § 2516(2). The application for a Title III order also (1) must show that normal investigative procedures have been tried and failed, or that they reasonably appear to be unlikely to succeed or to be too dangerous, see § 2518(1)(c); (2) must establish probable cause that the communication facility is being used in a crime; and (3) must show that the surveillance will be conducted in a way that minimizes the interception of communications that do not provide evidence of a crime. See § 2518(5). For comprehensive guidance on the requirements of 18 U.S.C. § 2518, agents and prosecutors should consult the Justice Department's Office of Enforcement Operations at (202) 514-6809.

b) Consent of a Party to the Communication, 18 U.S.C. § 2511(2)(c)-(d)

18 U.S.C. § 2511(2)(c) and (d) state:
(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.
(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one

of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

This language authorizes the interception of communications when one of the parties to the communication consents to the interception.[27] For example, if an undercover government agent or informant records a telephone conversation between himself and a suspect, his consent to the recording authorizes the interception. See, e.g., Obron Atlantic Corp. v. Barr, 990 F.2d 861 (6th Cir. 1993) (relying on § 2511(2)(c)). Similarly, if a private person records his own telephone conversations with others, his consent authorizes the interception unless the commission of a criminal or tortious act was at least a determinative factor in the person's motivation for intercepting the communication. See United States v. Cassiere, 4 F.3d 1006, 1021 (1st Cir. 1993) (interpreting § 2511(2)(d)).

Consent to Title III monitoring may be express or implied. See United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987). Implied consent exists when circumstances indicate that a party to a communication was "in fact aware" of monitoring, and nevertheless proceeded to use the monitored system. United States v. Workman, 80 F.3d 688, 693 (2d Cir. 1996); see also Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990) ("[I]mplied consent is consent in fact which is inferred from surrounding circumstances indicating that the party knowingly agreed to the surveillance.") (internal quotations omitted). In most cases, the key to establishing implied consent is showing that the consenting party received notice of the monitoring and used the monitored system despite the notice. See Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998). Proof of notice to the party generally supports the conclusion that the party knew of the monitoring. See Workman, 80 F.3d. at 693. Absent proof of notice, the government must "convincingly" show that the party knew about the interception based on surrounding circumstances in order to support a finding of implied consent. United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995).

i) "Bannering" and Implied Consent

Monitoring use of a computer network does not violate Title III after users view an appropriate "network banner" informing them that use of the network constitutes consent to monitoring.

In computer cases, the implied consent doctrine permits monitoring of a computer network that has been properly "bannered." A banner is a posted notice informing users as they log on to a network that their use may be monitored, and that subsequent use of the system will constitute consent to the monitoring. Every user who sees the banner before logging on to the network has received notice of the monitoring: by using the network in light of the notice, the user impliedly consents to monitoring pursuant to 18 U.S.C. § 2511(2)(c)-(d). See, e.g., Workman, 80 F.3d. at 693-94 (holding that explicit notices that prison telephones would be monitored generated implied consent to monitoring among inmates who subsequently used the telephones); United States v. Amen, 831 F.2d 373, 379 (2d Cir. 1987) (same). But see United States v. Thomas, 902 F.2d 1238, 1245 (7th Cir. 1990) (dicta) (questioning the reasoning of Amen).

The scope of consent generated by a banner generally depends on the banner's language: network banners are not "one size fits all." A narrowly worded banner may authorize only some kinds of monitoring; a broadly worded banner may permit monitoring in many circumstances for many reasons. In deciding what kind of banner is right for a given computer network, system providers look at the network's purpose, the system administrator's needs, and the users' culture. For example, a sensitive Department of Defense computer network might require a broad banner, while a state university network used by professors and students could use a narrow one. Appendix A contains several sample banners that reflect a range of approaches to network monitoring.

ii) Who is a "Party to the Communication" in a Network Intrusion?

Sections 2511(2)(c) and (d) permit any "person" who is a "party to the communication" to consent to monitoring of that communication. In the case of wire communications, a "party to the communication" is usually easy to identify. For example, either conversant in a two-way telephone conversation is a party to the communication. See, e.g., United States v. Davis, 1 F.3d 1014, 1015 (10th Cir. 1993). In a computer network environment, in contrast, the simple framework of a two-way communication between two parties breaks down. When a hacker launches an attack against a computer network, for example, he may route the attack through a handful of compromised computer systems before directing the attack at a final victim. At the victim's computer, the hacker may direct the attack at a user's network account, at the system administrator's "root" account, or at common files. Finding a "person" who is a "party to the communication" -- other than the hacker himself, of course -- can be a difficult (if not entirely metaphysical) task. Because of these difficulties, agents and prosecutors should adopt a cautious approach to the "party to the communication" consent exception. In hacking cases, the computer trespasser exception discussed in subsection (d) below may provide a more certain basis for monitoring communications.

A few courts have suggested that the owner of a computer system may satisfy the "party to the communication" language when a user sends a communication to the owner's system. See United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993) (stating that the consent exception of § 2511(2)(d) authorizes monitoring of computer system misuse because the owner of the computer system is a party to the communication); United States v. Seidlitz, 589 F.2d 152, 158 (4th Cir. 1978) (concluding in *dicta* that a company that leased and maintained a compromised computer system was "for all intents and purposes a party to the communications" when company employees intercepted intrusions into the system from an unauthorized user using a supervisor's hijacked account). Even accepting this interpretation, however, adhering to it may pose serious practical difficulties. Because hackers often loop from one victim computer through to another, creating a "daisy chain" of systems carrying the traffic, agents have no way of knowing ahead of time which computer will be the ultimate destination for any future communication. If a mere pass-through victim cannot be considered a "party to the communication" -- an issue unaddressed by the courts -- a hacker's decision to loop from one victim to another could change who can consent to monitoring. In that case, agents trying to monitor with the victim's consent would have no way of knowing whether that victim will be a "party to the communication" for any future communication.

c) The Provider Exception, 18 U.S.C. § 2511(2)(a)(i)

Employees or agents of communications service providers may intercept and disclose communications to protect the providers' rights or property. For example, system administrators of computer networks generally may monitor hackers intruding into their networks and then disclose the fruits of monitoring to law enforcement without violating Title III. This privilege belongs to the provider alone, however, and cannot be exercised by law enforcement. Once the provider has communicated with law enforcement, the computer trespasser exception may provide a basis for monitoring by law enforcement.

18 U.S.C. § 2511(2)(a)(i) permits

an operator of a switchboard, or [a]n officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire

communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

The "protection of the rights or property of the provider" clause of § 2511(2)(a)(i) grants providers the right "to intercept and monitor [communications] placed over their facilities in order to combat fraud and theft of service." United States v. Villanueva, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998). For example, employees of a cellular phone company may intercept communications from an illegally "cloned" cell phone in the course of locating its source. See United States v. Pervaz, 118 F.3d 1, 5 (1st Cir. 1997). The exception also permits providers to monitor misuse of a system in order to protect the system from damage, theft, or invasions of privacy. For example, system administrators can track hackers within their networks in order to prevent further damage. Cf. Mullins, 992 F.2d at 1478 (concluding that need to monitor misuse of computer system justified interception of electronic communications pursuant to § 2511(2)(a)(i)).

Importantly, the provider exception of § 2511(2)(a)(i) does not permit providers to conduct unlimited monitoring. See United States v. Auler, 539 F.2d 642, 646 (7th Cir. 1976) ("This authority of the telephone company to intercept and disclose wire communications is not unlimited."). Instead, the exception permits providers and their agents to conduct reasonable monitoring that balances the providers' needs to protect their rights and property with their subscribers' right to privacy in their communications. See United States v. Harvey, 540 F.2d 1345, 1350 (8th Cir. 1976) ("The federal courts . . . have construed the statute to impose a standard of reasonableness upon the investigating communication carrier."). Providers investigating unauthorized use of their systems have broad authority to monitor and then disclose evidence of unauthorized use under § 2511(2)(a)(i), but should attempt to tailor their monitoring and disclosure so as to minimize the interception and disclosure of private communications unrelated to the investigation. See, e.g., United States v. Freeman, 524 F.2d 337, 340 (7th Cir. 1975) (concluding that phone company investigating use of illegal "blue boxes," which were devices designed to steal long-distance service, acted permissibly under § 2511(2)(a)(i) when it intercepted the first two minutes of every conversation obtained by a "blue box," but did not intercept legitimately authorized communications). In particular, there must be a "substantial nexus" between the monitoring and the threat to the provider's rights or property. United States v. McLaren, 957 F. Supp. 215, 219 (M.D. Fla. 1997). Further, although providers legitimately may protect their rights or property by gathering evidence of wrongdoing for criminal prosecution, see United States v. Harvey, 540 F.2d 1345, 1352 (8th Cir. 1976), they cannot use the rights or property exception to gather evidence of crime unrelated to their rights or property. See Bubis v. United States, 384 F.2d 643, 648 (9th Cir. 1967) (interpreting Title III's predecessor statute, 47 U.S.C. § 605, and holding impermissible provider monitoring to convict blue box user of interstate transmission of wagering information).

Agents and prosecutors must resist the urge to use the provider exception to satisfy law enforcement needs. Although the exception permits providers to intercept and disclose communications to law enforcement to protect their rights or property, see Harvey, 540 F.2d at 1352, it does not permit law enforcement officers to direct or ask system administrators to monitor for law enforcement purposes. For example, in McClelland v. McGrath, 31 F. Supp. 2d 616 (N.D. Ill. 1998), police officers investigating a kidnaping traced the kidnaper's calls to an unauthorized "cloned" cellular phone. Eager to learn more about the kidnaper's identity and location, the police asked the cellular provider to intercept the kidnaper's communications and relay any information to the officers that might assist them in locating the kidnaper. The provider agreed, listened to the kidnaper's calls, and then passed on the information to the police, leading to the kidnaper's arrest. Later, the kidnaper sued the officers for intercepting his phone calls, and the officers argued that § 2511(2)(a)(i) authorized the interceptions because the provider could monitor the cloned phone to protect its rights against theft. Although the

court noted that the suit "might seem the very definition of chutzpah," it held that § 2511(2)(a)(i) did not authorize the interception to the extent that the police had directed the provider to monitor for law enforcement purposes unrelated to the provider's rights or property:

What the officers do not seem to understand . . . is that they are not free to ask or direct [the provider] to intercept any phone calls or disclose their contents, at least not without complying with the judicial authorization provisions of the Wiretap Act, regardless of whether [the provider] would have been entitled to intercept those calls on its own initiative.

Id. at 619. Because the purpose of the monitoring appeared to be to locate and identify the kidnaper (a law enforcement interest), rather than to combat telephone fraud (a provider interest), the court refused to grant summary judgment for the officers on the basis of § 2511(2)(a)(i). See id; see also United States v. Savage, 564 F.2d 728, 731 (5th Cir. 1977) (agreeing with district court ruling that a police officer exceeded the provider exception by commandeering a telephone operator's monitoring).

In light of such difficulties, agents and prosecutors should adopt a cautious approach to accepting the fruits of future monitoring conducted by providers under the provider exception. (As discussed below, law enforcement may be able to avoid this problem by reliance on the computer trespasser exception.) Law enforcement agents generally should feel free to accept the fruits of monitoring that a provider collected pursuant to § 2511(2)(a)(i) prior to communicating with law enforcement about the suspected criminal activity. After law enforcement and the provider have communicated with each other, however, law enforcement should only accept the fruits of a provider's monitoring if certain requirements have been met that indicate that the provider is monitoring and disclosing to protect its rights or property. These requirements are: 1) the provider is a victim of the crime and affirmatively wishes both to intercept and to disclose to protect the provider's rights or property, 2) law enforcement verifies that the provider's intercepting and disclosure was motivated by the provider's wish to protect its rights or property, rather than to assist law enforcement, 3) law enforcement has not tasked, directed, requested, or coached the monitoring or disclosure for law enforcement purposes, and 4) law enforcement does not participate in or control the actual monitoring that occurs. Although not required by law, it is highly recommends that agents obtain a written document from the private provider indicating the provider's understanding of its rights and its desire to monitor and disclose to protect its rights or property. Review by a CTC in the relevant district (see Introduction, p. ix) or the Computer Crime and Intellectual Property Section at (202) 514-1026 is also recommended. By following these procedures, agents can greatly reduce the risk that any provider monitoring and disclosure will exceed the acceptable limits of § 2511(2)(a)(i). A sample provider letter appears in Appendix G.

The computer trespasser exception, discussed in subsection (d) below, was created in part to enable law enforcement to avoid the need to rely on prospective monitoring by a provider. It is important for agents and prosecutors to keep in mind that the computer trespasser exception will in certain cases offer a more reliable basis than the provider exception for monitoring an intruder once the provider has communicated with law enforcement.

Law enforcement involvement in provider monitoring of government networks creates special problems. Because the lines of authority often blur, law enforcement agents should exercise extreme care.

The rationale of the provider exception presupposes that a sharp line exists between providers and law enforcement officers. Under this scheme, providers are concerned with protecting their networks from abuse, and law enforcement officers are concerned with investigating crime and prosecuting wrongdoers. This line can seem to break down, however, when the network to be protected belongs to an agency or branch of the government. For example, federal government entities such as NASA, the Postal Service, and the military services have both massive computer networks and considerable law enforcement presences (within both military criminal investigative services and civilian agencies'

Inspectors General offices). Because law enforcement officers and system administrators within the government generally consider themselves to be "on the same team," it is tempting for law enforcement agents to commandeer provider monitoring and justify it under a broad interpretation of the protection of the provider's "rights or property." Although the courts have not addressed the viability of this theory of provider monitoring, such an interpretation, at least in its broadest form, may be difficult to reconcile with some of the cases interpreting the provider exception. See, e.g., McLaren, 957 F. Supp. at 219. CCIPS counsels a cautious approach: agents and prosecutors should assume that the courts interpreting § 2511(2)(a)(i) in the government network context will enforce the same boundary between law enforcement and provider interests that they have enforced in the case of private networks. See, e.g., Savage, 564 F.2d at 731; McClelland, 31 F. Supp. 2d at 619. Accordingly, a high degree of caution is appropriate when law enforcement agents wish to accept the fruits of monitoring under the provider exception from a government provider. Agents and prosecutors may call CCIPS at (202) 514-1026 or the CTC within their district (see Introduction, p. ix) for additional guidance in specific cases.

The "necessary to the rendition of his service" clause of § 2511(2)(a)(i) provides the second context in which the provider exception applies. This language permits providers to intercept, use, or disclose communications in the ordinary course of business when the interception is unavoidable. See United States v. New York Tel. Co., 434 U.S. 159, 168 n.13 (1977) (noting that § 2511(2)(a)(i) "excludes all normal telephone company business practices" from the prohibition of Title III). For example, a switchboard operator may briefly overhear conversations when connecting calls. See, e.g., United States v. Savage, 564 F.2d 728, 731-32 (5th Cir. 1977); Adams v. Sumner, 39 F.3d 933, 935 (9th Cir. 1994). Similarly, repairmen may overhear snippets of conversations when tapping phone lines in the course of repairs. See United States v. Ross, 713 F.2d 389, 392-93 (8th Cir. 1983). Although the "necessary incident to the rendition of his service" language has not been interpreted in the context of electronic communications, these cases suggest that this phrase would likewise permit a system administrator to intercept communications in the course of repairing or maintaining a network.[28]

d) The Computer Trespasser Exception, 18 U.S.C. § 2511(2)(i)

18 U.S.C. § 2511(2)(i) allows victims of computer attacks to authorize law enforcement to intercept wire or electronic communications of a computer trespasser. Law enforcement may intercept the communications of a computer trespasser "transmitted to, through, or from" a protected computer if four requirements are met. First, the owner or operator of the protected computer must authorize the interception of the trespasser's communications. 18 U.S.C. § 2511(2)(i)(I). In general, although not specifically required by statute, it is good practice for investigators to seek written consent for the interception from the computer's owner or a high-level agent of that owner. Second, the person who intercepts the communications must be "lawfully engaged in an investigation." 18 U.S.C. § 2511(2)(i)(II). Third, the person who intercepts the communications must have "reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation." 18 U.S.C. § 2511(2)(i)(III). Fourth, the interception should not acquire any communications other than those transmitted to or from the computer trespasser. 18 U.S.C. § 2511(2)(i)(IV). Thus, investigators may not invoke the computer trespass exception unless they are able to avoid intercepting communications of users who are authorized to use the computer and have not consented to the interception.

Title III defines "computer trespasser" to mean a person who accesses a protected computer without authorization; the definition further excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the protected computer." 18 U.S.C. § 2510(21). Under this definition, customers of a service provider who violate the provider's terms of service are not computer trespassers, as they are merely exceeding the scope of their authorization. Similarly, an employee of a company who violates the computer use policy is not a computer trespasser. Finally, a "protected computer" is defined in 18 U.S.C. § 1030(e)(2) to include any computer used in interstate or foreign commerce or communication, as well as most computers used by the United States government or financial institutions. Thus, almost any computer connected to the Internet will be a "protected computer." Unless extended by Congress, the computer trespasser exception, part of the USA PATRIOT Act of 2001, will sunset December 31, 2005. See PATRIOT Act §§ 217, 224, 115 Stat. 272, 290-91, 295 (2001).

The computer trespasser exception may be used in combination with other authorities, such as the provider exception of § 2511(2)(a)(i). A provider who has monitored its system to protect its rights and property under § 2511(2)(a)(i), and who has subsequently contacted law enforcement to report some criminal activity, may continue to monitor the criminal activity on its system under the direction of law enforcement using the computer trespasser exception. In such circumstances, the provider will then be acting under color of law as an agent of the government.

e) The Extension Telephone Exception, 18 U.S.C. § 2510(5)(a)

According to 18 U.S.C. § 2510(5)(a), Title III is not violated by the use of
any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.[29]

As originally drafted, Congress intended this exception to have a fairly narrow purpose: the exception primarily was designed to permit businesses to monitor by way of an "extension telephone" the performance of their employees who spoke on the phone to customers. The "extension telephone" exception makes clear that when a phone company furnishes an employer with an extension telephone for a legitimate work-related purpose, the employer's monitoring of employees using the extension phone for legitimate work-related purposes does not violate Title III. See Briggs v. American Air Filter Co., 630 F.2d 414, 418 (5th Cir. 1980) (reviewing legislative history of Title III); Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983) (applying exception to permit monitoring of sales representatives); James v. Newspaper Agency Corp. 591 F.2d 579, 581 (10th Cir. 1979) (applying exception to permit monitoring of newspaper employees' conversations with customers).

The case law interpreting the extension telephone exception is notably erratic, largely owing to the ambiguity of the phrase "ordinary course of business." Some courts have interpreted "ordinary course of business" broadly to mean "within the scope of a person's legitimate concern," and have applied the extension telephone exception to contexts such as intra-family disputes. See, e.g., Simpson v. Simpson, 490 F.2d 803, 809 (5th Cir. 1974) (holding that husband did not violate Title III by recording wife's phone calls); Anonymous v. Anonymous, 558 F.2d 677, 678-79 (2d Cir. 1977) (holding that husband did not violate Title III in recording wife's conversations with their daughter in his custody). Other courts have rejected this broad reading, and have implicitly or explicitly excluded surreptitious activity from conduct within the "ordinary course of business." See Kempf v. Kempf, 868 F.2d 970, 973 (8th Cir. 1989) (holding that Title III prohibits all wiretapping activities unless specifically excepted, and that there is no express exception for interspousal wiretapping); United States v. Harpel, 493 F.2d 346, 351 (10th Cir. 1974) ("We hold as a matter of law that a telephone extension used without authorization or consent to surreptitiously record a private telephone conversation is not used in the ordinary course of business."); Pritchard v. Pritchard, 732 F.2d 372, 374 (4th Cir. 1984) (rejecting view that § 2510(5)(a) exempts interspousal wiretapping from Title III liability). Some of the courts that have embraced the narrower construction of the extension telephone exception have stressed that it permits only limited work-related monitoring by employers. See, e.g., Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992) (holding that employer monitoring of employee was not authorized by the extension telephone exception in part because the scope of the interception was broader than that normally required in the ordinary course of business).

The exception in 18 U.S.C. § 2510(5)(a)(ii) that permits the use of "any telephone or telegraph instrument, equipment or facility, or any component thereof" by "an investigative or law enforcement officer in the ordinary course of his duties" is a common source of confusion. This language does not permit agents to intercept private communications on the theory that a law enforcement agent may need to intercept communications "in the ordinary course of his duties." As Chief Judge Posner has explained:

> Investigation is within the ordinary course of law enforcement, so if 'ordinary' were read literally warrants would rarely if ever be required for electronic eavesdropping, which was surely not Congress's intent. Since the purpose of the statute was primarily to regulate the use of wiretapping and other electronic surveillance for investigatory purposes, "ordinary" should not be read so broadly; it is more reasonably interpreted to refer to routine noninvestigative recording of telephone conversations. . . . Such recording will rarely be very invasive of privacy, and for a reason that does after all bring the ordinary-course exclusion rather close to the consent exclusion: what is ordinary is apt to be known; it imports implicit notice.

Amati v. City of Woodstock, 176 F.3d 952, 955 (7th Cir. 1999). For example, routine taping of all telephone calls made to and from a police station may fall within this law enforcement exception, but nonroutine taping designed to target a particular suspect ordinarily would not. See id.; accord United

States v. Hammond, 286 F.3d 189, 192 (4th Cir. 2002) (concluding that routine recording of calls made from prison fall within law enforcement exception); United States v. Van Poyck, 77 F.3d 285, 292 (9th Cir. 1996) (same).

f) The 'Inadvertently Obtained Criminal Evidence' Exception, 18 U.S.C. § 2511(3)(b)(iv)

18 U.S.C. § 2511(3)(b) lists several narrow contexts in which a provider of electronic communication service to the public can divulge the contents of communications. The most important of these exceptions permits a public provider to divulge the contents of any communications that were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.
18 U.S.C. § 2511(3)(b)(iv). Although this exception has not yet been applied by the courts in any published cases involving computers, its language appears to permit providers to report criminal conduct (e.g., child pornography or evidence of a fraud scheme) in certain circumstances without violating Title III. Cf. 18 U.S.C. § 2702(b)(6)(A) (creating an analogous rule for stored communications).

g) The 'Accessible to the Public' Exception, 18 U.S.C. § 2511(2)(g)(i)

18 U.S.C. § 2511(2)(g)(i) permits "any person" to intercept an electronic communication made through a system "that is configured so that . . . [the] communication is readily accessible to the general public." Although this exception has not yet been applied by the courts in any published cases involving computers, its language appears to permit the interception of an electronic communication that has been posted to a public bulletin board, a public chat room, or a Usenet newsgroup. See S. Rep. No. 99-541, at 36 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3590 (discussing bulletin boards).

E. Remedies For Violations of Title III and the Pen/Trap Statute

Agents and prosecutors must adhere strictly to the dictates of Title III and the Pen/Trap statute when planning electronic surveillance, as violations can result in civil penalties, criminal penalties, and suppression of the evidence obtained. See 18 U.S.C. § 2511(4) (criminal penalties for Title III violations); 18 U.S.C. § 2520 (civil damages for Title III violation); 18 U.S.C. § 3121(d) (criminal penalties for pen/trap violations); 18 U.S.C. § 2518(10)(a) (suppression for certain Title III violations). As a practical matter, however, courts may conclude that the electronic surveillance statutes were violated even after agents and prosecutors have acted in good faith and with full regard for the law. For example, a private citizen may sometimes wiretap his neighbor and later turn over the evidence to the police, or agents may intercept communications using a court order that the agents later learn is defective. Similarly, a court may construe an ambiguous portion of Title III differently than did the investigators, leading the court to find that a violation of Title III occurred. In these circumstances, prosecutors and agents must understand not only what conduct the surveillance statutes prohibit, but also what the ramifications might be if a court finds that the statutes have been violated.

1. Suppression Remedies

Title III provides for statutory suppression of wrongfully intercepted oral and wire communications, but not electronic communications. The Pen/Trap statute does not provide a statutory suppression remedy. Constitutional violations may result in suppression of the evidence wrongfully obtained.

a) Statutory Suppression Remedies

i) General: Interception of Wire Communications Only

The statutes that govern electronic surveillance grant statutory suppression remedies to defendants only in a specific set of cases. In particular, a defendant may only move for suppression on statutory grounds when the defendant was a party to an oral or wire communication that was intercepted in violation of Title III. See 18 U.S.C. §§ 2510(11), 2518(10)(a). See also United States v. Giordano, 416 U.S. 505, 524 (1974) (stating that "[w]hat disclosures are forbidden [under § 2515], and are subject to motions to suppress, is . . . governed by § 2518(10)(a)"); United States v. Williams, 124 F.3d 411, 426 (3d Cir. 1997). Section 2518(10)(a) states:

[A]ny aggrieved person . . . may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that--
(i) the communication was unlawfully intercepted;
(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
(iii) the interception was not made in conformity with the order of authorization or approval.

18 U.S.C. § 2518(10)(a). Notably, Title III does not provide a statutory suppression remedy for unlawful interceptions of electronic communications. See Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 461 n.6 (5th Cir. 1994); United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990). Similarly, the Pen/Trap statute does not provide a statutory suppression remedy for violations. See United States v. Fregoso, 60 F.3d 1314, 1320-21 (8th Cir. 1995); United States v. Thompson, 936 F.2d 1249, 1249-50 (11th Cir. 1991).

ii) Unauthorized Parties

The language of Title III appears to offer a suppression remedy to any party to an unlawfully intercepted wire communication, regardless of whether the party was authorized or unauthorized to use the communication system. See 18 U.S.C. § 2510(11) (defining an "aggrieved person" who may move to suppress under § 2518(10)(a) as "a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed"). Despite this broad definition, it is unclear whether a computer hacker could move for suppression of evidence that recorded the hacker's unauthorized activity within the victim's computer network. The one court that has evaluated this question expressed serious doubts. See United States v. Seidlitz, 589 F.2d 152, 160 (4th Cir. 1978) (stating in *dicta* that "we seriously doubt that [a hacker whose communications were monitored by the system administrator of a victim network] is entitled to raise . . . objections to the evidence [under Title III]").

The Fourth Circuit's suggestion in Seidlitz is consistent with other decisions interpreting the definition of "aggrieved person" in 18 U.S.C. § 2510(11). Relying on the legislative history of Title III, the Supreme Court has stressed that Title III's suppression remedy was not intended "generally to press the scope of the suppression role beyond present search and seizure law." Scott v. United States, 436 U.S. 128, 139 (1978) (quoting S. Rep. No. 90-1097, at 96 (1968), and citing Alderman v. United States, 394

U.S. 165, 175-76 (1969)). If monitoring does not violate a suspect's reasonable expectation of privacy under the Fourth Amendment, the cases suggest, the suspect cannot be an "aggrieved" person who can move for suppression under Title III. See United States v. King, 478 F.2d 494, 506 (9th Cir. 1973) ("[A] defendant may move to suppress the fruits of a wire-tap [under Title III] only if his privacy was actually invaded."); United States v. Baranek, 903 F.2d 1068, 1072 (6th Cir. 1990) ("[We] do not accept defendant's contention that fourth amendment law is not involved in the resolution of Title III suppression issues . . . . Where, as here, we have a case with a factual situation clearly not contemplated by the statute, we find it helpful on the suppression issue . . . to look to fourth amendment law."). Because monitoring a hacker's attack ordinarily does not violate the hacker's reasonable expectation of privacy, see "Constitutional Suppression Remedies," infra, it is unclear whether a hacker can be an "aggrieved person" entitled to move for suppression of such monitoring under § 2518(10)(a). No court has addressed this question directly. Of course, civil and criminal penalties for unlawful monitoring continue to exist, even if the unlawful monitoring itself targets unauthorized use. See, e.g., McClelland v. McGrath, 31 F. Supp. 616 (N.D. Ill. 1998) (declining to dismiss civil suit brought by a kidnaper against police officers for unlawful monitoring of the kidnaper's unauthorized use of a cloned cellular phone).

iii) Suppression Following Interception with a Defective Title III Order

Under § 2518(10)(a), the courts generally will suppress evidence resulting from any unlawful interception of an aggrieved party's wire communication that takes place without a court order. However, when investigators procure a Title III order that later turns out to be defective, the courts will suppress the evidence obtained with the order only if the defective order "fail[ed] to satisfy any of those statutory requirements that directly and substantially implement the congressional intention [in enacting Title III] to limit the use of intercept procedures to those situations clearly calling for the employment of this extraordinary investigative device." United States v. Giordano, 416 U.S. 505, 527 (1974).

This standard requires the courts to distinguish technical defects from substantive ones. If the defect in the Title III order concerns only technical aspects of Title III, the fruits of the interception will not be suppressed. In contrast, courts will suppress the evidence if the defect reflects a failure to comply with a significant requirement of Title III. Compare Giordano, 416 U.S. at 527-28 (holding that failure to receive authorization from Justice Department official listed in § 2516(1) for order authorizing interception of wire communications requires suppression in light of importance of such authorization to statutory scheme) with United States v. Moore, 41 F.3d 370, 376-77 (8th Cir. 1994) (applying good faith exception of United States v. Leon, 468 U.S. 897 (1984), to challenge of Title III order and reversing district court's suppression order on ground that judge's failure to sign the Title III order in the correct place was merely a technical defect). Defects that directly implicate constitutional concerns such as probable cause and particularity, see Berger v. New York, 388 U.S. 41, 58-60 (1967), will generally be considered substantive defects that require suppression. See United States v. Ford, 553 F.2d 146, 173 (D.C. Cir. 1977).

iv) The "Clean Hands" Exception in the Sixth Circuit

18 U.S.C. § 2518(10)(a)(i) states that an aggrieved person may move to suppress the contents of wire communications when "the communication was unlawfully intercepted." The language of this statute is susceptible to the interpretation that the government cannot use the fruits of an illegally intercepted wire communication as evidence in court, even if the government itself did not intercept the communication. Under this reading, if a private citizen wiretaps another private citizen and then hands over the results to the government, the government could not use the evidence in court. See United States v. Vest, 813 F.2d 477, 481 (1st Cir. 1987).

The Sixth Circuit, however, has fashioned a "clean hands" exception that permits the government to use any illegally intercepted communication so long as the government "played no part in the unlawful interception." United States v. Murdock, 63 F.3d 1391, 1404 (6th Cir. 1995). In Murdock, the defendant's wife had surreptitiously recorded her estranged husband's phone conversations at their family-run funeral home. When she later listened to the recordings, she heard evidence that her husband had accepted a $90,000 bribe to award a government contract to a local dairy while serving as president of the Detroit School Board. Mrs. Murdock sent an anonymous copy of the recording to a competing bidder for the contract, who offered the copy to law enforcement. The government then brought tax evasion charges against Mr. Murdock on the theory that Mr. Murdock had not reported the $90,000 bribe as taxable income.

Following a trial in which the recording was admitted in evidence against him, the jury convicted Mr. Murdock, and he appealed. The Sixth Circuit affirmed, ruling that although Mrs. Murdock had violated Title III by recording her husband's phone calls, this violation did not bar the admission of the recordings in a subsequent criminal trial. The court reasoned that Mrs. Murdock's illegal interception could be analogized to a Fourth Amendment private search, and concluded that Title III did not preclude the government "from using evidence that literally falls into its hands" because it would have no deterrent effect on the government's conduct. Id. at 1403.

Since the Sixth Circuit decided Murdock, three circuits have rejected the "clean hands" exception, and instead have embraced the First Circuit's Vest rule that the government cannot use the fruits of unlawful interception even if the government was not involved in the initial interception. See Berry v. Funk, 146 F.3d 1003, 1013 (D.C. Cir. 1998) (dicta); Chandler v. United States Army, 125 F.3d 1296, 1302 (9th Cir. 1997); In re Grand Jury, 111 F.3d 1066, 1077-78 (3d Cir. 1997). The remaining circuits have not addressed whether they will recognize a "clean hands" exception to Title III.

b) Constitutional Suppression Remedies

Defendants may move to suppress evidence from electronic surveillance of communications networks on either statutory or Fourth Amendment constitutional grounds. Although Fourth Amendment violations generally lead to suppression of evidence, see Mapp v. Ohio, 367 U.S. 643, 655 (1961), defendants move to suppress the fruits of electronic surveillance on constitutional grounds only rarely. This is true for two related reasons. First, Congress's statutory suppression remedies tend to be as broad or broader in scope than their constitutional counterparts. See, e.g., Chandler, 125 F.3d at 1298; Ford, 553 F.2d at 173. Cf. United States v. Torres, 751 F.2d 875, 884 (7th Cir. 1984) (noting that Title III is a "carefully thought out, and constitutionally valid . . . effort to implement the requirements of the Fourth Amendment."). Second, electronic surveillance statutes often regulate government access to evidence that is not protected by the Fourth Amendment. See United States v. Hall, 488 F.2d 193, 198 (9th Cir. 1973) ("Every electronic surveillance is not constitutionally proscribed and whether the interception is to be suppressed must turn upon the facts of each case."). For example, the Supreme Court has held that the use and installation of pen registers does not constitute a Fourth Amendment "search." See Smith v. Maryland, 442 U.S. 735, 742 (1979). As a result, use of a pen/trap device in violation of the pen/trap statute ordinarily does not lead to suppression of evidence on Fourth Amendment grounds. See United States v. Thompson, 936 F.2d 1249, 1251 (11th Cir. 1991).

It is likely that a hacker would not enjoy a constitutional entitlement under the Fourth Amendment to suppression of unlawful monitoring of his unauthorized activity. As the Fourth Circuit noted in Seidlitz, a computer hacker who breaks into a victim computer "intrude[s] or trespasse[s] upon the physical property of [the victim] as effectively as if he had broken into the . . . facility and instructed the

computers from one of the terminals directly wired to the machines." Seidlitz, 589 F.2d at 160. See also Compuserve, Inc. v. Cyber Promotions, Inc. 962 F. Supp. 1015, 1021 (S.D. Ohio 1997) (noting cases analogizing computer hacking to trespassing). A trespasser does not have a reasonable expectation of privacy where his presence is unlawful. See Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (noting that "[a] burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as 'legitimate'"); Amezquita v. Colon, 518 F.2d 8, 11 (1st Cir. 1975) (holding that squatters had no reasonable expectation of privacy on government land where the squatters had no colorable claim to occupy the land). Accordingly, a computer hacker would have no reasonable expectation of privacy in his unauthorized activities that were monitored from within a victim computer. "[H]aving been 'caught with his hand in the cookie jar'," the hacker has no constitutional right to the suppression of evidence of his unauthorized activities. Seidlitz, 589 F.2d at 160.

2. Defenses to Civil and Criminal Actions

Agents and prosecutors are generally protected from liability under Title III for reasonable decisions made in good faith in the course of their official duties.

Civil and criminal actions may result when law enforcement officers violate the electronic surveillance statutes. In general, the law permits such actions when law enforcement officers abuse their authority, but protects officers from suit for reasonable good-faith mistakes made in the course of their official duties. The basic approach was articulated over a half century ago by Judge Learned Hand:

There must indeed be means of punishing public officers who have been truant to their duties; but that is quite another matter from exposing such as have been honestly mistaken to suit by anyone who has suffered from their errors. As is so often the case, the answer must be found in a balance between the evils inevitable in either alternative.

Gregoire v. Biddle, 177 F.2d 579, 580 (2d Cir. 1949). When agents and prosecutors are subject to civil or criminal suits for electronic surveillance, the balance of evils has been struck by both a statutory good-faith defense and a widely (but not uniformly) recognized judge-made qualified-immunity defense.

a) Good-Faith Defense

Both Title III and the Pen/Trap statute offer a statutory good-faith defense. According to these statutes, a good faith reliance on . . . a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization . . . is a complete defense against any civil or criminal action brought under this chapter or any other law.
18 U.S.C. § 2520(d) (good-faith defense for Title III violations). See also 18 U.S.C. § 3124(e) (good-faith defense for pen/trap violations).
The relatively few cases interpreting the good-faith defense are notably erratic. In general, however, the courts have permitted law enforcement officers to rely on the good-faith defense when they make honest mistakes in the course of their official duties. See, e.g., Kilgore v. Mitchell, 623 F.2d 631, 633 (9th Cir. 1980) ("Officials charged with violation of Title III may invoke the defense of good faith under § 2520 if they can demonstrate: (1) that they had a subjective good faith belief that they were acting in compliance with the statute; and (2) that this belief was itself reasonable."); Hallinan v. Mitchell, 418 F. Supp. 1056, 1057 (N.D. Cal. 1976) (good-faith exception protects Attorney General from civil suit after Supreme Court rejects Attorney General's interpretation of Title III). In contrast, the courts have not permitted private parties to rely on good-faith "mistake of law" defenses in civil wiretapping cases. See, e. g., Williams v. Poulos, 11 F.3d 271, 285 (1st Cir. 1993); Heggy v. Heggy, 944 F.2d 1537, 1541-42 (10th Cir. 1991).

b) Qualified Immunity

The courts have generally recognized a qualified immunity defense to Title III civil suits in addition to the statutory good-faith defense. See Tapley v. Collins, 211 F.3d 1210, 1216 (11th Cir. 2000) (holding that public officials sued under Title III may invoke qualified immunity in addition to the good faith defense); Blake v. Wright, 179 F.3d 1003, 1013 (6th Cir. 1999) (holding that qualified immunity protects police chief from suit by employees who were monitored where "the dearth of law surrounding the . . . statute fails to clearly establish whether [the defendant's] activities violated the law."); Davis v. Zirkelbach, 149 F.3d 614, 618, 620 (7th Cir. 1998) (qualified immunity defense applies to police officers and prosecutors in civil wiretapping case); Zweibon v. Mitchell, 720 F.2d 162 (D.C. Cir. 1983). But see Berry v. Funk, 146 F.3d 1003, 1013-14 (D.C. Cir. 1998) (distinguishing Zweibon, and concluding that qualified immunity does not apply to Title III violations because the statutory good-faith defense exists).
Under the doctrine of qualified immunity,

> government officials performing discretionary functions generally are shielded from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.

Harlow v. Fitzgerald, 457 U.S. 800, 818 (1982). In general, qualified immunity protects government officials from suit when "[t]he contours of the right" violated were not so clear that a reasonable official would understand that his conduct violated the law. Anderson v. Creighton, 483 U.S. 635, 640 (1987); Burns v. Reed, 500 U.S. 478, 496 (1991) (prosecutors receive qualified immunity for legal advice to police).
Of course, whether a statutory right under Title III is "clearly established" for purposes of qualified immunity is in the eye of the beholder. The sensitive privacy interests implicated by Title III may lead some courts to rule that a Title III privacy right is "clearly established" even if no courts have recognized

the right in analogous circumstances. See, e.g., McClelland v. McGrath, 31 F. Supp. 2d 616, 619-20 (N.D. Ill. 1998) (holding that police violated the "clearly established" rights of a kidnaper who used a cloned cellular phone when the police asked the cellular provider to intercept the kidnaper's unauthorized communications to help locate the kidnaper, and adding that the kidnaper's right to be free from monitoring was "crystal clear" despite § 2511(2)(a)(i)).

V. EVIDENCE

A. Introduction

Although the primary concern of this manual is obtaining computer records in criminal investigations, the ultimate goal is to obtain evidence admissible in court. A complete guide to offering computer records in evidence is beyond the scope of this manual. However, this chapter explains some of the more important issues that can arise when the government seeks the admission of computer records under the Federal Rules of Evidence.

Most federal courts that have evaluated the admissibility of computer records have focused on computer records as potential hearsay. The courts generally have admitted computer records upon a showing that the records fall within the business records exception, Fed. R. Evid. 803(6):

Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

See, e.g., United States v. Salgado, 250 F.3d 438, 452 (6th Cir. 2001); United States v. Cestnik, 36 F.3d 904, 909-10 (10th Cir. 1994); United States v. Goodchild, 25 F.3d 55, 61-62 (1st Cir. 1994); United States v. Moore, 923 F.2d 910, 914 (1st Cir. 1991); United States v. Briscoe, 896 F.2d 1476, 1494 (7th Cir. 1990); United States v. Catabran, 836 F.2d 453, 457 (9th Cir. 1988). Applying this test, the courts have indicated that computer records generally can be admitted as business records if they were kept pursuant to a routine procedure for motives that tend to assure their accuracy.

However, the federal courts are likely to move away from this "one size fits all" approach as they become more comfortable and familiar with computer records. Like paper records, computer records are not monolithic: the evidentiary issues raised by their admission should depend on what kind of computer records a proponent seeks to have admitted. For example, computer records that contain text often can

be divided into two categories: computer-generated records, and records that are merely computer-stored. See People v. Holowko, 486 N.E.2d 877, 878-79 (Ill. 1985). The difference hinges upon whether a person or a machine created the records' contents. Computer-stored records refer to documents that contain the writings of some person or persons and happen to be in electronic form. E-mail messages, word processing files, and Internet chat room messages provide common examples. As with any other testimony or documentary evidence containing human statements, computer-stored records must comply with the hearsay rule. If the records are admitted to prove the truth of the matter they assert, the offeror of the records must show circumstances indicating that the human statements contained in the record are reliable and trustworthy, see Advisory Committee Notes to Proposed Rule 801 (1972), and the records must be authentic.

In contrast, computer-generated records contain the output of computer programs, untouched by human hands. Log-in records from Internet service providers, telephone records, and ATM receipts tend to be computer-generated records. Unlike computer-stored records, computer-generated records do not contain human "statements," but only the output of a computer program designed to process input following a defined algorithm. Of course, a computer program can direct a computer to generate a record that mimics a human statement: an e-mail program can announce "You've got mail!" when mail arrives in an inbox, and an ATM receipt can state that $100 was deposited in an account at 2:25 pm. However, the fact that a computer rather than a human being has created the record alters the evidentiary issues that the computer-generated records present. See, e.g., 2 J. Strong, McCormick on Evidence § 294, at 286 (4th ed. 1992). The evidentiary issue is no longer whether a human's out-of-court statement was truthful and accurate (a question of hearsay), but instead whether the computer program that generated the record was functioning properly (a question of authenticity). See id.; Richard O. Lempert & Steven A. Saltzburg, A Modern Approach to Evidence 370 (2d ed. 1983); Holowko, 486 N.E.2d at 878-79.

Finally, a third category of computer records exists: some computer records are both computer-generated *and* computer-stored. For example, a suspect in a fraud case might use a spreadsheet program to process financial figures relating to the fraudulent scheme. A computer record containing the output of the program would derive from both human statements (the suspect's input to the spreadsheet program) and computer processing (the mathematical operations of the spreadsheet program). Accordingly, the record combines the evidentiary concerns raised by computer-stored and computer-generated records. The party seeking the admission of the record should address both the hearsay issues implicated by the original input and the authenticity issues raised by the computer processing.

As the federal courts develop a more nuanced appreciation of the distinctions to be made between different kinds of computer records, they are likely to see that the admission of computer records generally raises two distinct issues. First, the government must establish the authenticity of all computer records by providing "evidence sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). Second, if the computer records are computer-stored records that contain human statements, the government must show that those human statements are not inadmissible hearsay.

B. Authentication

Before a party may move for admission of a computer record or any other evidence, the proponent must show that it is authentic. That is, the government must offer evidence "sufficient to support a finding that the [computer record or other evidence] in question is what its proponent claims." Fed. R. Evid. 901(a). See United States v. Simpson, 152 F.3d 1241, 1250 (10th Cir. 1998).

The standard for authenticating computer records is the same for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form. See United States v. Vela, 673 F.2d 86, 90 (5th Cir. 1982); United States v. DeGeorgia, 420 F.2d 889, 893 n.11 (9th Cir. 1969). But see United States v. Scholle, 553 F.2d 1109, 1125 (8th Cir. 1977) (stating in dicta that "the complex nature of computer storage calls for a more comprehensive foundation"). For example, witnesses who testify to the authenticity of computer records need not have special qualifications. The witness does not need to have programmed the computer himself, or even need to understand the maintenance and technical operation of the computer. See United States v. Salgado, 250 F.3d 438, 453 (6th Cir. 2001) (stating that "it is not necessary that the computer programmer testify in order to authenticate computer-generated records"); United States v. Moore, 923 F.2d 910, 915 (1st Cir. 1991) (citing cases). Instead, the witness simply must have first-hand knowledge of the relevant facts to which she testifies. See generally United States v. Whitaker, 127 F.3d 595, 601 (7th Cir. 1997) (FBI agent who was present when the defendant's computer was seized can authenticate seized files) ; United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (telephone company billing supervisor can authenticate phone company records); Moore, 923 F.2d at 915 (head of bank's consumer loan department can authenticate computerized loan data).

Challenges to the authenticity of computer records often take on one of three forms. First, parties may challenge the authenticity of both computer-generated and computer-stored records by questioning whether the records were altered, manipulated, or damaged after they were created. Second, parties may question the authenticity of computer-generated records by challenging the reliability of the computer program that generated the records. Third, parties may challenge the authenticity of computer-stored records by questioning the identity of their author.

1. Authenticity and the Alteration of Computer Records

Computer records can be altered easily, and opposing parties often allege that computer records lack authenticity because they have been tampered with or changed after they were created. For example, in United States v. Whitaker, 127 F.3d 595, 602 (7th Cir. 1997), the government retrieved computer files from the computer of a narcotics dealer named Frost. The files from Frost's computer included detailed records of narcotics sales by three aliases: "Me" (Frost himself, presumably), "Gator" (the nickname of Frost's co-defendant Whitaker), and "Cruz" (the nickname of another dealer). After the government permitted Frost to help retrieve the evidence from his computer and declined to establish a formal chain of custody for the computer at trial, Whitaker argued that the files implicating him through his alias were not properly authenticated. Whitaker argued that "with a few rapid keystrokes, Frost could have easily added Whitaker's alias, 'Gator' to the printouts in order to finger Whitaker and to appear more helpful to the government." Id.

The courts have responded with considerable skepticism to such unsupported claims that computer records have been altered. Absent specific evidence that tampering occurred, the mere possibility of tampering does not affect the authenticity of a computer record. See Whitaker, 127 F.3d at 602 (declining to disturb trial judge's ruling that computer records were admissible because allegation of

tampering was "almost wild-eyed speculation . . . [without] evidence to support such a scenario"); United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness."); United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985) ("The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party opposing admission would have to show only that a better security system was feasible."). This is consistent with the rule used to establish the authenticity of other evidence such as narcotics. See United States v. Allen, 106 F.3d 695, 700 (6th Cir. 1997) ("Merely raising the possibility of tampering is insufficient to render evidence inadmissible."). Absent specific evidence of tampering, allegations that computer records have been altered go to their weight, not their admissibility. See Bonallo, 858 F.2d at 1436.

2. Establishing the Reliability of Computer Programs

The authenticity of computer-generated records sometimes implicates the reliability of the computer programs that create the records. For example, a computer-generated record might not be authentic if the program that creates the record contains serious programming errors. If the program's output is inaccurate, the record may not be "what its proponent claims" according to Fed. R. Evid. 901. Defendants in criminal trials often attempt to challenge the authenticity of computer -generated records by challenging the reliability of the programs. See, e.g., United States v. Salgado, 250 F.3d 438, 452-53 (6th Cir. 2001); United States v. Liebert, 519 F.2d 542, 547-48 (3d Cir. 1975). The courts have indicated that the government can overcome this challenge so long as
the government provides sufficient facts to warrant a finding that the records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof[.]
United States v. Briscoe, 896 F.2d 1476, 1494-95 (7th Cir. 1990). See also United States v. Oshatz, 912 F.2d 534, 543 (2d Cir. 1990) (stating that defense should have sufficient time to check the validity of a program and cross-examine government experts regarding error in calculations); Liebert, 519 F.2d at 547; DeGeorgia, 420 F.2d. at 893 n.11. Cf. Fed. R. Evid. 901(b)(9) (indicating that matters created according to a process or system can be authenticated with "[e]vidence describing a process or system used . . . and showing that the process or system produces an accurate result"). In most cases, the reliability of a computer program can be established by showing that users of the program actually do rely on it on a regular basis, such as in the ordinary course of business. See, e.g., Salgado, 250 F.3d at 453 (holding that "evidence that the computer was sufficiently accurate that the company relied upon it in conducting its business" was sufficient for establishing trustworthiness); United States v. Moore, 923 F.2d 910, 915 (1st Cir. 1991) ("[T]he ordinary business circumstances described suggest trustworthiness, . . . at least where absolutely nothing in the record in any way implies the lack thereof.") (computerized tax records held by the I.R.S.); Briscoe, 896 F.2d at 1494 (computerized telephone records held by Illinois Bell). When the computer program is not used on a regular basis and the government cannot establish reliability based on reliance in the ordinary course of business, the government may need to disclose "what operations the computer had been instructed to perform [as well as] the precise instruction that had been given" if the opposing party requests. United States v. Dioguardi, 428 F.2d 1033, 1038 (C.A.N.Y. 1970). Notably, once a minimum standard of trustworthiness has been established, questions as to the accuracy of computer records "resulting from . . . the operation of the computer program" affect only the weight of the evidence, not its admissibility. United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988).

Prosecutors may note the conceptual overlap between establishing the authenticity of a computer-generated record and establishing the trustworthiness of a computer record for the business record exception to the hearsay rule. In fact, federal courts that evaluate the authenticity of computer-generated records often assume that the records contain hearsay, and then apply the business records exception. See, e.g., Salgado, 250 F.3d at 452-53 (applying business records exception to telephone records generated "automatically" by a computer) United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989) (same); United States v. Vela, 673 F.2d 86, 89-90 (5th Cir. 1982) (same). As discussed later in this chapter, this analysis is technically incorrect in many cases: computer records generated entirely by computers cannot contain hearsay and cannot qualify for the business records exception because they do not contain human "statements." See Chapter 5.C, infra. As a practical matter, however, prosecutors who lay a foundation to establish a computer-generated record as a business record will also lay the foundation to establish the record's authenticity. Evidence that a computer program is sufficiently trustworthy so that its results qualify as business records according to Fed. R. Evid. 803(6) also establishes the authenticity of the record. Cf. United States v. Saputski, 496 F.2d 140, 142 (9th Cir. 1974).

3. Identifying the Author of Computer-Stored Records

Although handwritten records may be penned in a distinctive handwriting style, computer-stored records consist of a long string of zeros and ones that do not necessarily identify their author. This is a particular problem with Internet communications, which offer their authors an unusual degree of anonymity. For example, Internet technologies permit users to send effectively anonymous e-mails, and Internet Relay Chat channels permit users to communicate without disclosing their real names. When prosecutors seek the admission of such computer-stored records against a defendant, the defendant may challenge the authenticity of the record by challenging the identity of its author.

Circumstantial evidence generally provides the key to establishing the authorship and authenticity of a computer record. For example, in United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998), prosecutors sought to show that the defendant had conversed with an undercover FBI agent in an Internet chat room devoted to child pornography. The government offered a printout of an Internet chat conversation between the agent and an individual identified as "Stavron," and sought to show that "Stavron" was the defendant. The district court admitted the printout in evidence at trial. On appeal following his conviction, Simpson argued that "because the government could not identify that the statements attributed to [him] were in his handwriting, his writing style, or his voice," the printout had not been authenticated and should have been excluded. Id. at 1249.

The Tenth Circuit rejected this argument, noting the considerable circumstantial evidence that "Stavron" was the defendant. See id. at 1250. For example, "Stavron" had told the undercover agent that his real name was "B. Simpson," gave a home address that matched Simpson's, and appeared to be accessing the Internet from an account registered to Simpson. Further, the police found records in Simpson's home that listed the name, address, and phone number that the undercover agent had sent to "Stavron." Accordingly, the government had provided evidence sufficient to support a finding that the defendant was "Stavron," and the printout was properly authenticated. See id. at 1250; see also United States v. Tank, 200 F.3d 627, 630-31 (9th Cir. 2000) (concluding that district court properly admitted chat room log printouts in circumstances similar to those in Simpson); United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (holding that e-mail messages were properly authenticated where messages included defendant's e-mail address, defendant's nickname, and where defendant followed up messages with phone calls). But see United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (concluding that

web postings purporting to be statements made by white supremacist groups were properly excluded on authentication grounds absent evidence that the postings were actually posted by the groups); St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999) (holding that evidence from a webpage could not be authenticated, since information from the Internet is "inherently untrustworthy").

C. Hearsay

Federal courts have often assumed that all computer records contain hearsay. A more nuanced view suggests that in fact only a portion of computer records contain hearsay. When a computer record contains the assertions of a person, whether or not processed by a computer, and is offered to prove the truth of the matter asserted, the record can contain hearsay. In such cases, the government must fit the record within a hearsay exception such as the business records exception, Fed. R. Evid. 803(6). When a computer record contains only computer-generated data untouched by human hands, however, the record cannot contain hearsay. In such cases, the government must establish the authenticity of the record, but does not need to establish that a hearsay exception applies for the records to be admissible in court.

1. Inapplicability of the Hearsay Rules to Computer-Generated Records

The hearsay rules exist to prevent unreliable out-of-court statements by human declarants from improperly influencing the outcomes of trials. Because people can misinterpret or misrepresent their experiences, the hearsay rules express a strong preference for testing human assertions in court, where the declarant can be placed on the stand and subjected to cross-examination. See Ohio v. Roberts, 448 U.S. 56, 62-66 (1980). This rationale does not apply when an animal or a machine makes an assertion: beeping machines and barking dogs cannot be called to the witness stand for cross-examination at trial. The Federal Rules have adopted this logic. By definition, an assertion cannot contain hearsay if it was not made by a human person. See Fed. R. Evid. 801(a) ("A 'statement' is (1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion.") (emphasis added) ; Fed. R. Evid. 801(b) ("A declarant is a person who makes a statement.") (emphasis added).
As several courts and commentators have noted, this limitation on the hearsay rules necessarily means that computer-generated records untouched by human hands cannot contain hearsay. One state supreme court articulated the distinction in an early case involving the use of automated telephone records:
The printout of the results of the computer's internal operations is not hearsay evidence. It does not represent the output of statements placed into the computer by out of court declarants. Nor can we say that this printout itself is a "statement" constituting hearsay evidence. The underlying rationale of the hearsay rule is that such statements are made without an oath and their truth cannot be tested by cross-examination. Of concern is the possibility that a witness may consciously or unconsciously misrepresent what the declarant told him or that the declarant may consciously or unconsciously misrepresent a fact or occurrence. With a machine, however, there is no possibility of a conscious misrepresentation, and the possibility of inaccurate or misleading data only materializes if the machine is not functioning properly.
State v. Armstead, 432 So.2d 837, 840 (La. 1983). See also People v. Holowko, 486 N.E.2d 877, 878-79 (Ill. 1985) (automated trap and trace records); United States v. Duncan, 30 M.J. 1284, 1287-89 (N-

M.C.M.R. 1990) (computerized records of ATM transactions); 2 J. Strong, McCormick on Evidence § 294, at 286 (4th ed.1992); Richard O. Lempert & Stephen A. Saltzburg, A Modern Approach to Evidence 370 (2d ed. 1983). Cf. United States v. Fernandez-Roque, 703 F.2d 808, 812 n.2 (5th Cir. 1983) (rejecting hearsay objection to admission of automated telephone records because "the fact that these calls occurred is not a hearsay statement"). Accordingly, a properly authenticated computer-generated record is admissible. See Lempert & Saltzburg, at 370.

The insight that computer-generated records cannot contain hearsay is important because courts that assume the existence of hearsay may wrongfully exclude computer-generated evidence if a hearsay exception does not apply. For example, in United States v. Blackburn, 992 F.2d 666 (7th Cir. 1993), a bank robber left his eyeglasses behind in an abandoned stolen car. The prosecution's evidence against the defendant included a computer printout from a machine that tests the curvature of eyeglass lenses; the printout revealed that the prescription of the eyeglasses found in the stolen car exactly matched the defendant's. At trial, the district court assumed that the computer printout was hearsay, but concluded that the printout was an admissible business record according to Fed. R. Evid. 803(6). On appeal following conviction, the Seventh Circuit also assumed that the printout contained hearsay, but agreed with the defendant that the printout could not be admitted as a business record:

> the [computer-generated] report in this case was not kept in the course of a regularly conducted business activity, but rather was specially prepared at the behest of the FBI and with the knowledge that any information it supplied would be used in an ongoing criminal investigation. . . . In finding this report inadmissible under Rule 803(6), we adhere to the well-established rule that documents made in anticipation of litigation are inadmissible under the business records exception.

Id. at 670. See also Fed. R. Evid. 803(6) (stating that business records must be "made . . . by or transmitted by, a person").

Fortunately, the Blackburn court ultimately affirmed the conviction, concluding that the computer printout was sufficiently reliable that it could have been admitted under the residual hearsay exception, Rule 803(24). See id. at 672. However, instead of considering a reversal of the conviction because Rule 803(6) did not apply, the court should have asked whether the computer printout from the lens-testing machine contained hearsay at all. This question would have revealed that the computer-generated printout could not be excluded properly on hearsay grounds because it contained no human "statements."

2. Applicability of the Hearsay Rules to Computer-Stored Records

Computer-stored records that contain human statements must satisfy an exception to the hearsay rule if they are offered for the truth of the manner asserted. Before a court will admit the records, the court must establish that the statements contained in the record were made in circumstances that tend to ensure their trustworthiness. See, e.g., Jackson, 208 F.3d at 637 (concluding that postings from the websites of white supremacist groups contained hearsay, and rejecting the argument that the postings were the business records of the ISPs that hosted the sites).

As discussed in the Introduction to this chapter, courts generally permit computer-stored records to be admitted as business records according to Fed. R. Evid. 803(6). Different circuits have articulated slightly different standards for the admissibility of computer-stored business records. Some courts simply apply the direct language of Fed. R. Evid. 803(6), which appears in the beginning of this chapter. See e.g., United States v. Moore, 923 F.2d 910, 914 (1st Cir. 1991); United States v. Catabran, 836 F.2d 453, 457 (9th Cir. 1988). Other circuits have articulated doctrinal tests specifically for computer records that largely (but not exactly) track the requirements of Rule 803(6). See, e.g., United States v. Cestnik, 36 F.3d 904, 909-10 (10th Cir. 1994) ("Computer business records are admissible if (1) they are kept

pursuant to a routine procedure designed to assure their accuracy, (2) they are created for motives that tend to assure accuracy (e.g., not including those prepared for litigation), and (3) they are not themselves mere accumulations of hearsay.") (quoting Capital Marine Supply v. M/V Roland Thomas II, 719 F.2d 104, 106 (5th Cir. 1983)); United States v. Briscoe, 896 F.2d 1476, 1494 (7th Cir. 1990) (computer-stored records are admissible business records if they "are kept in the course of regularly conducted business activity, and [that it] was the regular practice of that business activity to make records, as shown by the testimony of the custodian or other qualified witness.") (quoting United States v. Chappell, 698 F.2d 308, 311 (7th Cir. 1983)). Notably, the printout itself may be produced in anticipation of litigation without running afoul of the business records exception. The requirement that the record be kept "in the course of a regularly conducted business activity" refers to the underlying data, not the actual printout of that data. See United States v. Sanders, 749 F.2d 195, 198 (5th Cir. 1984).

From a practical perspective, the procedure for admitting a computer-stored record pursuant to the business records exception is the same as admitting any other business record. Consider an e-mail harassment case. To help establish that the defendant was the sender of the harassing messages, the prosecution may seek the introduction of records from the sender's ISP showing that the defendant was the registered owner of the account from which the e-mails were sent. Ordinarily, this will require testimony from an employee of the ISP ("the custodian or other qualified witness") that the ISP regularly maintains customer account records for billing and other purposes, and that the records to be offered for admission are such records that were made at or near the time of the events they describe in the regular course of the ISP's business. Again, the key is establishing that the computer system from which the record was obtained is maintained in the ordinary course of business, and that it is a regular practice of the business to rely upon those records for their accuracy.

The business record exception is the most common hearsay exception applied to computer records. Of course, other hearsay exceptions may be applicable in appropriate cases, such as the public records exception of Fed. R. Evid. 803(8). See, e.g., United States v. Smith, 973 F.2d 603, 605 (8th Cir. 1992) (police computer printouts); Hughes v. United States, 953 F.2d 531, 540 (9th Cir. 1992) (computerized IRS printouts).

D. Other Issues

The authentication requirement and the hearsay rule usually provide the most significant hurdles that prosecutors will encounter when seeking the admission of computer records. However, some agents and prosecutors have occasionally considered two additional issues: the application of the best evidence rule to computer records, and whether computer printouts are "summaries" that must comply with Fed. R. Evid. 1006.

1. The Best Evidence Rule

The best evidence rule states that to prove the content of a writing, recording, or photograph, the "original" writing, recording, or photograph is ordinarily required. See Fed. R. Evid. 1002. Agents and prosecutors occasionally express concern that a mere printout of a computer-stored electronic file may not be an "original" for the purpose of the best evidence rule. After all, the original file is merely a

collection of 0's and 1's; in contrast, the printout is the result of manipulating the file through a complicated series of electronic and mechanical processes.

Fortunately, the Federal Rules of Evidence have expressly addressed this concern. The Federal Rules state that

[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".

Fed. R. Evid. 1001(3). Thus, an accurate printout of computer data always satisfies the best evidence rule. See Doe v. United States, 805 F. Supp. 1513, 1517 (D. Haw. 1992); see also Laughner v. State, 769 N.E.2d 1147, 1159 (Ind. Ct. App. 2002) (holding that AOL Instant Message logs that police had cut-and-pasted into a word-processing file satisfied best evidence rule). According to the Advisory Committee Notes that accompanied this rule when it was first proposed, this standard was adopted for reasons of practicality:

While strictly speaking the original of a photograph might be thought to be only the negative, practicality and common usage require that any print from the negative be regarded as an original. Similarly, practicality and usage confer the status of original upon any computer printout.

Advisory Committee Notes, Proposed Federal Rule of Evidence 1001(3) (1972).

2. Computer Printouts as "Summaries"

Federal Rule of Evidence 1006 permits parties to offer summaries of voluminous evidence in the form of "a chart, summary, or calculation" subject to certain restrictions. Agents and prosecutors occasionally ask whether a computer printout is necessarily a "summary" of evidence that must comply with Fed. R. Evid. 1006. In general, the answer is no. See Sanders, 749 F.2d at 199; Catabran, 836 F.2d at 456-57; United States v. Russo, 480 F.2d 1228, 1240-41 (6th Cir. 1973). Of course, if the computer printout is merely a summary of other admissible evidence, Rule 1006 will apply just as it does to other summaries of evidence. See United States v. Allen, 234 F.3d 1278, 2000 WL 1160830, at *1 (9th Cir. Aug. 11, 2000) (unpublished).

###

ENDNOTES

1. Technically, the Electronic Communications Privacy Act of 1986 amended Chapter 119 of Title 18 of the U.S. Code, codified at 18 U.S.C. §§ 2510-22, and created Chapter 121 of Title 18, codified at 18 U.S.C. §§ 2701-12. As a result, some courts and commentators use the term "ECPA" to refer collectively to both §§ 2510-22 and §§ 2701-12. This manual adopts a simpler convention for the sake of clarity: §§ 2510-22 will be referred to by its original name, "Title III," (as Title III of the Omnibus Crime Control and Safe Streets Act, passed in 1968), and §§ 2701-12 as "ECPA."

2. After viewing evidence of a crime stored on a computer, agents may need to seize the computer temporarily to ensure the integrity and availability of the evidence before they can obtain a warrant to search the contents of the computer. See, e.g., Hall, 142 F.3d at 994-95; United States v. Grosenheider, 200 F.3d 321, 330 n.10 (5th Cir. 2000). The Fourth Amendment permits agents to seize a computer temporarily so long as they have probable cause to believe that it contains evidence of a crime, the agents seek a warrant expeditiously, and the duration of the warrantless seizure is not "unreasonable" given the totality of the circumstances. See United States v. Place, 462 U.S. 696, 701 (1983); United States v. Martin, 157 F.3d 46, 54 (2d Cir. 1998); United States v. Licata, 761 F.2d 537, 540-42 (9th Cir. 1985).

3. Consent by employers and co-employees is discussed separately in the workplace search section of this chapter. See Chapter 1.D.

4. Of course, agents executing a search pursuant to a valid warrant or an exception to the warrant requirement need not rely on the plain view doctrine to justify the search. The warrant or exception itself justifies the search. See generally Chapter 2.D, "Searching Computers Already in Law Enforcement Custody."

5. The membership currently includes Australia, Austria, Belarus, Brazil, Canada, Denmark, Finland, France, Germany, India, Indonesia, Israel, Italy, Japan, the Republic of Korea, Luxembourg, Malaysia, Morocco, The Netherlands, Norway, Philippines, Romania, Russia, Spain, Sweden, Thailand, the United Kingdom, and the United States.

6. Creating a duplicate copy of an entire drive (often known simply as "imaging") 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 (as well as other data such as deleted file fragments). 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, a file-by-file 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.

7. Such distinctions may also be important from the perspective of asset forfeiture. Property used to commit or promote an offense involving obscene material may be forfeited criminally pursuant to 18 U.S.C. § 1467. Property used to commit or promote an offense involving child pornography may be

forfeited criminally pursuant to 18 U.S.C. § 2253 and civilly pursuant to 18 U.S.C. § 2254. Agents and prosecutors can contact the Asset Forfeiture and Money Laundering Section at (202) 514-1263 for additional assistance.

8. The Steve Jackson Games litigation raised many important issues involving the PPA and ECPA before the district court. On appeal, however, the only issue raised was "a very narrow one: whether the seizure of a computer on which is stored private E-mail that has been sent to an electronic bulletin board, but not yet read (retrieved) by the recipients, constitutes an 'intercept' proscribed by 18 U.S.C. § 2511(1)(a)." Steve Jackson Games, 36 F.3d at 460. This issue is discussed in the electronic surveillance chapter. See Chapter 4, infra.

9. This raises a fundamental distinction overlooked in Steve Jackson Games: the difference between a Rule 41 search warrant that authorizes law enforcement to execute a search, and an ECPA search warrant that compels a provider of electronic communication service or remote computing service to disclose the contents of a subscriber's network account to law enforcement. Although both are called "search warrants," they are very different in practice. ECPA search warrants required by 18 U.S.C. § 2703(a) are court orders that are served much like subpoenas: ordinarily, the investigators transmit the warrant to the provider, and the provider then divulges to the investigators within a certain period of time the information described in the warrant. In contrast, normal Rule 41 search warrants typically authorize agents to enter onto private property, search for and then seize the evidence described in the warrant. Compare Chapter 2 (discussing search and seizure with a Rule 41 warrant) with Chapter 3 (discussing electronic evidence that can be obtained under ECPA). This distinction is especially important when a court concludes that ECPA was violated and then must determine the remedy. Because the warrant requirement of 18 U.S.C. § 2703(a) is only a statutory standard, a non-constitutional violation of § 2703(a) should not result in suppression of the evidence obtained. See Chapter 3.H (discussing remedies for violations of ECPA).

10. In this respect, Rule 41 search warrants differ from federal ECPA search warrants under 18 U.S.C. § 2703(a), which may be served outside the issuing district. See Chapter 3.D.5, infra.

11. Focusing on the computers rather than the information may also lead to a warrant that is too narrow. If relevant information is in paper or photographic form, agents may lack authority to seize it.

12. An unusual number of computer search and seizure decisions involve child pornography. This is true for two reasons. First, computer networks provide an easy means of possessing and transmitting contraband images of child pornography. Second, the fact that possession of child pornography transmitted over state lines is a felony often leaves defendants with little recourse but to challenge the procedure by which law enforcement obtained the contraband images. Investigators and prosecutors should contact the Child Exploitation and Obscenity Section at (202) 514-5780 or an Assistant U.S. Attorney designated as a Child Exploitation and Obscenity Coordinator for further assistance with child exploitation investigations and cases.

13. Of course, the reality that agents legally may retain hardware for an extended period of time does not preclude agents from agreeing to requests from defense counsel for return of seized hardware and files. In several cases, agents have offered suspects electronic copies of innocent files with financial or personal value that were stored on seized computers. If suspects can show a legitimate need for access to seized files or hardware and the agents can comply with suspects' requests without either jeopardizing the investigation or imposing prohibitive costs on the government, agents should consider offering their assistance as a courtesy.

14. This is true for two reasons. First, account holders may not retain a "reasonable expectation of privacy" in information sent to network providers because sending the information to the providers may constitute a disclosure under the principles of United States v. Miller, 425 U.S. 435, 440-43 (1976)

(holding that bank records are disclosed information and thus not subject to Fourth Amendment protection), and Smith v. Maryland, 442 U.S. 735, 741-46 (1979) (finding no reasonable expectation of privacy in dialed telephone numbers). See Chapter 1.B.3 ("Reasonable Expectation of Privacy and Third Party Possession"). Second, the Fourth Amendment generally permits the government to issue a subpoena compelling the disclosure of information and property even if it is protected by a Fourth Amendment "reasonable expectation of privacy." When the government does not actually conduct the search for evidence, but instead merely obtains a court order that requires the recipient of the order to turn over evidence to the government within a specified period of time, the order complies with the Fourth Amendment so long as it is not overbroad, seeks relevant information, and is served in a legal manner. See United States v. Dionisio, 410 U.S. 1, 7-12 (1973); In re Horowitz, 482 F.2d 72, 75-80 (2d Cir. 1973) (Friendly, J.). This analysis also applies when a suspect has stored materials remotely with a third party, and the government serves the third party with the subpoena. The cases indicate that so long as the third party is in possession of the target's materials, the government may subpoena the materials from the third party without first obtaining a warrant based on probable cause, even if it would need a warrant to execute a search directly. See United States v. Barr, 605 F. Supp. 114, 119 (S.D.N.Y. 1985) (subpoena served on private third-party mail service for the defendant's undelivered mail in the third party's possession); United States v. Schwimmer, 232 F.2d 855, 861-63 (8th Cir. 1956) (subpoena served on third-party storage facility for the defendant's private papers in the third party's possession); Newfield v. Ryan, 91 F.2d 700, 702-05 (5th Cir. 1937) (subpoena served on telegraph company for copies of defendants' telegrams in the telegraph company's possession).

15. The inclusion of wire communications (e.g. voice mail) in this category, made effective by the PATRIOT Act, will sunset on December 31, 2005, unless extended by Congress. See PATRIOT Act §§ 209, 224, 115 Stat. 272, 283, 295 (2001).

16. The government may extend the delay of notice for additional 90-day periods on application to a court. See 18 U.S.C. § 2705(a)(4).

17. Unless extended by Congress, the PATRIOT Act's definition of "court of competent jurisdiction" in 18 U.S.C. §§ 2711(3) will sunset on December 31, 2005, and § 2703(d)'s reference to "a court of competent jurisdiction" will again reference § 3127(2)(A) directly. See PATRIOT Act §§ 220, 224, 115 Stat. 272, 291-92, 295 (2001).

18. The inclusion of wire communications (e.g. voice mail) in this category will sunset on December 31, 2005, unless extended by Congress. See PATRIOT Act §§ 209, 224, 115 Stat. 272, 283, 295 (2001).

19. The inclusion of wire communications (e.g. voice mail) in this category will sunset on December 31, 2005, unless extended by Congress. See PATRIOT Act §§ 209, 224, 115 Stat. 272, 283, 295 (2001).

20. The amendment to ECPA providing for out of district search warrants will sunset on December 31, 2005, unless extended by Congress. See PATRIOT Act §§ 220, 224, 115 Stat. 272, 291-92, 295 (2001).

21. Even a public provider may disclose customers' non-content records freely to any person other than a government entity. See 18 U.S.C. §§ 2702(a)(3), (c)(5).

22. The emergency disclosure provisions of § 2702(b)(6)(C) and § 2702(c) were added by the PATRIOT Act. The PATRIOT Act also simplified the treatment of voluntary disclosures of non-content records by providers (by moving all such provisions from § 2703(c) to § 2702) and clarifying that service providers have the authority to disclose non-content records to protect their rights and property. All these changes will sunset on December 31, 2005, unless extended by Congress. See PATRIOT Act §§ 212, 224, 115 Stat. 272, 284-85, 295 (2001).

23. In this regard, as in several others, ECPA mirrors the Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq. ("RFPA"). See Organizacion JD Ltda. v. United States Department of Justice, 124 F.3d 354, 360 (2d Cir. 1997) (noting that "Congress modeled . . . ECPA after the RFPA," and looking to the

RFPA for guidance on how to interpret "customer and subscriber" as used in ECPA); Tucker v. Waddell, 83 F.3d 688, 692 (4th Cir.1996) (examining the RFPA in order to construe ECPA). The courts have uniformly refused to read a statutory suppression remedy into the analogous provision of the RFPA. See United States v. Kington, 801 F.2d 733, 737 (5th Cir. 1986); United States v. Frazin, 780 F.2d 1461, 1466 (9th Cir.1986) ("Had Congress intended to authorize a suppression remedy [for violations of the RFPA], it surely would have included it among the remedies it expressly authorized.")

24. For example, the opinion contains several statements about ECPA's requirements that are inconsistent with each other and individually incorrect. At one point, the opinion states that ECPA required the Navy either to obtain a search warrant ordering AOL to disclose McVeigh's identity, or else give prior notice to McVeigh and then use a subpoena or a § 2703(d) court order. See 983 F. Supp. at 219. On the next page, the opinion states that the Navy needed to obtain a "warrant or the like" to obtain McVeigh's name from AOL. See id. at 220. However, pursuant to the former 18 U.S.C. § 2703(c)(1)(C), the Navy could have obtained McVeigh's name properly with a subpoena, and did not need to give notice of the subpoena to McVeigh.

25. The Ninth Circuit temporarily expanded the scope of "interceptions" to stored electronic communications in a pro se civil case, Konop v. Hawaiian Airlines, 236 F.3d. 1305 (9th Cir. 2001). In Konop, the court dismissed the reasoning of Smith and the pre-PATRIOT Act statutory distinction between wire and electronic communications and concluded that it would be "senseless" to treat wire communications and electronic communications differently. Id. at 1046. Accordingly, the court held that obtaining a copy of an electronic communication in "electronic storage" can constitute an interception of the communication. See id. The court, however, subsequently withdrew that opinion. See Konop v. Hawaiian Airlines, 262 F.3d. 972 (9th Cir. 2001).

26. Prohibited "use" and "disclosure" are beyond the scope of this manual.

27. State surveillance laws may differ. Some states forbid the interception of communications unless all parties consent.

28. The final clause of § 2511(2)(a)(i), which prohibits public telephone companies from conducting "service observing or random monitoring" unrelated to quality control, limits random monitoring by phone companies to interception designed to ensure that the company's equipment is in good working order. Seel James G. Carr, The Law of Electronic Surveillance, § 3.3(f), at 3-75. This clause has no application to non-voice computer network transmissions.

29. Unlike other Title III exceptions, the extension telephone exception is technically a limit on the statutory definition of "intercept." See 18 U.S.C. § 2510(4)-(5). However, the provision acts just like other exceptions to Title III monitoring that authorize interception in certain circumstances.

APPENDIX A: Sample Network Banner Language

Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions. First, banners may be used to generate consent to real-time monitoring under Title III. Second, banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA. Third, in the case of government networks, banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network under O'Connor v. Ortega, 480 U.S. 709 (1987). Fourth, in the case of a non-government network, banners may establish a system administrator's "common authority" to consent to a law enforcement search pursuant to United States v. Matlock, 415 U.S. 164 (1974).

CCIPS does not take any position on whether providers of network services should use network banners, and, if so, what types of banners they should use. Further, there is no formal "magic language" that is necessary. However, it is important to realize that banners may be worded narrowly or broadly, and the scope of consent and waiver triggered by a particular banner will in general depend on the scope of its language. Here is a checklist of issues that may be considered when drafting a banner:

- a) Does the banner state that use of the network constitutes consent to monitoring? Such a statement helps establish the user's consent to real-time interception pursuant to 18 U.S.C. § 2511(2)(c)(monitoring by law enforcement agency) or § 2511(2)(d)(provider monitoring).
- b) Does the banner state that use of the network constitutes consent to the retrieval and disclosure of information stored on the network? Such a statement helps establish the user's consent to the retrieval and disclosure of such information and/or records pursuant to 18 U.S.C. §§ 2702(b)(3), 2702(c)(2), and 2703(c)(1)(C).
- c) In the case of a government network, does the banner state that a user of the network shall have no reasonable expectation of privacy in the network? Such a statement helps establish that the user lacks a reasonable expectation of privacy pursuant to O'Connor v. Ortega, 480 U.S. 709 (1987).
- d) In the case of a non-government network, does the banner make clear that the network system administrator(s) may consent to a law enforcement search? Such a statement helps establish the system administrator's common authority to consent to a search under United States v. Matlock, 415 U.S. 164 (1974).
- e) Does the banner contain express or implied limitations or authorizations relating to the purpose of any monitoring, who may conduct the monitoring, and what will be done with the fruits of any monitoring?
- f) Does the banner state what users are authorized to access the network, and the consequences of unauthorized use of the network? Such notice makes it easier to establish knowledge of unauthorized use, and therefore may aid prosecution under 18 U.S.C. § 1030.
- g) Does the banner require users to "click through" or otherwise acknowledge the banner before using the network? Such a step may make it easier to establish that the network user actually received the notice that the banner is designed to provide.

Network providers who decide to banner all or part of their network should consider their needs and the needs of their users carefully before selecting particular language. For example, a sensitive government computer network may require a broadly worded banner that permits access to all types of electronic information. Here are three examples of broad banners:

1. WARNING! This computer system is the property of the United States Department of Justice and may be accessed only by authorized users. Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution. The Department may monitor any activity or communication on the system and retrieve any information stored within the system. By accessing and using this computer, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored locally on the hard drive or other media in use with this unit (e.g., floppy disks, PDAs and other hand-held peripherals, CD-ROMs, etc.)

2. This is a Department of Defense (DoD) computer system. DoD computer systems are provided for the processing of Official U.S. Government information only. All data contained within DoD computer systems is owned by the Department of Defense, and may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner, by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System personnel may disclose any potential evidence of crime found on DoD computer systems for any reason. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, INTERCEPTION, RECORDING, READING, COPYING, or CAPTURING and DISCLOSURE.
3. You are about to access a United States government computer network that is intended for authorized users only. You should have no expectation of privacy in your use of this network. Use of this network constitutes consent to monitoring, retrieval, and disclosure of any information stored within the network for any purpose including criminal prosecution.
   In other cases, network providers may wish to establish a more limited monitoring policy. Here are three examples of relatively narrow banners that will generate consent to monitoring in some situations but not others:
4. 4) This computer network belongs to the Grommie Corporation and may be used only by Grommie Corporation employees and only for work-related purposes. The Grommie Corporation reserves the right to monitor use of this network to ensure network security and to respond to specific allegations of employee misuse. Use of this network shall constitute consent to monitoring for such purposes. In addition, the Grommie Corporation reserves the right to consent to a valid law enforcement request to search the network for evidence of a crime stored within the network.
5. Warning: Patrons of the Cyber-Fun Internet Café may not use its computers to access, view, or obtain obscene materials. To ensure compliance with this policy, the Cyber-Fun Internet Café reserves the right to record the names and addresses of World Wide Web sites that patrons visit using Cyber-Fun Internet Café computers.
6. It is the policy of the law firm of Rowley & Yzaguirre to monitor the Internet access of its employees to ensure compliance with law firm policies. Accordingly, your use of the Internet may be monitored. The firm reserves the right to disclose the fruits of any monitoring to law enforcement if it deems such disclosure to be appropriate.

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).**[1]
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[(2)] 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

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 email 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[3]) 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.**

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

APPENDIX C: Sample Language for Preservation Request Letters under 18 U.S.C. § 2703(f)

[Internet Service Provider]
[Address]
VIA FAX to (xxx) xxx-xxxx
Dear :
I am writing to [confirm our telephone conversation earlier today and to] make a formal request for the preservation of records and other evidence pursuant to 18 U.S.C. § 2703(f) pending further legal process.
You are hereby requested to preserve, for a period of 90 days, the records described below currently in your possession, including records stored on backup media, in a form that includes the complete record. You also are requested not to disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. **If compliance with this request may result in a permanent or temporary termination of service to the accounts described below, or otherwise alert the subscriber or user of these accounts as to your actions to preserve the referenced files and records, please contact me before taking such actions.**
This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request.
This preservation request applies to the following records and evidence:
A. All stored communications and other files reflecting communications to or from [Email Account / User name / IP Address or Domain Name (between DATE1 at TIME1 and DATE2 at TIME2)];
B. All files that have been accessed by [Email Account / User name / IP Address or Domain Name (between DATE1 at TIME1 and DATE2 at TIME2)] or are controlled by user accounts associated with [Email Account / User name / IP Address or Domain Name (between DATE1 at TIME1 and DATE2 at TIME2)];
C. All connection logs and records of user activity for [Email Account / User name / IP Address or Domain Name (between DATE1 at TIME1 and DATE2 at TIME2)], including;
1. Connection date and time;
2. Disconnect date and time;
3. Method of connection (e.g., telnet, ftp, http);
4. Type of connection (e.g., modem, cable / DSL, T1/LAN);
5. Data transfer volume;
6. User name associated with the connection and other connection information, including the Internet Protocol address of the source of the connection;
7. Telephone caller identification records;
8. Records of files or system attributes accessed, modified, or added by the user;
9. Connection information for other computers to which the user of the [Email Account / User name / IP Address or Domain Name (between DATE1 at TIME1 and DATE2 at TIME2)]connected, by any means, during the connection

period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, the identities (account and screen names) and subscriber information, if known, for any person or entity to which such connection information relates, and all other information related to the connection from ISP or its subsidiaries.

All records and other evidence relating to the subscriber(s), customer(s), account holder(s), or other entity(ies) associated with [Email Account / User name / IP Address or Domain Name (between DATE1 at TIME1 and DATE2 at TIME2)], including, without limitation, subscriber names, user names, screen names or other identities, mailing addresses, residential addresses, business addresses, e-mail addresses and other contact information, telephone numbers or other subscriber number or identifier number, billing records, information about the length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form.
Any other records and other evidence relating to [Email Account / User name / IP Address or Domain Name (between DATE1 at TIME1 and DATE2 at TIME2)]. Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content and connection logs associated with or relating to postings, communications and any other activities to or through [Email Account / User name / IP Address or Domain Name (between DATE1 at TIME1 and DATE2 at TIME2)], whether such records or other evidence are in electronic or other form.
Very truly yours,

Assistant United States Attorney

APPENDIX D

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 email account; a pen register/trap and trace order to collect addresses on email 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 email account

The sample application and order below are specifically designed for use to locate and/or identify the person using a specified web-based email 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 email addresses to which the user sends email messages from the web-based account, nor to collect the addresses from which the account owner receives email. That type of order -- which might be used, for example, to discover the co-conspirators of a criminal known to use email 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 email 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:

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

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 email. 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)

APPLICATION

_____, 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[4] _____. 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.[5]

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 email and Worldwide Web traffic [6] 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

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)

ORDER

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

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.

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 email 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 email 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 email attachments and are activated by unassuming authorized users, and "bombs" which are programs designed to bombard a target email 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 pornography 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 necessary 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?**

APPENDIX G: Sample Letter for Provider Monitoring

[Note: as discussed in Chapter 4.D.3.c of this manual, agents and prosecutors should adopt a cautious approach to accepting the fruits of future monitoring conducted by providers under the provider exception. Furthermore, law enforcement may be able to avoid this issue by reliance on the computer trespasser exception. However, in cases in which law enforcement chooses to accept the fruits of future monitoring by providers, this letter may reduce the risk that any provider monitoring and disclosure will exceed the acceptable limits of § 2511(2)(a)(i).]

This letter is intended to inform [law enforcement agency] of [Provider's] decision to conduct monitoring of unauthorized activity within its computer network pursuant to 18 U.S.C. § 2511(2)(a)(i), and to disclose some or all of the fruits of this monitoring to law enforcement if [Provider] deems it will assist in protecting its rights or property. On or about [date], [Provider] became aware that it was the victim of unauthorized intrusions into its computer network. [Provider] understands that 18 U.S.C. § 2511(2)(a)(i) authorizes
an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service[.]
This statutory authority permits [Provider] to engage in reasonable monitoring of unauthorized use of its network to protect its rights or property, and also to disclose intercepted communications to [law enforcement] to further the protection of [Provider]'s rights or property. Under 18 U.S.C. § 2702(c)(3), [Provider] is also permitted to disclose customer records or other information related to such monitoring if such disclosure protects the [Provider]'s rights and property.
To protect its rights and property, [Provider] plans to [continue to] conduct reasonable monitoring of the unauthorized use in an effort to evaluate the scope of the unauthorized activity and attempt to discover the identity of the person or persons responsible. [Provider] may then wish to disclose some or all of the fruits of its interception, records, or other information related to such interception, to law enforcement to help support a criminal investigation concerning the unauthorized use and criminal prosecution for the unauthorized activity of the person(s) responsible.
[Provider] understands that it is under absolutely no obligation to conduct any monitoring whatsoever, or to disclose the fruits of any monitoring, records, or other information related to such monitoring, and that 18 U.S.C. § 2511(2)(a)(i) does not permit [law enforcement] to direct or request [Provider] to intercept, disclose, or use monitored communications, associated records, or other information for law enforcement purposes.
Accordingly, [law enforcement] will under no circumstances initiate, encourage, order, request, or solicit [Provider] to conduct nonconsensual monitoring absent an appropriate court order or a relevant exception to the Wiretap Act (e.g., 18 U.S.C. § 2511(2)(i)), and [Provider] will not engage in monitoring solely or primarily to assist law enforcement absent such circumstances. Any monitoring and/or disclosure will be at [Provider's] initiative.
[Provider] also recognizes that the interception of wire and electronic communications beyond the permissible scope of 18 U.S.C. § 2511(2)(a)(i) may potentially subject it to civil and criminal penalties.

Sincerely,

APPENDIX H: Sample Authorization For Monitoring of Computer Trespasser Activity

This letter authorizes [law enforcement agency] to monitor computer trespasser activity on [Owner / Operator]'s computer. [Owner / Operator] maintains a computer [exclusively for the use of X financial institution(s) / the United States Government / that is used in interstate or foreign commerce / and the use of this computer by a financial institution or the United States Government is affected by such unauthorized activity]. Therefore, this computer is a "protected computer" under 18 U.S.C. § 1030(e)(2).

An unauthorized user, without a contractual basis for any access, has accessed this computer, and is therefore a computer trespasser as defined by 18 U.S.C. § 2510(21). The [Owner / Operator] understands that under 18 U.S.C. § 2511(2)(i)(I), [law enforcement agency] may not "intercept [the trespasser's] wire or electronic communications...transmitted to, through, or from" this computer without authorization from [Owner / Operator].

To protect its computer from the adverse effects of computer trespasser activity, the [Owner / Operator] authorizes [law enforcement agency] to monitor the communications of the trespasser to, through, and from this protected computer. The fruits of such monitoring may support a criminal investigation and possible prosecution of the person(s) responsible for such unauthorized use.

This authorization in no way represents consent to the interception, retrieval, or disclosure of communications other than those transmitted to or from the computer trespasser, and [law enforcement agency] may not acquire such communications in the course of its monitoring, pursuant to 18 U.S.C. § 2511(3)(i)(IV), except under separate lawful authority.

Sincerely,

ENDNOTES

1. "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