Preface and Acknowledgments

This publication (the Manual) is the third edition of "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" and updates the previous version published in September 2002. During this seven-year period, case law related to electronic evidence has developed significantly. Of particular note has been the development of topics such as the procedures for warrants used to search and seize computers, the procedures for obtaining cell phone location information, and the procedures for the compelled disclosure of the content of electronic communications. In addition, as possession of electronic devices has become the norm, courts have had the opportunity in a large number of cases to address questions such as the application of the search incident to arrest doctrine to electronic devices.

Nathan Judish took primary responsibility for the revisions in this Manual, under the supervision of Richard Downing. Tim O'Shea and Jared Strauss took responsibility for revising Chapters 1 and 5, Josh Goldfoot for revising Chapter 2, Michelle Kane for revising Chapter 3, and Jenny Ellickson for revising Chapter 4. Scott Eltringham provided critical support to the editing and publishing of this Manual. Further assistance was provided by (in alphabetical order): Mysti Degani, Michael DuBose, Mark Eckenwiler, John Lynch, Jaikumar Ramaswamy, Betty Shave, Joe Springsteen, and Mick Stawasz. This edition continues to owe a debt to Orin S. Kerr, principal author of the 2001 edition. The editors would also like to thank the members of the CHIP working group.

This manual is intended as assistance, not authority. The research, analysis, and conclusions herein reflect current thinking on difficult and dynamic areas of the law; they do not represent the official position of the Department of Justice or any other agency. This manual has no regulatory effect, confers no rights or remedies, and does not have the force of law or a U.S. Department of Justice directive. See United States v. Caceres, 440 U.S. 741 (1979).

Electronic copies of this document are available from the Computer Crime and Intellectual Property Section's website, www.cybercrime.gov. The electronic version will be periodically updated, and prosecutors and agents are advised to check the website's version for the latest developments. Inquiries, comments, and corrections should be directed to Nathan Judish at (202) 514-1026. Requests for paper copies or written correspondence may be honored only when made by law enforcement officials or by public institutions. Such requests should be sent to the following address:

Attn: Search and Seizure Manual
Computer Crime and Intellectual Property Section
10th & Constitution Ave., NW
John C. Keeney Bldg., Suite 600
Washington, DC 20530

Michael M. DuBose
Chief, Computer Crime & Intellectual Property Section
Criminal Division
Department of Justice

Introduction

Computers and the Internet have entered the mainstream of American life. Millions of Americans spend hours every day using computers and mobile devices to send and receive email, surf the Internet, maintain databases, and participate in countless other activities.

Unfortunately, those who commit crimes have not missed the information revolution. Criminals use mobile 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 email; 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 dealer 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. Indeed, virtually every class of crime can involve some form of digital evidence.

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, email, word processing files, and image 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 mobile phone seized 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 briefly addressing the different roles computers can play in criminal offenses and the goals investigators and prosecutors should keep in mind when drafting search warrants. It then addresses issues that arise in drafting search warrants, in the forensic analysis of computers seized pursuant to warrants, and in post-seizure challenges to the search process. Finally, it addresses special limitations on the use of search warrants to search computers, such as the limitations imposed by the Privacy Protection Act, 42 U.S.C. § 2000aa. Questions addressed in the chapter include: 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 are the time requirements for the review of computers seized pursuant to a search warrant? What is the law governing when the government must search and return seized computers?

The focus of Chapter 3[1] is the Stored Communications Act, 18 U.S.C. §§ 2701-12 ("SCA"). The SCA governs how investigators can obtain stored account records and contents from network service providers, including Internet service providers ("ISPs"), telephone companies, and cell phone service providers. SCA issues arise often in cases involving the Internet: when investigators seek stored information concerning Internet accounts from providers of Internet service, they must comply with the statute. Topics covered in this section include: How can the government obtain email and account logs from ISPs? When does the government need to obtain a search warrant, as opposed to an 18 U.S.C. § 2703(d) order or a subpoena? When can providers disclose email and records to the government voluntarily? What remedies will courts impose when the SCA has been violated?

Chapter 4 reviews the legal framework that governs electronic surveillance, with particular emphasis on how the statutes apply to surveillance on communications networks. In particular, the chapter discusses the Wiretap Act, 18 U.S.C. §§ 2510-22 (referred to here as "Title III"), as well as the Pen Register and Trap and Trace Devices statute, 18 U.S.C. §§ 3121-27. 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 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 email from the government network server (implicating the SCA, 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 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 Chapter 5, which discusses evidentiary issues that arise frequently in computer-related cases. Prosecutors should always be concerned with admissibility issues that may arise in court proceedings. Chapter 5 addresses both hearsay and Confrontation Clause issues associated with computer records. It then discusses authentication of computer-stored records and records created by computer processes, including common challenges to authenticity, such as claims that computer records have been tampered with. It also discusses the best evidence rule and the use of summaries containing electronic evidence. Questions addressed in this chapter include: When are computer-generated records not hearsay? How can the contents of a website be authenticated? This Manual then concludes with appendices that offer sample forms, letters, and orders.

Computer crime investigations raise many novel issues. 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 United States Attorney who has been designated as a Computer Hacking and Intellectual Property ("CHIP") attorney. Every CHIP attorney receives extensive training in computer crime issues and is primarily responsible for providing expertise relating to the topics covered in this manual within his or her district. CHIPs 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, a CCIPS attorney is 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.

1 In previous versions of this Manual, the SCA was referred to as the Electronic Communications Privacy Act. The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), but ECPA itself also included amendments to the Wiretap Act and created the Pen Register and Trap and Trace Devices statute addressed in Chapter 4. See Pub. L. No. 99-508, 100 Stat. 1848 (1986). In this Manual, "the SCA" will refer to 18 U.S.C. §§ 2701-12, and "ECPA" will refer to the 1986 statute.

Chapter 1

Searching and Seizing Computers Without a Warrant

A. Introduction

The Fourth Amendment limits the ability of government agents to search for and seize evidence without a warrant. This chapter explains the constitutional limits of warrantless searches and seizures 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 "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property,"United States v. Jacobsen, 466 U.S. 109, 113 (1984), and the Court has also characterized the interception of intangible communications as a seizure. See Berger v. New York, 388 U.S. 41, 59-60 (1967). Furthermore, the Court has held that a "'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed." Jacobsen, . 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). In addition, a warrantless search that violates a person's reasonable expectation of privacy will nonetheless be constitutional if it falls within an established exception to the warrant requirement. SeeIllinois v. Rodriguez, 497 U.S. 177, 185-86 (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 permissible 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, 361 (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, 34-35 (2001); in conversations taking place in an enclosed phone booth, see Katz, 389 U.S. at 352; 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, ; 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 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, USB drives, or cell phones? If the answer is "yes," then the government ordinarily must obtain a warrant, or fall within an exception to the warrant requirement, before it accesses the information stored inside.

When confronted with this issue, courts have analogized the expectation of privacy in a computer to the expectation of privacy in closed containers such as suitcases, footlockers, or briefcases. 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. SeeUnited States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (finding reasonable expectation of privacy in a personal computer); United States v. Buckner, 473 F.3d 551, 554 n.2 (4th Cir. 2007) (same); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers."); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001); United States v. Al-Marri, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002) ("Courts have uniformly agreed that computers should be treated as if they were closed containers."); 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); see also United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007) ("A personal computer is often a repository

for private information the computer's owner does not intend to share with others. For most people, their computers are their most private spaces." (internal quotation omitted)).[1]

Although courts have generally agreed that electronic storage devices can be analogized to closed containers, they have reached differing conclusions about whether a computer or other storage device should be classified as a single closed container or whether each individual file stored within a computer or storage device should be treated as a separate closed container. In two cases, the Fifth Circuit 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. In a subsequent case, the Fifth Circuit 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. See United States v. Slanina, 283 F.3d 670, 680 (5th Cir. 2002), vacated on other grounds , 537 U.S. 802 (2002), aff'd, 359 F.3d 356, 358 (5th Cir. 2004). See also People v. Emerson, 766 N.Y.S.2d 482, 488 (N.Y. Sup. Ct. 2003) (adopting intermediate position of treating computer folders rather than individual files as closed containers); United States v. Beusch, 596 F.2d 871, 876-77 (9th Cir. 1979) (holding that when a physical ledger contains some information that falls within the scope of a warrant, law enforcement may seize the entire ledger, rather than individual responsive pages).

Other appellate courts have treated individual computer files as separate entities, at least in the search warrant context. See, e.g., Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001) (approving off-site review of a computer to "separate relevant files from unrelated files"). Similarly, the Tenth Circuit has refused to allow such exhaustive searches of a computer's hard drive in the absence of a warrant or some exception to the warrant requirement. SeeUnited 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 that the person has made openly available. See 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."); Wilson v. Moreau, 440 F. Supp. 2d 81, 104 (D.R.I. 2006) (finding no expectation of privacy in documents user stored on computers available for public use in a public

library); United States v. Gines-Perez, 214 F. Supp. 2d 205, 224-26 (D.P.R. 2002) (finding no reasonable expectation of privacy in information placed on the Internet); United States v. Butler, 151 F. Supp. 2d 82, 83-84 (D. Me. 2001) (finding no reasonable expectation of privacy in hard drives of shared university computers). Thus, several courts have held that a defendant has no reasonable expectation of privacy in files shared freely with others. See United States v. King, 509 F.3d 1338, 1341-42 (11th Cir. 2007) (holding that defendant did not have a legitimate expectation of privacy in the contents of a "shared drive" of his laptop while it was connected to a network); United States v. Barrows, 481 F.3d 1246, 1249 (10th Cir. 2007) (holding no reasonable expectation of privacy exists where defendant networked his computer "for the express purpose of sharing files"); United States v. Stults, 2007 WL 4284721, at *1 (D. Neb. Dec. 3, 2007) (finding no reasonable expectation of privacy in computer files that the defendant made available using a peer-to-peer file sharing program). Similarly, 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 1390. See also United States v. Gorshkov, (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 or obtained by fraud. See United States v. Caymen, 404 F.3d 1196, 1200 (9th Cir. 2005); 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, or a user may leave information on a shared computer network. 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 in part upon whether the third-party possession has eliminated the individual's reasonable expectation of privacy.[2]

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 closed container 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. Young, 350 F.3d 1302, 1308 (11th Cir. 2003) (holding that Federal Express's terms of service, which allowed it to access customers' packages, eliminated customer's reasonable expectation of privacy in package); 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).

Government acquisition 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. SeeUnited States v. Torres, 751 F.2d 875, 884 (7th Cir. 1984); 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 lose Fourth Amendment protection in their computer files if they relinquish control of the files.

Ordinarily, once an item has been received by the intended recipient, the sender's reasonable expectation of privacy in the item terminates. See United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995) (sender's expectation of privacy in letter "terminates upon delivery"). More generally, the Supreme Court has repeatedly held that the Fourth Amendment is not violated when information revealed to a third party is disclosed by the third party to the government, regardless of any 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 SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party . . . he cannot object if the third party conveys that information or records thereof to law enforcement authorities"); 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).

Courts have applied these principles to electronic communications. For example, in United States v. Horowitz, 806 F.2d 1222 (4th Cir. 1986), the defendant emailed 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 1224-26. See also Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (stating that sender of email "would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose 'expectation of privacy ordinarily terminates upon delivery' of the letter"); United States v. Meriwether, 917 F.2d 955, 959 (6th Cir. 1990) (defendant had no reasonable expectation of privacy in message sent to a pager); United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) (stating that a sender of an email "cannot be afforded a reasonable expectation of privacy once that message is received.").

Defendants will occasionally raise a Fourth Amendment challenge to the acquisition of account records and subscriber information held by Internet service providers where law enforcement obtained the records using less process than a search warrant. As discussed in Chapter 3.D, the Stored Communications Act permits the government to obtain transactional records with an "articulable facts" court order and specified subscriber information with a subpoena. See 18 U.S.C. §§ 2701-2712. These statutory procedures comply with the Fourth Amendment because customers of communication 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. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (finding no Fourth Amendment protection for network account holder's basic subscriber information obtained from communication service provider).[3] This rule accords with prior cases finding no Fourth Amendment protection in customer account records. See, e.g., United States v. Fregoso, 60 F.3d 1314, 1321 (8th Cir. 1995) (telephone records); In re Grand Jury Proceedings, 827 F.2d 301, 302-03 (8th Cir. 1987) (Western Union customer records). Similarly, use of a pen register to capture email to/from address information or Internet Protocol addresses of websites provided to an Internet service provider for routing communications does not implicate the Fourth Amendment. See United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (email and Internet users have no reasonable expectation of privacy in to/from addresses of their messages or in IP addresses of websites visited).

Although an individual normally loses a reasonable expectation of privacy in an item delivered to a recipient, there is an exception to this rule when the individual 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, she usually retains control of the package and thus retains a reasonable expectation of privacy in its contents. See, e.g., United States v. James, 353

F.3d 606, 614 (8th Cir. 2003) (finding that defendant retained Fourth Amendment rights in sealed envelope containing computer disks which he had left with a friend for storage); 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).

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), overruled on other grounds United States v. W. R. Grace, 526 F.3d 499 (9th Cir. 2008) (en banc) 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. See also United States v. Allen, 106 F.3d 695, 699 (6th Cir. 1997) ("Once a hotel guest's rental period has expired or been lawfully terminated, the guest does not have a legitimate expectation of privacy in the hotel room." (internal quotation marks omitted)).

4. Private Searches

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 marks 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. 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. 1997) (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. Where agents exceed the scope of the private warrantless search, any evidence uncovered may be vulnerable to a motion to suppress.

Private individuals often find contraband or other incriminating evidence on computers and bring that information to law enforcement, and the private search doctrine applies in these cases. In one common scenario, an individual leaves his computer with a repair technician. The technician discovers images of child pornography on the computer, contacts law enforcement, and shows those images to law enforcement. Courts have agreed that such searches by repairmen prior to

their contact with law enforcement are private searches and do not implicate the Fourth Amendment. See United States v. Grimes, 244 F.3d 375, 383 (5th Cir. 2001); United States v. Hall, 142 F.3d 988, 993 (7th Cir. 1998); United States v. Anderson, 2007 WL 1121319 at *5-6 (N.D. Ind. Apr. 16, 2007); United States v. Grant, 434 F. Supp. 2d 735, 744-45 (D. Neb. 2006); United States v. Caron, 2004 WL 438685, at *4-5 (D. Me. Mar. 9, 2004); 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).

One private search question that arises in computer cases is whether law enforcement agents must limit themselves to only files examined by the repair technician or whether all data on a particular storage device is within the scope of the initial private search. The Fifth Circuit has taken an expansive approach to this question. See United States v. Runyan, 275 F.3d 449, 464-65 (5th Cir. 2001) (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 this approach, a third-party search of a single file on a computer allows a warrantless search by law enforcement of the computer's entire contents. See id. Other courts, however, may not follow the Fifth Circuit's approach and instead 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 provide the probable cause needed to obtain a warrant for a further search.[4]

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). This test draws a line between situations where the government is a mere knowing witness to the search and those where the government is an active participant or driving force. However, this line can be difficult to discern. For

example, in United States v. Smith, 383 F.3d 700 (8th Cir. 2004), police detectives participating in "parcel interdiction" at Federal Express removed a suspicious package from a conveyer belt, submitted it to a canine sniff, and delivered the package to the Federal Express manager, telling the manager that "if she wanted to open it that would be fine." However, because the police did not actually ask or order the manager to open the package, and because there was no evidence that the manager felt obligated to open the package, the Court found that the manager was not a "government agent" for Fourth Amendment purposes. Id. at 705. See also United States v. Momoh, 427 F.3d 137, 141-42 (1st Cir. 2005) (DHL employee's desire to comply with FAA regulations did not make her a government agent absent "affirmative encouragement"). By contrast, in United States v. Souza, 223 F.3d 1197 (10th Cir. 2000), the Court found that a UPS employee was a government agent. In Souza, the police identified and removed the package from the conveyer belt, submitted it to a canine sniff, and told the UPS employee that they suspected it contained drugs. The police then told the employee that they could not tell her to open the package, but they pointed to it and said "but there it is on the floor." Id. at 1200. The employee began to open the package, but when she had difficulty, the police assisted her. While the officers' actual aid in opening the package made this an easy case, the Court's analysis suggests that the officers' other actions--identifying the package and encouraging the employee to open it--might have made the employee a government agent, particularly without evidence that the employee had an independent motivation to open it. See id. at 1202.

Other circuits have adopted more rule-like tests that focus on only the first two 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).

Two noteworthy private search cases involve an individual who hacked into computers of child pornographers for the purpose of collecting and disclosing evidence of their crimes. The hacker, who refused to identify himself or meet directly with law enforcement, emailed the incriminating evidence to law enforcement. In both cases, the evidence was admissible because when it was gathered, the individual was not an agent of law enforcement. In the first case, United States v. Steiger, 318 F.3d 1039 (11th Cir. 2003), the court had little difficulty in determining that the search did not implicate the Fourth Amendment. Because the relevant searches by the hacker took place before the hacker contacted law enforcement, the hacker was not acting as a government agent, and the private search doctrine applied. See id. at 1045. In the Steiger case, a law enforcement agent thanked the anonymous hacker, assured him he would not be prosecuted, and expressed willingness to receive other information from him. Approximately a year later (and seven months after his last previous contact with law enforcement), the hacker provided to law enforcement information he had illegally obtained from another child pornographer, which gave rise to United States v. Jarrett, 338 F.3d 339 (4th Cir. 2003). In Jarrett, the court ruled that although "the Government operated close to the line," the contacts in Steiger between the hacker and law enforcement did not create an agency relationship that carried forward to Jarrett. Id. at

346-47. Moreover, although the government created an agency relationship through further contacts with the hacker during the second investigation, that agency relationship arose after the relevant private search and disclosure. See id. at 346. Thus, the hacker's private search in Jarrett did not violate the Fourth Amendment.

5. Use of Specialized 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 constituted 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. 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 that reveals 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 quotation marks omitted)).

Defendants have occasionally--and unsuccessfully--invoked Kyllo in cases in which the government used cell tower information or an electronic device to locate a cell phone. For example, in United States v. Bermudez, 2006 WL 3197181 (S.D. Ind. June 30, 2006), aff'd 509 F.3d 820 (7th Cir. 2007), the court rejected a Kyllo challenge to the use of an electronic device to locate a cell phone because cell phones are used to transmit signals to parties outside a home. In rejecting the defendant's Kyllo argument, the court explained that "the cell phone signals were knowingly exposed to a third-party, to wit, the cell phone company." Id. at *13.

C. Exceptions to the Warrant Requirement in Cases Involving Computers

Warrantless searches that intrude upon 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). The authority to consent may be actual or apparent. See United States v. Buckner, 473 F.3d 551, 555 (4th Cir. 2007). The 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 226-27. The government carries the burden of proving that consent was voluntary. See United States v. Matlock, 415 U.S. 164, 177 (1974); Buckner, 473 F.3d at 554.

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 location, to what extent does the consent authorize the retrieval of information stored in computers at the location? 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?[5]

Finally, consent to search may be revoked "prior to the time the search is completed." United States v. Lattimore, 87 F.3d 647, 651 (4th Cir. 1996) (quoting 3 Wayne R. LaFave, Search and Seizure § 8.2(f), at 674 (3d ed. 1996)). When agents obtain consent to remove computers for off-site review and analysis, the time required for review can be substantial. In such cases, law enforcement should keep in mind that before incriminating evidence is found, the consent may be revoked. In cases involving physical documents obtained by consent, courts have allowed the government to keep copies of the documents made by the government prior to the revocation of consent, but they have forced the government to return copies made after consent was revoked. See Mason v. Pulliam, 557 F.2d 426, 429 (5th Cir. 1977); Vaughn v. Baldwin, 950 F.2d 331, 334 (6th Cir. 1991). There is little reason for courts to distinguish copying paper documents from copying hard drives, and one district court recently stated that a defendant who revoked the consent to search his computer retained no reasonable expectation of privacy in a mirror image copy of his hard drive made by the FBI. See United States v. Megahed, 2009 WL 722481, at *3 (M.D. Fla. Mar. 18, 2009).

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 marks omitted). The standard for measuring the scope of consent under the Fourth Amendment is objective reasonableness: "[W]hat 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, 333-34 (6th Cir. 1991).

Computer cases often raise the question of whether general 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) (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) (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); United States v. Tucker, 305 F.3d 1193, 1202 (10th Cir. 2002) (allowing computer search pursuant to parole agreement allowing search of "any other property under [defendant's] control"); United States v. Lemmons, 282 F.3d 920, 924-25 (7th Cir. 2002) (defendant expanded initial consent to search of cameras and recordings to include computer files when he invited officer to look at computer and failed to object to officer's search for pornographic images). 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. Al-Marri, 230 F. Supp. 2d 535, 540-41 (S.D.N.Y. 2002) (upholding search of computer in residence and citing principle that separate consent to search closed container in fixed premises is unnecessary); United States v. Galante, 1995 WL 507249, at *3 (S.D.N.Y. Aug. 25, 1995) (general consent to search car included consent to have officer access memory of cellular telephone found in the car, in light of circuit precedent involving closed containers); Reyes, 922 F. Supp. at 834.

When agents obtain consent for one reason but then conduct a search for another reason, they should be careful to make sure that the scope of consent encompasses their actual search. For example, in United States v. Turner, 169 F.3d 84 (1st Cir. 1999), the First Circuit suppressed images of child pornography found on computers after agents procured the defendant's consent to search his property for other evidence. In Turner, detectives searching for physical evidence of an attempted sexual assault obtained written consent to search the defendant's "premises" and "personal property." Before the defendant signed the consent form, the detectives discovered a large knife and blood stains in his apartment, and they explained to him that they were looking for more evidence of the assault that the suspect might have left behind. See id. at 85-86. While several agents searched for physical evidence, one detective searched the contents of the defendant's personal computer and discovered stored images of child pornography. The defendant was thereafter 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 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). Of course, as with other scope-of-consent cases, cases analyzing the reason for a search are fact specific, and courts' interpretations of the scope of consent are not always narrow. See United States v. Marshall, 348 F.3d 281, 287-88 (1st Cir. 2003) (finding that consent to search for "stolen items" did not

preclude seizing and viewing video tapes where video equipment, but not video tapes, were reported stolen); United States v. Raney, 342 F.3d 551, 556-58 (7th Cir. 2003) (finding consent to search for "materials in the nature of" child exploitation and child erotica was broad enough to encompass search of homemade adult pornography where the defendant had expressed an intent to make similar homemade pornography with a minor).

Finally, the scope of consent usually relates to the target item, location, and purpose of the search, rather than the search methodology used. For example, in United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005), an agent received permission to conduct a "complete search" of the defendant's computer for child pornography. The agent explained that he would use a "pre-search" disk to find and display image files, allowing the agent to easily ascertain whether any images contained child pornography. Id. at 1248. When the disk, for unexplained reasons, failed to function, the agent conducted a manual search for image files, eventually discovering several pieces of child pornography. Id. Although the agent ultimately used a different search methodology than the one he described to the defendant, the Court approved the manual search because it did not exceed the scope of the described disk search. Id. at 1249-50. See also United States v. Long, 425 F.3d 482, 487 (7th Cir. 2005) (finding that agent's use of "sophisticated" Encase forensic software did not exceed scope of consent to search laptop).

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. Moreover, investigators who have seized a computer based on consent and who have developed probable cause may consider obviating concerns with either the scope of consent or revocation of consent by obtaining a search warrant. For a sample consent to search form, see Appendix J.

b. Third-Party Consent

i. General Principles

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, 119-20 (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' 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).

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 (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). Nevertheless, specific facts may overcome an individual's expectation of privacy even in password-protected files. In United States v. Buckner, 407 F. Supp. 2d 777 (W.D. Va. 2006), the Court held that the defendant's wife could validly consent to a search of the family computer, including her husband's password-protected files. The Court distinguished Trulock by noting that the computer was leased solely in the wife's name, the allegedly fraudulent activity that provoked the search had occurred through accounts in the wife's name, the computer was located in a common area of the house, none of the files were encrypted, and the computer was on even though the husband had apparently fled the area. Id. at 780-81. Furthermore, 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 quotation marks 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. For example, in United States v. Morgan, 435 F.3d 660 (6th Cir. 2006), investigators received consent from the defendant's wife to search a computer located in the common area of the home. The wife told police that she had access to the computer, that neither she nor her husband used individual usernames or passwords, and that she had recently installed spyware on the computer to monitor her husband's suspected viewing of child pornography. Id. at 663-64. She did not tell the police that she had her own, separate computer for her primary use. Id at 662. Nevertheless, the Court found that the police could reasonably rely on her statements and conclude that she had authority to consent to the search. Id. at 664. See also United States v. Andrus, 483 F.3d 711, 720-21 (10th Cir. 2007) (holding that parent had apparent authority to consent to search of computer in room of adult child, where parent had unrestricted access to adult child's bedroom and paid for Internet access).

The Supreme Court has held, however, that investigators cannot rely on a third party's consent to search a residence when the target of the search is present and expressly objects to the search. See Georgia v. Randolph, 547 U.S. 103, 121 (2006). The court's conclusion was based on its determination that a "co-tenant wishing to open the door to a third party has no recognized authority in law or social practice to prevail over a present and objecting co-tenant." Id. at 114. Moreover, unless police remove a potential objector "for the sake of avoiding a possible objection," Randolph does not apply to "potential" objectors who have not taken part in the consent colloquy, even if the potential objector is nearby. Id at 121. For example, in United States v. Hudspeth, 518 F.3d 954 (8th Cir. 2008) (en banc), officers arrested the defendant at his workplace for possession of child pornography, and the defendant refused to consent to a search of his home. Nevertheless, his wife subsequently consented to a search of a computer in their home. The Eighth Circuit upheld the search, explaining that "unlike Randolph, the officers in the present case were not confronted with a 'social custom' dilemma, where two physically present co-tenants have contemporaneous competing interests and one consents to a search, while the other objects." Id. at 960. See also United States v. Crosbie, 2006 WL 1663667, at *2 (S.D. Ala. June 9, 2006) (defendant's wife's consent to computer search was valid even though wife had ordered her husband out of the house, thus depriving him of the "opportunity to object").

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 a search of all of the couple's property. See, e.g., Trulock v. Freeh, 275 F.3d 391, 398, 403-04 (4th Cir. 2001) (holding that woman did not have authority to consent to search of computer files of the man with whom she lived, when she had told agents that she did not know the password to access his files); 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, 497 U.S. 177 (1990)).

iii. Parents

Parents can consent to searches of their children's computers 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 Wayne 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) ("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. Andrus, 483 F.3d 711, 713, 720-21 (10th Cir. 2007) (parent had apparent authority to consent to search of computer in room of 51-year-old son who did not pay rent, where parent had unrestricted access to adult child's bedroom and paid for Internet access); United States v. Rith, 164 F.3d 1323, 1331 (10th Cir. 1999) (suggesting that parents were 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. Computer Repair Technicians

As discussed above in Section B.4, computer searches by repairman prior to contact with law enforcement are private searches and do not implicate the Fourth Amendment. Most commonly, law enforcement will use information revealed through a repairman's private search as a basis to secure a warrant for a full search of the computer. In some cases, however, law enforcement officers have relied on the consent of the repairman as the basis for a search of the computer that exceeds the scope of the initial private search. District courts have split on whether computer repairmen have the authority to authorize such searches. Compare United States v. Anderson, 2007 WL 1121319, at *6 (N.D. Ind. Apr. 16, 2007) (technicians had "actual and apparent authority" to consent to a search of computer brought in for repair because they had authority to access the computer), with United States v. Barth, 26 F. Supp. 2d 929, 938 (W.D. Tex. 1998) (repairman lacked actual or apparent authority to consent to search of hard drive because the defendant had given the hard drive to the technician only for a limited purpose unrelated to the specific files and only for a limited period of time).

v. System Administrators

Computer network accounts, including the accounts provided by private employers to their employees, by government entities to public employees, and by large commercial service providers to their customers, often contain information relevant to criminal investigations. When investigators suspect that a computer network account contains relevant evidence, they may want to know whether the network's owner or manager has authority to voluntarily disclose information related to the account. As a practical matter, 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. However, whether a system administrator (generally at the direction of an appropriate supervisory official) may voluntarily consent to disclose information from or regarding a user's account varies based on whether the network belongs to a communication service provider, a private business, or a government entity.

Regarding public commercial communication service providers (such as Google or Yahoo!), the primary barrier to voluntary disclosure by the service provider is statutory, not constitutional. As discussed in Chapter 3, any attempt to obtain a system administrator's consent to disclose information regarding an account must comply with the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712. Section 2702 of the SCA prohibits public service providers from voluntarily disclosing to the government information pertaining to their customers except in certain specified situations--which often track Fourth Amendment exceptions--such as with the consent of the user, to protect the service provider's rights and property, or in an emergency. See Chapter 3.E, infra. Significantly for Fourth Amendment purposes, commercial service providers typically have terms of service that confirm their authority to access information stored on their systems, and such terms of service may establish a service provider's common authority over their users' accounts. See United States v. Young, 350 F.3d 1302, 1308-09 (11th Cir. 2003)

(holding that Federal Express's terms of service, which authorized it to inspect packages, gave it common authority to consent to a government search of a package); see also United States v. Beckett, 544 F. Supp. 2d 1346, 1350 (S.D. Fla. 2008) ("where service providers have an agreement to share information under circumstances similar to those in our case (for investigation, to cooperate with law enforcement, and to take legal action), there is no objectively reasonable expectation of privacy and therefore no Fourth Amendment protection for subscriber information"). But see Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904-08 (9th Cir. 2008) (finding government employee had reasonable expectation of privacy in pager messages stored by provider of communication service based on "informal policy that the text messages would not be audited").

As discussed more fully in Section D.1.b below, private-sector employers generally have broad authority to consent to searches in the workplace, and this authority extends to workplace networks. For example, in United States v. Ziegler, 474 F.3d 1184 (9th Cir. 2007), the Ninth Circuit held that an employer could consent to a search of the computer it provided to an employee and stated that "the computer is the type of workplace property that remains within the control of the employer even if the employee has placed personal items in it." Id. at 1191 (internal quotation marks omitted). Thus, law enforcement can generally rely on the consent of an appropriate manager to search a private workplace network. In contrast, as discussed in Section D.2 below, the Fourth Amendment rules for government computer networks differ significantly from the rules that apply to private networks. Searches of government computer networks are *not* evaluated under Matlock; instead, they are evaluated under the standards of O'Connor v. Ortega, 480 U.S. 709 (1987).

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., United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (government employee had no reasonable expectation of privacy in computer in light of computer use policy); American Postal Workers Union, Columbus Area Local AFL-CIO v. United States Postal Service, 871 F.2d 556, 559-61 (6th Cir. 1989) (postal employees retained no reasonable expectation of privacy in government lockers after signing waivers). For an expanded discussion of workplace searches, see Section D below.

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 been 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."); Security and Law Enforcement Employees, Dist. 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

The exigent circumstances exception to the warrant requirement generally applies when one of the following circumstances is present: (1) evidence is in imminent danger of destruction; (2) a threat puts either the police or the public in danger; (3) the police are in "hot pursuit" of a suspect; or (4) the suspect is likely to flee before the officer can secure a search warrant. Georgia v. Randolph, 547 U.S. 103, 117 n.6 (2006) (collecting cases); Brigham City v. Stuart, 547 U.S. 398, 403-06 (2006) (police appropriately entered house to stop assault when occupants did not respond to the officers' verbal directions); Illinois v. McArthur, 531 U.S. 326, 331-33 (2001) (police appropriately seized house for two hours while warrant was obtained); Cupp v. Murphy, 412 U.S. 291, 294-96 (1973) (murder suspect was temporarily seized and his fingernails scraped to prevent destruction of evidence). Of the four factors justifying an exigent circumstances search, the first--that the evidence is in imminent danger of destruction--is generally the most relevant in the context of computer searches.

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) whether those in possession of the contraband know that 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); see also United States v. Plavcak, 411 F.3d 655, 664-65 (6th Cir. 2005) (agents appropriately seized computer without warrant when targets were caught burning relevant documentary evidence and then ran from residence carrying computer); United States v. Trowbridge, 2007 WL 4226385, at *4-5 (N.D. Tex. Nov. 29, 2007) (agents appropriately seized computers without a warrant based on exigent circumstances where agents were concerned for their safety during a fast-moving investigation and it was likely that computer evidence would be destroyed).

Exigent circumstances can arise in computer cases before the evidence has been properly secured because electronic data is inherently perishable. Computer data can be effectively put out of law enforcement reach with widely-available and powerful encryption programs that can be triggered with just a few keystrokes. In addition, computer commands can destroy data in a matter of seconds, as can moisture, high 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 and seized the computer immediately. The district court held that the agents did not need a warrant to seize the computer because the defendant's acts had created exigent circumstances. See id. at 1392. See also United States v. Gorshkov, 2001 WL 1024026, at *4 (W.D. Wash. May 23, 2001) (circumstances justified downloading without a warrant data from computer in Russia where probable cause existed to believe 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).

With some electronic devices, exigent circumstances may arise because information may be lost when the device's battery dies, or new information may cause older information to be lost permanently. For example, 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, or the 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. 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). In United States v. Parada, 289 F. Supp. 2d 1291 (D. Kan. 2003), a court reached the same result for a cell phone, although the court's analysis may have been based in part on a misunderstanding of how cell phones function. The court held that exigent circumstances justified the search of a cell phone because the phone had limited memory and subsequent calls could overwrite previously stored numbers, whether the phone was on or off. See id. at 1303-04.

However, in electronic device cases, as in all others, the existence of exigent circumstances is tied to the facts of the individual case, and other courts have rejected claims that exigent circumstances justified a search of an electronic device. For example, in United States v. Morales-Ortiz, 376 F. Supp. 2d 1131, 1142 (D.N.M. 2004), the court held that exigent circumstances did not justify a search of the names and numbers held within a cell phone's address book. The court distinguished a search of the cell phone's address book records from the search of the incoming call log approved in Parada. See id.; see also United States v. Wall, 2008 WL 5381412, at *3-4 (S.D. Fla. Dec. 22, 2008) (noting that cell phones store text messages until they are deleted by the user and therefore rejecting argument that exigent circumstances justified search of seized cell phone); 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); United States v. Reyes, 922 F. Supp. 818, 835-36 (S.D.N.Y. 1996) (exigent circumstances could

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

Recent technological advances in pagers, cell phones, and PDAs may have an impact on the existence of exigent circumstances justifying the search of these devices without a warrant. Some of the advances may undercut the basis for finding exigent circumstances. For example, current electronic devices are more likely to rely on a storage mechanism (such as flash memory) that does not require battery power to maintain storage. However, other technological advances have created new exigencies. For example, a "kill command" can be sent to some devices that will cause the device to encrypt itself or overwrite data stored on the device. Similarly, other devices can be set to delete information stored on the device after a certain period of time. See United States v. Young, 2006 WL 1302667, at *13 (N.D.W.Va. May 9, 2006) (exigent circumstances justified searching a cell phone for text messages where the cell phone had an option for automatically deleting text messages after one day).

Importantly, because "a warrantless search must be strictly circumscribed by the exigencies which justify its initiation," Mincey v. Arizona, 437 U.S. 385, 393 (1978) (internal quotation marks omitted), exigent circumstances that support the warrantless seizure of a computer may not support the subsequent search of the computer by law enforcement. "Recognizing the generally less intrusive nature of a seizure, the [Supreme] Court has frequently approved warrantless seizures of property, on the basis of probable cause, for the time necessary to secure a warrant." Segura v. United States, 468 U.S. 796, 806 (1984) (internal citations omitted). Thus, the need to seize a container to prevent the destruction of evidence does not necessarily authorize agents to take further steps without a warrant. See United States v. Doe, 61 F.3d 107, 110-11 (1st Cir. 1995); David, 756 F. Supp. at 1392 (exigency justified seizure but not search of computer); Morales-Ortiz, 376 F. Supp. 2d at 1142 n.2 (emphasizing that while exigent circumstances may justify seizing a pager to preserve evidence, the exception does not justify manipulating the pager in order to retrieve messages). In addition, absent an immediate need to access the data, practical factors may favor a forensic analysis of a seized computer based on a search warrant. A trained analyst working in a forensic setting can often extract detailed and relevant information from a computer that would not be recovered through a hastily conducted search.

3. 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 Robinson, 414 U.S. 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.

The permissible temporal scope for a search incident to arrest varies based on whether the item searched is an item "immediately associated with the person of an arrestee," such as clothing or a wallet, or other personal property near the arrestee, such as luggage. United States v. Chadwick, 433 U.S. 1, 15 (1977). Two Supreme Court cases illustrate this distinction. First, United States v. Edwards, 415 U.S. 800, 808-09 (1974), demonstrates the substantial time allowed for a search incident to arrest of items immediately associated with the person of an arrestee: the Court upheld a search of a defendant's clothing after a night in jail. In contrast, in United States v. Chadwick, the Court held that officers impermissibly searched a footlocker seized incident to arrest when they searched the locker away from the site of the arrest ninety minutes after the arrest. See Chadwick, 433 U.S. at 14-16. The Court stated that "[o]nce law enforcement officers have reduced luggage or other personal property not immediately associated with the person of the arrestee to their exclusive control, and there is no longer any danger that the arrestee might gain access to the property to seize a weapon or destroy evidence, a search of that property is no longer an incident of the arrest." Id. at 15.

The Supreme Court recently revisited the search incident to arrest doctrine in Arizona v. Gant, 129 S. Ct. 1710 (2009). There, the Court authorized a search of a passenger compartment of a vehicle incident to arrest in only two situations: first, "when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search"; and second, "when it is reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle." Id. at 1719 (internal quotation marks omitted). Caution is appropriate until courts consider whether the reasoning of Gant is limited to vehicle searches, but there is good reason to conclude that the "evidence relevant to the crime of arrest" requirement should apply only to such searches. Gant states that its second exception is based on "circumstances unique to the vehicle context" and cites Justice Scalia's concurrence in Thornton v. United States, 541 U.S. 615, 632 (2004). That concurrence proposed the second exception in the context of vehicle searches and explained that "[a] motorist may be arrested for a wide variety of offenses; in many cases, there is no reasonable basis to believe relevant evidence might be found in the car." Thornton, 541 U.S. at 632.

Beginning with pagers and now extending to cell phones and personal digital assistants, courts have generally agreed that the search incident to arrest doctrine applies to portable electronic devices. First, numerous cases over the last decade have approved searches of pagers incident to arrest. See United States v. Brookes, 2005 WL 1940124, at *3 (D.V.I. Jun. 16, 2005); 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); United States v. Reyes, 922 F. Supp. 818, 833 (S.D.N.Y. 1996); United States v. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995); United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993); see also United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996) (same holding, but relying on an exigency theory). More recently, many courts have upheld searches of cell phones incident to arrest. United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007); United States v. Valdez, 2008 WL 360548, at *2-4 (E.D. Wis. Feb. 8, 2008); United States v. Curry, 2008 WL 219966, at *10 (D. Me. Jan. 23, 2008); United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1278-79 (D. Kan. 2007); United States v. Dennis, 2007 WL 3400500, at *7-8 (E.D. Ky. Nov. 13, 2007); United States v. Mendoza, 421 F.3d 663, 666-68 (8th Cir. 2005); United States v. Brookes, 2005 WL 1940124, at *3 (D.V.I. Jun. 16, 2005); United States v. Cote, 2005 WL 1323343, at *6 (N.D. Ill. May 26, 2005). In addition, one

appellate court has approved a search incident to arrest of an electronic address book. See United States v. Goree, 2002 WL 31050979, at *5-6 (6th Cir. Sept. 12, 2002).

Courts have disagreed about whether a search incident to arrest of a cell phone is more like the footlocker in Chadwick (and thus subject to strict temporal requirements) or the search of the personal property in Edwards (and thus subject to more flexible temporal requirements). The only appellate court to consider the issue held that a cell phone found on the defendant's person constitutes personal property "immediately associated" with the arrestee. Finley, 477 F.3d at 260 n.7. See also United States v. Wurie, 2009 WL 1176946, at *5 (D. Mass. 2009); Brookes, 2005 WL 1940124, at *3 (analogizing pager and cell phone to wallet or address book); Cote, 2005 WL 1323343, at *6 (upholding search of cell phone at police station two and a half hours after arrest). However, two district courts have analogized cell phones to the footlocker in Chadwick and held that cell phone searches not contemporaneous with arrest violated the Fourth Amendment. See United States v. Lasalle, 2007 WL 1390820, at *7 (D. Haw. May 9, 2007) (rejecting cell phone search more than two hours and fifteen minutes after arrest); United States v. Park, 2007 WL 1521573, at *5-9 (N.D. Cal. May 23, 2007) (rejecting cell phone search approximately ninety minutes after arrest). See also United States v. Wall, 2008 WL 5381412, at *3-4 (S.D. Fla. Dec. 22, 2008) (search of cell phone performed at stationhouse after arrest could not be justified as incident to arrest).

Courts have not yet addressed whether electronic media with the vast storage capacity of today's laptop computers may be searched incident to arrest. However, courts 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. Molinaro, 877 F.2d 1341, 1347 (7th Cir. 1989) (citing cases); United States v. Castro, 596 F.2d 674, 677 (5th Cir. 1979). 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 these holdings are applied to searches incident to arrest where computers and similar storage media are recovered, agents should be able to review the contents of such devices without securing a search warrant.

On the other hand, courts may analogize a laptop to the footlocker in Chadwick, so a search incident to arrest of a laptop may be judged under Chadwick's restrictive temporal standard if it is not seized from the suspect's person. As a practical matter, it may not be feasible to conduct an appropriate search of a laptop incident to arrest (though a brief review may be possible in some cases, particularly as forensic tools designed for on-site review become available). A complete forensic search often requires that the data on a computer be copied and then searched using tools designed for forensic analysis, and such a full search may be impossible under Chadwick. Instead, agents may choose to seize a laptop incident to arrest and then obtain a search warrant for the subsequent thorough search.[7] When making an arrest, seizure of items on the arrestee's person or within his reach is entirely appropriate. See Edwards, 415 U.S. at 805.

4. 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, 136 (1990). Although officers may occasionally come upon incriminating evidence on the screen of a computer, the most common use of the plain view doctrine in the computer context occurs when agents examine a computer pursuant to a search warrant and discover evidence of a separate crime that falls outside the scope of the search warrant. For example, in United States v. Wong, 334 F.3d 831, 838 (9th Cir. 2003), an agent discovered child pornography on a hard drive while conducting a valid search of the drive for evidence of a murder. Because the agent was properly searching graphics files for evidence of the murder, the child pornography was properly seized and subsequently admitted under the plain view doctrine. The plain view doctrine can also be useful in other circumstances when agents are lawfully in a position to discover incriminating evidence on a computer. See, e.g., United States v. Herndon, 501 F.3d 683, 693 (6th Cir. 2007) (officer permissibly seized a computer based upon plain view after a probation agent showed the officer child pornography discovered on subject's computer); United States v. Tucker, 305 F.3d 1193, 1203 (10th Cir. 2002) (approving seizure of computer under plain view doctrine by officer conducting parole search of home after officer noticed that computer had recently visited child pornography newsgroup). Most computer plain view cases involve agents viewing incriminating images, but in some circumstances the names associated with files (especially child pornography) can be incriminating as well. Compare Commonwealth v. Hinds, 768 N.E.2d 1067, 1073 (Mass. 2002) (finding that an officer lawfully searching for evidence of assault could open and seize image files whose sexually explicit names were in "plain view" and incriminating), with United States v. Stierhoff, 477 F. Supp. 2d 423, 445-49 (D.R.I. 2007) (rejecting the government's argument that the label on a computer file, "offshore," was sufficiently incriminating to justify opening the file under the plain view exception).

The plain view doctrine does not authorize agents to open and view the contents of a container 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. This means that agents cannot rely on the plain view exception to justify opening a closed container that they are not otherwise authorized to view. See United States v. Maxwell, 45 M.J. 406, 422 (C.A.A.F. 1996) (holding that computer files opened by agents were not in plain view); 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 because "a label on a container is not an invitation to search it"). As discussed above in Section 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. Most courts have analyzed individual computer files as separate stored containers. See Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001); United States v. Carey, 172 F.3d 1268, 1273-75 (10th Cir. 1999). When each file is treated as a separate closed container, agents cannot rely on the plain view doctrine to open files on a computer. However, Fifth Circuit decisions 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), vacated on other grounds, 537 U.S. 802 (2002), aff'd, 359 F.3d 356, 358 (5th Cir. 2004), suggest 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.

The plain view doctrine arises frequently in the search warrant context because it is usually necessary to review all files on a computer to find evidence that falls within the scope of a warrant. As the Ninth Circuit explained in United States v. Adjani, 452 F.3d 1140, 1150 (9th Cir. 2006), "[c]omputer files are easy to disguise or rename, and were we to limit the warrant to such a specific search protocol [e.g., key word searches], much evidence could escape discovery simply because of [the defendants'] labeling of the files." As agents review a computer for information that falls within the scope of the warrant, they may discover evidence of an additional crime, and they are entitled to seize it under the plain view doctrine. Nevertheless, the Tenth Circuit's decision in United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999), provides a cautionary example regarding continuing the review of a computer after finding evidence of a second crime. 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. In subsequent cases, the Tenth Circuit has interpreted Carey narrowly, explaining that it "simply stands for the proposition that law enforcement may not expand the scope of a search beyond its original justification." United States v. Grimmett, 439 F.3d 1263, 1268 (10th Cir. 2006). For example, in United States v. Walser, 275 F.3d 981, 986-87 (10th Cir. 2001), the court found no Fourth Amendment violation when an officer with a warrant to search for electronic records of drug transactions opened a single computer file containing child pornography, suspended the search, and then returned to a magistrate for a second warrant to search for child pornography. See also United States v. Kearns, 2006 WL 2668544, at *8 (N.D. Ga. Feb. 21, 2006) (suggesting that agent who opened every file on a compact disk, regardless of file extension, in a search for evidence of fraud could have seized images of child pornography under the "plain view" doctrine as long as he did not abandon his search).

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 of 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. Wall, 2008 WL 5381412, at *3 (S.D. Fla. Dec. 22, 2008) (inventory search exception did not justify search of cell phone); 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, an officer's examination of 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 unless some other exception to the warrant requirement applies.

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 (or at the border's functional equivalent). According to the Court, routine searches at the border do not require a warrant, probable cause, or even reasonable suspicion that the search may uncover contraband or evidence. See 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).

The Supreme Court's most recent border search case, United States v. Flores-Montano, 541 U.S. 149 (2004), suggests that reasonable suspicion is not required for most non-destructive border searches of property. In Flores-Montano, the Court determined that the border search of an automotive fuel tank did not require reasonable suspicion. The Court explained that "the reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person--dignity and privacy interests of the person being searched--simply do not carry over to vehicles." Id. at 1585. Although there may be a lesser privacy interest in gas tanks than in other property (such as computers), the Court's analysis in Flores-Montano does not appear to be narrowly confined to gas tanks or vehicles. In response to the defendant's argument

that the Fourth Amendment protects property as much as privacy, the Court emphasized the lack of physical damage to the gas tank and concluded that "[w]hile it may be true that some searches of property are so destructive as to require a different result, this was not one of them." Id. at 1587. One appellate court has noted that "[t]he Supreme Court recently made clear that reasonable suspicion is usually not required for officers to conduct non-destructive border searches of property." United States v. Camacho, 368 F.3d 1182, 1183 (9th Cir. 2004).

Since Flores-Montano, courts have upheld suspicionless border searches of computers. In United States v. Arnold, 523 F.3d 941, 946 (9th Cir. 2008), the Ninth Circuit held that "reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices." In so holding, the Arnold court explicitly rejected the defendant's argument, previously adopted by the district court, that searching a laptop is more "intrusive" than a typical search of property and more like searching a home because of its large storage capacity. Instead, the Arnold court found no logical distinction between a suspicionless border search of a traveler's luggage and a similar suspicionless search of a laptop. See id. at 947. See also United States v. Hampe, 2007 WL 1192365, at *4 (D. Me. Apr. 18, 2007) (rejecting the Arnold district court analysis and holding that border search of computer files did not require reasonable suspicion); United States v. Romm, 455 F.3d 990, 996-97 (9th Cir. 2006) (upholding border search of computer and suggesting, but not holding, that reasonable suspicion is not required for non-destructive property searches at the border).

In United States v. Ickes, 393 F.3d 501, 506-07 (4th Cir. 2005), the Fourth Circuit also held that a search of a computer and disks within the defendant's car was permissible under the border search exception, emphasizing the breadth of the government's border search authority. The Ickes court did not address whether the search of the defendant's car, and the computer and disks it contained, was "routine." However, the court did note that, while most searches of computers at the border would likely result from reasonable suspicion, it would not "enthron[e] this notion as a matter of constitutional law." Id. at 507. See also United States v. Linarez-Delgado, 259 Fed. Appx. 506, 508 (3d Cir. 2007) ("Data storage media and electronic equipment, such as films, computer devices, and videotapes, may be inspected and viewed during a reasonable border search."). In addition, Ickes rejected the defendant's argument that border searches of computers should be limited based on computers' storage of expressive materials. Ickes, 359 F.3d at 506. See also Arnold, 523 F.3d at 948 (following Ickes and refusing to carve out a First Amendment exception to the border search doctrine).

In two pre-Flores-Montano cases, district courts upheld warrantless searches of computer disks for contraband computer files, finding that the searches were "routine" and did not require reasonable suspicion. In United States v. Irving, 2003 WL 22127913, at *5 (S.D.N.Y. Sept. 15, 2003), the court noted that "any other decision effectively would allow individuals to render graphic contraband, such as child pornography, largely immune to border search." On appeal, after Flores-Montano, the Second Circuit upheld the district court's denial of Irving's motion to suppress. United States v. Irving, 452 F.3d 110 (2d Cir. 2006). However, because the Second Circuit found that the customs agents who searched Irving had reasonable suspicion, it did not consider whether reasonable suspicion was required. Id. at 124. Similarly, 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), the court held that a search of the defendant's computer and floppy disks was a routine

search for which no suspicion was required. See id. . On appeal, the Fifth Circuit affirmed on other grounds and did not reach the issue of whether the seizure of the defendant's computer equipment could be considered routine. See Roberts, 274 F.3d at 1017.

7. Probation and Parole

Individuals on probation, parole, or supervised release enjoy a diminished expectation of privacy and may be subject to warrantless searches based on reasonable suspicion, or, potentially, without any particularized suspicion. In United States v. Knights, 534 U.S. 112, 122 (2001), the Supreme Court considered the validity of a warrantless search based on reasonable suspicion of a probationer's home where the conditions of the probation required the probationer to submit to a search at any time, with or without a warrant or reasonable cause. The Court did not rely on the "special needs" analysis of Griffin v. Wisconsin, 483 U.S. 868 (1987), a previous probation search case. Instead, the Court employed "ordinary Fourth Amendment analysis that considers all the circumstances of a search." Knights, 534 U.S. at 122. The Court noted the probationer's diminished expectation of privacy, the government's interests in preventing recidivism and reintegrating probationers into the community, and the government's concern that probationers are more likely to commit (and conceal) crime than ordinary citizens. See id. at 120-21. Balancing these factors, the Court found that the search required "no more than reasonable suspicion." Id. at 121.

In Samson v. California, 547 U.S. 843, 857 (2006), the Supreme Court extended Knights, holding that the Fourth Amendment does not prohibit a suspicionless search of a parolee. As in Knights, the Court employed a "totality of the circumstances" approach and considered the parole agreement that unambiguously allowed for suspicionless searches, the government's interests in supervising parolees, and the government's interest in reducing recidivism. See Samson, 547 U.S. at 852-53. However, the Court in Samson did not make clear whether its holding extended to probationers, and the Court noted that parolees have "fewer expectations of privacy than probationers." Id. at 850; see also United States v. Herndon, 501 F.3d 683, 688 n.2 (6th Cir. 2007) (noting that Samson's application to probationers is unclear).

Following Knights and Samson, the Sixth Circuit upheld a warrantless search of a probationer's computer based on reasonable suspicion that the probationer had violated his probation by using the Internet. See United States v. Herndon, 501 F.3d 683, 692 (6th Cir. 2007). Herndon, on probation for sexual exploitation of a minor, was subject to a specific condition prohibiting him from using the Internet and requiring him to allow his probation officer to search his computer at any time for Internet use. See Id. at 685. After Herndon told his probation officer that he had used the Internet to search for a job, the probation officer went to Herndon's residence and searched his computer and an external hard drive, ultimately finding child pornography. While finding that the probation condition did not meet the "special need" standard of Griffin because it did not itself specifically include a reasonable suspicion requirement, the court nevertheless found the search was "reasonable" under Knights: Herndon's reasonable expectation of privacy was "dramatically reduced" by the probation condition and was outweighed by the government's interest in preventing recidivism. Id. at 689-91. The Sixth Circuit concluded that the probation officer's search was proper, as it required "no more than reasonable suspicion." Id. at 691.

At least one court has upheld the warrantless search of a probationer's computer even in the absence of an explicit probation condition requiring the probationer to submit to a warrantless search. In United States v. Yuknavich, 419 F.3d 1302, 1311 (11th Cir. 2005), probationer Yuknavich had been convicted of child pornography-related charges. While his probation did not include a warrantless search provision, it did prohibit him from using the Internet, except for work purposes during work hours. During a routine home visit, Yuknavich's probation officers observed a computer connected to a modem, examined it, and discovered that Yuknavich had been downloading child pornography. The Court held that even in the absence of a provision in his probation agreement authorizing warrantless searches, Yuknavich's expectation of privacy in his computer was diminished by the condition specifically restricting his Internet access, especially in light of the crime for which he was on probation. See id. at 1310. Thus, the court followed Knights and held that the search of Yuknavich's computer required, at most, reasonable suspicion. See id. at 1311.

D. Special Case: Workplace Searches

Workplace searches occur often in computer cases, as workplace computers frequently store evidence of criminal activity. Whether such searches require a warrant depends on several factual distinctions, beginning with whether the workplace is in the public sector or the private sector. In general, 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 an employee with common authority over the area searched. For government workplaces, the inquiry into whether a warrant is required to conduct a workplace search is based on the "special needs" framework set forth in O'Connor v. Ortega, 480 U.S. 709 (1987). Under that framework, a government employee may, depending on circumstances, enjoy a reasonable expectation of privacy in his workplace. However, even when the employee has a reasonable expectation of privacy, employers can nevertheless conduct warrantless searches provided the searches are work-related, justified at their inception, and permissible in scope. Id. at 725-26.

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 email from the employer's network server raise issues under the Stored Communications Act, 18 U.S.C. §§ 2701-2712 (discussed in Chapter 3), and workplace monitoring of an employee's Internet use may implicate 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 CHIP in their district (see Introduction, p. xii) 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 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, 365 (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.

Some courts have held that a private-sector employee has no reasonable expectation of privacy in the contents of his work computer or email account when his employer has explicitly reserved the right to monitor the employee's computer use or search his computer files. See United States v. Bailey, 272 F. Supp. 2d 822, 835-36 (D. Neb. 2003); Muick v. Glenayre Electronics, 280 F.3d 741, 743 (7th Cir. 2002). However, these cases rely on precedents from the public-sector context without considering the distinction between private and public employers. For example, the fact that a private employer reserves the right to search an employee's computer should not imply that the government can seize the computer without a warrant, absent the employer consenting or conducting a private search. Prosecutors should be wary in relying on these cases. For example, in United States v. Ziegler, 456 F.3d 1138, 1144-46 (9th Cir. 2006), the Ninth Circuit initially held that a private-sector employee had no reasonable expectation of privacy in his workplace computer based on his employer's monitoring and computer use policy. However, this opinion was withdrawn and superseded by United States v. Ziegler, 474 F.3d 1184, 1189-90 (9th Cir. 2007), in which the court, relying on Mancusi v. DeForte, held that the employee in fact retained a reasonable expectation of privacy in his workplace computer.

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 most cases, private-sector employers will retain sufficient authority over workplace computers to consent to a government search of the computers. In United States v. Ziegler, 474 F.3d 1184, 1191 (9th Cir. 2007), the court held that an employer could consent to a search of the computer it provided to an employee, explaining that "the computer is the type of workplace property that remains within the control of the employer 'even if the employee has placed personal items in [it].'" The court also noted the existence of a workplace policy and practice of monitoring employee computer use. See id. 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. For more information on banners, see Appendix A.

When co-workers exercise common authority over a workspace, 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 730 (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. 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., United States v. King, 509 F.3d 1338, 1341-42 (11th Cir. 2007) (contractor had no reasonable expectation of privacy in "shared" files accessible by entire military base computer network); United States v. Barrows, 481 F.3d 1246, 1248-49 (10th Cir. 2007) (public employee had no reasonable expectation of privacy in his own computer in workplace when he left computer out and unprotected from use by others); Sheppard v. Beerman, 18 F.3d 147, 152 (2d Cir. 1994) (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) (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 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) (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. SeeO'Connor, 480 U.S. at 717 (plurality) ("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 does not 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, 559-61 (6th Cir. 1989) (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 computer log on "banners" that can eliminate a reasonable expectation of privacy in the computer.

Written employment policies and computer log on "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; they 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 thousand 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 Biby v. Board of Regents, 419 F.3d 845, 850-51 (8th Cir. 2005) (university policy stating that computer files and emails may be searched in response to litigation discovery requests eliminated computer user's reasonable expectation of privacy); United States v. Thorn, 375 F.3d 679, 683 (8th Cir. 2004) (computer use policy eliminated employee's reasonable expectation of privacy in computer); United States v. Angevine, 281 F.3d 1130, 1134-35 (10th Cir. 2002) (banner and computer policy eliminated a public employee's reasonable expectation of privacy in data downloaded from Internet); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (Air Force sergeant did not have a reasonable expectation of privacy in his government email account because email use was reserved for official business and network banner informed each user upon logging on to the network that use was subject to monitoring); Wasson v. Sonoma County Junior College Dist., span class="cite">4 F. Supp. 2d 893, 905-06 (N.D. Cal. 1997) (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) (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). 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), vacated on other grounds, 537 U.S. 802 (2002), aff'd, 359 F.3d 356, 358 (5th Cir. 2004); Leventhal v. Knapek, 266 F.3d 64, 73-74 (2d Cir. 2001) (noting that agency had not placed employee on notice that he had no expectation of privacy in his computer).

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). In addition, United States v. Long, 64 M.J. 57 (C.A.A.F. 2006), supplies an example of a court interpreting a banner very narrowly. In Long, a Department of Defense banner warned users that the government could monitor the computer system "for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures. . . ." The court held that a user maintained a reasonable expectation of privacy in her email, stating that the "banner described access to 'monitor' the computer system, not to engage in law enforcement intrusions by examining the contents of particular emails in a manner unrelated to maintenance of the e-mail system." Id. at 63. However, in a subsequent case before the same court with a similar computer banner, the court declined to follow Long. See United States v. Larson, 66 M.J. 212, 216 (2008) (finding no expectation of privacy in government computer where banner established consent to monitor). Sample banners appear in Appendix A.

Furthermore, courts may consider whether or how the employer actually enforces its policy when deciding whether the policy eliminates an employee's expectation of privacy. For example, in Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), a city employee had signed a computer use policy acknowledging that he had no expectation of privacy in his use of the pager provided to him by the city. Although the court noted that this policy would eliminate the employee's reasonable expectation policy "[i]f that were all," id. at 906, the court nevertheless found that the employee had a reasonable expectation of privacy because of an "informal policy that the text messages would not be audited" if the employee paid any charges incurred through his use of text messaging for non-official purposes. Id. See also Long, 64 M.J. at 64 (noting network administrator's testimony that he did not monitor individual email accounts when testing or monitoring the network).

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

Government employers and their agents can conduct "reasonable" work-related searches without a warrant 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, 678-79 (5th Cir. 2002), vacated on other grounds, 537 U.S. 802 (2002), aff'd, 359 F.3d 356, 358 (5th Cir. 2004) (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) (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 (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) (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 work-related and 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 quotation marks 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) (in 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 real reason 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) (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 (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 (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 (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) (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) (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). But see Wiley v. Department of Justice, 328 F.3d 1346, 1356-57 (Fed. Cir. 2003) (search of employee's car based on ten-month-old anonymous tip was not justified); Ortega v. O'Connor, 146 F.3d 1149, 1162 (9th Cir. 1998) (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 quotation marks 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) (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 (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 (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 (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. SeeO'Connor, 146 F.3d at 1163 ("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); Narducci v. Village of Bellwood, 444 F. Supp. 2d 924, 932 (N.D. Ill. 2006) (purpose of addressing threats to employees did not justify recording all employee phone calls, without notice to employees, for six years after complaints of threats had stopped).

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) (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 law enforcement that he could not conduct himself. 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.

E. 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 citizen deliver demands by email 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 money can be laundered through banks in different countries in order to hide its 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 on a computer located abroad (in "Country A"), U.S. law enforcement usually must seek assistance from law enforcement authorities in Country A. Because, in general, law enforcement officers exercise their functions in the territory of another country only

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 accepted practices); or (3) other clear indicia that such practice would not be objectionable in Country A. The U.S. view (and that of some other countries) is that prior consultation is not required to (1) access publicly available materials in Country A, such as those posted to a public website, and (2) access materials in Country A with the voluntary consent of a person who has lawful authority to disclose the materials. For advice regarding what constitutes voluntary consent or lawful authority for such disclosures, contact CCIPS.

Under certain circumstances, such as where the matter under consideration constitutes a violation of the foreign country's criminal law, 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) CCIPS's high-tech law enforcement contacts in many countries that are not a part of that network; (3) law enforcement contacts maintained by OIA; (4) 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. Immigration and Customs Enforcement); and (5) the Regional Security Officer (from the Diplomatic Security Service) at the American embassy (who may have good in-country law enforcement contacts). CCIPS can be reached at 202-514-1026; 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 another 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, a request to foreign law enforcement for preservation of the evidence should be made as soon as possible. Such a request, similar to a request under 18 U.S.C. § 2703(f) to a U.S. provider (See Chapter 3.G.1), 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 International Convention on Cybercrime, completed in 2001, obligates all Parties to have the ability to effect cross-border preservation requests, and the availability of this critical form of assistance therefore is expected to increase greatly in the near future. Significantly, many countries do not have preservation and, if they receive a preservation request, will instead do a search. Such a search may not be appropriate for some cases; for

example, it may risk tipping off the target of the investigation. Investigators may consult with CCIPS regarding the likely outcome of such a preservation request.

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 fifty member countries and continues to grow every year. Participating countries have a dedicated computer crime expert and a means to contact that office or person twenty-four hours a day. 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 Parties to have a 24-hour point of contact for cybercrime cases, and international 24-hour response capabilities are therefore expected to continue to increase. The G8 and Council of Europe lists will be consolidated.

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 indicate that direct access by United States law enforcement to a computer located abroad is crucial, 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.

---

1 Although courts have analogized electronic storage devices to closed containers, some courts have also noted characteristics of computers which distinguish them from other closed containers. In United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001), the Tenth Circuit observed that "[t]he advent of the electronic age and . . . the development of desktop computers that are able to hold the equivalent of a library's worth of information, go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file

cabinets, do not often inform the situations we now face as judges when applying search and seizure law." See also United States v. Stierhoff, 477 F. Supp. 2d 423, 445 (D.R.I. 2007) ("analogizing a computer file to a closed container is a logical, if not entirely accurate, starting point for addressing the plain view doctrine's application to computer files").

2 Regardless of whether an individual retains a reasonable expectation of privacy in an item or information held by a third party, the third party may disclose the item or information to the government provided the third party has common authority over the item or information. See United States v. Young, 350 F.3d 1302, 1308-09 (11th Cir. 2003); Section C.1.b, *infra*.

3 These cases do not resolve whether an individual maintains a reasonable expectation of privacy in the contents of email in his own email account stored with a provider. See Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904-08 (9th Cir. 2008) (finding reasonable expectation of privacy in pager messages stored by provider of communication service); Wilson v. Moreau, 440 F. Supp. 2d 81, 108 (D.R.I. 2006) (finding reasonable expectation of privacy in content of Yahoo! email account).

4 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"[illegible] given the totality of the circumstances. See Illinois v. McArthur, 531 U.S. 326, 332-34 (2001); 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).

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

6 In addition, cell phones increasingly resemble computers, as they now may incorporate functions such as Internet, email, and photography. A complete forensic search of such cell phones may disclose more evidence than a brief search incident to arrest. See generally Wayne Jansen and Rick Ayers, Guidelines on Cell Phone Forensics (National Institute of Standards and Technology No. 800-101, 2007).

Chapter 2

Searching and Seizing Computers With a Warrant

A. Introduction

This Chapter discusses the legal and practical rules governing the use of warrants to search for and seize evidence stored in computers and electronic media. Section B discusses the strategic considerations any investigator or attorney should bear in mind before applying to the court for a warrant. Section C discusses the issues that arise in drafting a computer search warrant and affidavit. Section D addresses forensic analysis of the media. Section E discusses challenges to the search process. Finally, Section F discusses the limited circumstances in which statutes or other rules prohibit the government from using search warrants to obtain computers or electronic media. A sample computer search warrant appears in Appendix F.

B. Devising a Search Strategy

Before drafting a warrant application and affidavit, careful consideration should be given to what sort of evidence a search might reveal. A search of a computer's hard drive can reveal many different types of evidence. A search strategy should be chosen after considering the many possible roles of the computer in the offense:

1) A computer can be *contraband*either because the computer is a repository of data that is contraband (such as child pornography) or because the computer is stolen property;

2) a computer can be a repository of data that is *evidence of a crime*such as a spreadsheet showing illegal drug transactions, a letter used in an ongoing fraud, or log files showing IP addresses assigned to the computer and websites accessed; or

3) a computer can be an *instrumentality of a crime*for example, the computer was used as a tool to hack into websites, distribute copyrighted videos, or produce illegal pornography.

Additionally, in devising a search strategy, investigators should bear in mind both the elements that must be proven should the prosecution go to trial and also the sources of electronic evidence that are relevant to those elements.

The typical computer user thinks of the contents of a hard drive in terms of what the computer's user interface chooses to reveal: files, folders, and applications, all neatly arranged and self-contained. This, however, is merely an abstraction presented to make the computer easier to use. That abstraction hides the evidence of computer usage that modern operating systems leave on hard drives. As computers run, they leave evidence on the hard driveconsiderably more evidence than just the files visible to users. Remnants of whole or partially deleted files can still remain on the drive. Portions of files that were edited away also might remain. "Metadata" and other artifacts left by the computer can reveal information about what files have recently been accessed, when a file was created and edited, and sometimes even how it was edited. Virtual

memory paging systems can leave traces of information on the hard drive that the user might have believed were stored only in volatile computer memory such as RAM and expected to disappear when the computer was shut down. Browsers, mail readers, chat clients, and other programs leave behind configuration files that might reveal online nicknames and passwords. Operating systems and applications record additional information on the hard drive, such as records of Internet usage, the attachment of peripherals and flash drives, and the times the computer was in use. Collectively, this information can reveal to an investigator not just what a computer happens to contain at the time of the search, but also evidence of who has used a computer, when, and how.

Obviously, discovering contraband or substantive evidence of a crime on the hard drive will be a frequent goal of a computer search. However, investigators should consider other goals that a computer search might meet. Consider the following examples:

1) It may be necessary to prove that a particular individual put contraband on the hard drive, rather than someone else with access to the computer. This might be shown through evidence that a particular user was logged on, or by evidence that the computer was used shortly after the offense to check the individual's bank account or email account.

2) It may be necessary to satisfy the investigator that a virus or other piece of malware was not responsible for the offense. Often, an investigator can establish this by running a simple virus-checking program on an image of the hard drive.

3) It may be necessary to show that a defendant had knowledge of some particular subject. Web browsing history, for example, might reveal that an individual was researching how to build a methamphetamine laboratory.

A prosecutor or investigator should carefully consider the appropriate goals in drafting the warrant so as to ensure that sufficient evidence may be collected pursuant to the warrant.

C. Drafting the Affidavit, Application, and Warrant

An affidavit and application for a warrant to search a computer are in most respects the same as any other search warrant affidavit and application: the affiant swears to facts that establish that there is probable cause to believe that evidence of crime (such as records), contraband, fruits of crime, or instrumentalities of crime is present in a private space (such as a computer's hard drive, or other media, which in turn may be in another private space, such as a home or office), and the warrant describes with particularity the things (records and other data, or perhaps the computer itself) to be searched and seized. The process of drafting an affidavit and application, then, falls into two general steps: establishing probable cause to search the computer, and describing with particularity the data to be taken from the computer or the computer hardware itself.

1. Include Facts Establishing Probable Cause

The probable cause necessary to search a computer or electronic media is probable cause to believe that the media *contains* or *is* contraband, evidence of a crime, fruits of crime, or an

instrumentality of a crime. See Fed. R. Crim. P. 41(c). Evidence of crime can include evidence of ownership and control. See, e.g., United States v. Horn, 187 F.3d 781, 787-88 (8th Cir. 1999) (approving in child pornography case a warrant provision authorizing seizure of "[r]ecords, documents, receipts, keys, or other objects showing access to, and control of, the residence"). According to the Supreme Court, the probable cause standard is satisfied by an affidavit that establishes "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).

Often, no special facts in the affidavit are necessary to establish probable cause to search a computer. As a general rule, "[a] container that may conceal the object of a search authorized by a warrant may be opened immediately; the individual's interest in privacy must give way to the magistrate's official determination of probable cause." United States v. Ross, 456 U.S. 798, 823 (1982). Thus, if a warrant authorizes a search of a premises (for example, a doctor's office) for a particularized list of records (for example, false Medicare bills), then the warrant should authorize agents to search a computer they encounter on the premises if they reasonably believe the warrant describes records that might be stored on that computer. See, e.g., United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008) (agents were justified in searching a computer "where there was ample evidence that the documents authorized in the warrant could be found" on that computer); United States v. Rogers, 521 F.3d 5, 9-10 (1st Cir. 2008) (holding that "videotape is a plausible repository for a photo," such that a warrant authorizing seizure of "photos of DW" allowed seizure and review of videotape for such photos). In such a case, it is necessary to establish probable cause to believe that the records will be found on the premises, but it is no more necessary to establish that a computer or other electronic storage media will be found there than it is necessary to establish that file cabinets, piles of paper, or other record storage systems will be found there. In short, the probable cause requirement should 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. 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").

However, in United States v. Payton, ___ F.3d ___, 2009 WL 2151348 (9th Cir. July 21, 2009), the Ninth Circuit held that law enforcement is not necessarily entitled to examine a computer that may contain evidence that falls within the scope of a warrant. See id. at * 3. In Payton, an officer executing a search warrant that authorized a seizure of drug sales records and other financial records searched a computer capable of storing such records. The court held that because the warrant did not specifically authorize a search of the computer, and because nothing else present at the scene of the search suggested that records falling within the scope of the warrant would be found on the computer, the search violated the Fourth Amendment. *See id.* Under Payton, it is good policy for prosecutors and agents seeking a warrant in the Ninth Circuit to always seek

specific authorization to search computers, though failure to do so will not necessarily invalidate the search.

Probable cause will look different in every case, but in the computer search context a few common scenarios have emerged. They are discussed below.

a. Probable Cause Established Through an Internet Protocol Address

In a common computer search scenario, investigators learn of online criminal conduct. Using records obtained from a victim or from a service provider, investigators determine the Internet Protocol ("IP") address used to commit the crime. Using a subpoena or other process discussed in Chapter 3, investigators then compel the Internet Service Provider ("ISP") that has control over that IP address to identify which of its customers was assigned that IP address at the relevant time, and to provide (if known) the user's name, street address, and other identifying information. In some cases, investigators confirm that the person named by the ISP actually resides at that the street address by, for example, conducting a mail cover or checking utility bills.

Affidavits that describe such an investigation are typically sufficient to establish probable cause, and the probable cause is strengthened if the affidavit corroborates with some additional facts the association of an IP address with a physical address. See, e.g., United States v. Perez, 484 F.3d 735, 740 (5th Cir. 2007) (probable cause established through IP address used to access child pornography and ISP records of physical address); 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); United States v. Carter, 549 F. Supp. 2d 1257, 1261 (D. Nev. 2008) (probable cause established through IP address, ISP records, and utility records); United States v. Hanson, 2007 WL 4287716, at *8 (D. Me. Dec. 5, 2007) (finding probable cause based on IP address and physical address despite "no direct knowledge whether any computer hardware . . . was physically located at the" residence); United States v. Huitt, 2007 WL 2355782, at *4 (D. Idaho Aug. 17, 2007) (probable cause established through IP address and separate email address both linked to same physical location).

Defendants sometimes will argue that the mere association of an IP address with a physical address is insufficient to establish probable cause because it is technologically possible for individuals not residing at that address to use the defendant's Internet connection. Most often, this argument takes the form of a defendant arguing that he has, or could have had, an open wireless Internet connection, which would have allowed any nearby person with commonly available equipment to use the defendant's Internet connection and IP address. Courts have consistently rejected this argument because the probable cause standard for warrants requires only a fair probability that evidence or contraband will be found. See, e.g., Perez, 484 F.3d at 740 (probable cause standard met by the association of an IP address with a physical address despite defendant's argument that he could have had an "unsecure wireless connection" allowing others to use his IP address); Carter, 549 F. Supp. 2d at 1267-69 (rejecting argument that affidavit for search warrant should have mentioned the possibility of an open wireless connection); United States v. Latham, 2007 WL 4563459, at *11 (D. Nev. Dec. 18, 2007)

(finding probable cause even though "[i]t was possible that someone other than Larry Latham or a resident of his household had accessed the internet either through his wireless router or by 'spoofing' his address in order to engage in the exchange of child pornography"). Indeed, this argument is particularly weak because the wireless access point itself will typically contain evidence within the scope of the warrant. For similar reasons, courts have rejected challenges to a finding of probable cause based on the failure of an affidavit to rule out "hacking, 'spoofing', tampering, theft, destruction, or viral infections by others." United States v. Hibble, 2006 WL 2620349, at *4 (D. Ariz. Sept. 11, 2006) (citing United States v. Gourde, 440 F.3d 1065, 1073 n.5 (9th Cir. 2006) (en banc)). As the Fifth Circuit explained, "though it was possible that the transmissions originated outside of the residence to which the IP address was assigned, it remained likely that the source of the transmissions was inside that residence." Perez, 484 F.3d at 740. Alternative explanations "are more suited to being raised as a defense at trial." Hibble, 2006 WL 2620349, at *4.

b. Probable Cause Established Through Online Account Information

In another scenario, a defendant establishes an account with an online servicesuch as a Web-based email service or a pornography siteand the credit card information or contact information associated with that account is used to identify the defendant and support probable cause to search computer media in the defendant's home. For example, in United States v. Kelley, 482 F.3d 1047, 1053 (9th Cir. 2007), an affidavit established probable cause through the real name and physical address associated with several America Online "screen names" used to receive child pornography. Similarly, in United States v. Terry, 522 F.3d 645, 648 (6th Cir. 2008), probable cause to search a home was established by demonstrating that an AOL email account was used to send child pornography, that the account's owner lived in that home, and that the account's owner had a computer in that home that he had used to send email through that account in the past. See also United States v. Wilder, 526 F.3d 1, 6 (1st Cir. 2008) ("it was a fair inference from his subscription to the Lust Gallery website, as described in the affidavit, that downloading and preservation in his home of images of child pornography might very well follow").

Frequently, this scenario arises when investigators have discovered a child pornography website or email group and have successfully obtained its membership list. In United States v. Gourde, 440 F.3d 1065, 1070-71 (9th Cir. 2006) (en banc), the affidavit established probable cause through the defendant's membership in a known child pornography website, without independent evidence such as an IP address. Several other courts have also held that it is reasonable to infer from a defendant's voluntary membership in a child pornography website or "e-group" (a hybrid of an email discussion list and web forum) that the defendant downloaded or kept child pornography, although many of these courts pointed to corroborating evidence as well. See, e.g., United States v. Wagers, 452 F.3d 534, 539-40 (6th Cir. 2006); United States v. Shields, 458 F.3d 269, 279 (3d Cir. 2006) (membership in on-line child pornography Yahoo group, combined with "suggestive" email address of "LittleLolitaLove" supported probable cause); United States v. Martin, 426 F.3d 68, 77 (2d Cir. 2005) ("those who view are likely to download and store child pornography"); United States v. Froman, 355 F.3d 882, 890-91 (5th Cir. 2004) (considering factors of joining a group, remaining a member for a month, and using screen names "that reflect his interest in child pornography").

Not all courts, however, have agreed that membership alone supports probable cause. In United States v. Coreas, 419 F.3d 151 (2d Cir. 2005), a Second Circuit panel sharply disagreed with the panel in Martin. Coreas involved an affidavit that, after false accusations were excised, contained "[s]imply" the allegation that the defendant, "by clicking a button, responded affirmatively to a three-sentence invitation to join [a child pornography] e-group." Coreas, 419 F.3d at 156. The court held that this allegation "does not remotely satisfy Fourth Amendment standards" because "a 'person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person.'" Id. (quoting Ybarra v. Illinois, 444 U.S. 85, 91 (1979)). Similarly, in United States v. Falso, 544 F.3d 110, 121 (2d Cir. 2008), the Second Circuit held that there was no substantial basis for probable cause in a warrant that alleged only that it "appear[ed]" that the defendant "gained access or attempted to gain access" to a child pornography site.

c. Probable Cause Established Through Off-Line Conduct

In some cases, the defendant's name and address are known through traditional investigative techniques, and agents wish to search the individual's computer for evidence related to the crime. These cases are no different from any other computer search case: the objective of the affidavit is to establish "a fair probability that contraband or evidence of a crime would be found in computers at" the place to be searched. United States v. Adjani, 452 F.3d 1140, 1145 (9th Cir. 2006) (internal quotation marks and brackets omitted). For example, in United States v. Khanani, 502 F.3d 1281, 1290 (11th Cir. 2007), the court found probable cause to search an accountant's computer because the affidavit identified him as accountant for an employer of illegal aliens, stated that a tax return for that employer was found in the trash outside the office, and stated that an agent saw computers inside the office. See also United States v. Flanders, 468 F.3d 269, 271 (5th Cir. 2006) (probable cause to search a computer supported by defendant's "past sexual abuse of his daughter, coupled with his decision to take a digital photograph of that child naked").

d. Staleness

Defendants often claim that the facts alleged in the warrant affidavit were too stale to establish probable cause at the time the warrant was issued. Most such challenges have occurred in child pornography cases, and the courts have generally found little merit in these arguments: "When a defendant is suspected of possessing child pornography, the staleness determination is unique because it is well known that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes." United States v. Irving, 452 F.3d 110, 125 (2d Cir. 2006) (internal quotations marks omitted); see also United States v. Paull, 551 F.3d 516, 522 (6th Cir. 2009) ("because the crime is generally carried out in the secrecy of the home and over a long period, the same time limitations that have been applied to more fleeting crimes do not control the staleness inquiry for child pornography"); United States v. Watzman, 486 F.3d 1004, 1008 (7th Cir. 2007) (crediting affidavit saying that child pornographers "keep and collect items containing child pornography over long periods of time"); United States v. Newsom, 402 F.3d 780, 783 (7th Cir. 2005) ("[i]nformation a year old is not necessarily stale as a matter of law, especially where child pornography is concerned"); United States v. Riccardi, 405 F.3d 852, 861 (10th Cir. 2005) (five-year old information that defendant sought to convert a Polaroid photograph to a digital format was not stale); 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). 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). But see United States v. Doan, 2007 WL 2247657, at *3 (7th Cir. Aug. 6, 2007) (seventeen-month-old information, combined with a lack of information about "the duration of the website subscriptions, the download capability accompanying those subscriptions, the last date Doan accessed the websites, whether Doan downloaded images from these sites, whether Doan owned a computer, or whether Doan had internet access at his home" insufficient to establish probable cause); 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); United States v. Frechette, 2008 WL 4287818, at *4 (W.D. Mich. Sept. 17, 2008) (sixteen-month-old information stale in a child pornography case).

2. Describe With Particularity the Things to be Seized

a. The Particularity Requirement

The Fourth Amendment requires that every warrant "particularly describ[e]" two things: "the place to be searched" and "the persons or things to be seized." U.S. Const. Amend. IV; see United States v. Grubbs, 547 U.S. 90, 97 (2006). Describing with particularity the "things to be seized" 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 (1927) ("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 should be limited to the scope of the probable cause established in the warrant. See In re Grand Jury Investigation Concerning Solid State Devices, Inc., 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. Seizing Hardware vs. Seizing Information

The most important decision agents must make when describing the property in the warrant is whether the seizable property is the computer *hardware* or merely the *information* that the hardware contains. 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 to be seized, and then request the authority to seize the information in whatever form it may be stored (whether electronic or not).

c. Hardware seizures

Depending on the nature of the crime being investigated, computer hardware might itself be contraband, an instrumentality of a crime, or fruits of crime and therefore may be physically

seized under Rule 41. For example, a computer that stores child pornography is itself contraband. See United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (upholding seizure of entire computer as contraband in child pornography case). A computer may also be used as an instrumentality of crime, as when it is used to commit a hacking offense or send threats. See, e.g., United States v. Adjani, 452 F.3d 1140, 1145-46 (9th Cir. 2006) (computer used to send extortive threat is instrumentality); Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (computer used to operate bulletin board distributing obscene materials is instrumentality); United States v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) (computer used to send or receive child pornography is instrumentality). Although it could be argued that any computer that is used to store evidence of crime is an instrumentality, the reasoning in *Davis* suggests that in order for a computer to qualify as an instrumentality, more substantial use of the computer in the crime is necessary. See Davis, 111 F.3d at 1480 (stating that "the computer equipment was more than merely a 'container' for the files; it was an instrumentality of the crime").

If the computer hardware is itself contraband, an instrumentality of crime, or fruits of crime, the warrant should describe the hardware and indicate that the hardware will be seized. In most cases investigators will simply seize the hardware during the search, and then search through the defendant's computer for the contraband files back at a 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. 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; in many of these cases, the computers contain child pornography and are thus contraband. 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).

d. Information seizures

When electronic storage media are to be searched because they store information that is evidence of crime, the items to be seized under the warrant should usually focus on the content of the relevant files rather than the physical storage media.

Many investigations seek to search computers for evidence of a crime only; the computer might contain business records relevant to a white-collar prosecution, for example, but the computer itself does not store contraband and was not used to commit the crime. The computer is "evidence" only to the extent that some of the data it stores is evidence. See United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008) ("Computers, like briefcases and cassette tapes, can be repositories for documents and records.").

When probable cause to search relates in whole or in part to information stored on the computer, rather than to the computer itself, the warrant should identify that information with particularity, focusing 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. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (stating that the ability of a computer to store "a huge array" of information "makes the particularity requirement that much more important"); United States v. Vilar, 2007 WL 1075041, at *36 (S.D.N.Y. Apr. 4, 2007) ("underlying information must be identified with particularity and its seizure independently supported by probable cause"); United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (stating that a warrant to seize evidence stored on a computer should specify "which type of files are sought"); 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). In cases where the computer is merely a storage device for evidence, failure to focus on the relevant files may lead to a Fourth Amendment violation. For example, in United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005), which involved an investigation into harassing phone calls, the court held that a warrant authorizing seizure of all storage media and "not limited to any particular files" violated the Fourth Amendment.

Agents should be particularly careful when seeking authority to seize a broad class of information. This sometimes 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*, *Inc.*, 130 F.3d 853, 857 (9th Cir. 1997). A similarly dangerous phrase, "any and all data, including but not limited to" a list of items, has been held to turn a computer search warrant into an unconstitutional general warrant. United States v. Fleet Management Ltd., 521 F. Supp. 2d 436, 443-44 (E.D. Pa. 2007); *see also* Otero, 563 F.3d at 1132 (warrant authorizing seizure of "any and all information and/or data" fails the particularity requirement).

Instead, the description of the files to be seized should be limited. One successful technique has been to identify records that relate to a particular crime and to include specific categories of the types of records likely to be found. For example, the Ninth Circuit upheld such a warrant that

limited the search for evidence of a specific (and specified) crime. See United States v. Adjani, 452 F.3d 1140, 1148 (9th Cir. 2006). It is sometimes helpful to also specify the target of the investigation (if known) and the time frame of the records involved (if known). 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."); United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (concluding that warrant to seize "[a]ll computers" was 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.").

Thus, 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, 2008, 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 2008 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 form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

Mentioning that records might appear in electronic form is helpful for agents and lawyers who read the warrant. However, 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. Giberson, 527 F.3d 882, 888 (9th Cir. 2008) ("[t]he format of a record or document should not be dispositive to a Fourth Amendment inquiry"); United States v. Pontefract, 2008 WL 4461850, at *3 (W.D. La. Oct. 1, 2008) (warrant that specified photographs but not computers allowed the search of a computer for photographs because "in today's digital world, a laptop computer is as likely a place to find photographs as a photo album"). 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"). This approach is consistent with a forthcoming amendment to Rule 41(e) (which, assuming no contrary congressional action, is scheduled to take effect on December 1, 2009) specifying that a "warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information."

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. Scharfman, 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); 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).

3. Establishing the Necessity for Imaging and Off-Site Examination

With limited exceptions, a search of a hard drive or other media requires too much time to conduct on-site during the execution of a warrant. The search warrant affidavit should explain why it is necessary to image an entire hard drive (or physically seize it) and later examine it for responsive records.

Examining a computer for evidence of crime is nearly always a time consuming process. 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. See United States v. Hill, 322 F. Supp. 2d 1081, 1089-90 (C.D. Cal. 2004) (Kozinski, J.), aff'd 459 F.3d 966 (9th Cir. 2006); 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."). Moreover, evidence of a crime will not always take the form of a file. It may be in a log, operating system artifact, or other piece of recorded data that can be difficult to locate and retrieve without the appropriate tools and time. 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. See United States v. Hill, 459 F.3d 966, 974-75 (9th Cir. 2006) ("the officers would have to examine every one of what may be thousands of files on a diska process that could take many hours and perhaps days.").

Because examining a computer for evidence of crime is so time consuming, it will be infeasible in almost every case to do an on-site search of a computer or other storage media for evidence of crime. Agents cannot reasonably be expected to spend more than a few hours searching for evidence on-site, and in some circumstances (such as executing a search at a suspect's home) an extended search may be unreasonable. See United States v. Santarelli, 778 F.2d 609, 615-16 (11th Cir. 1985). In cases involving large quantities of paper documents, courts traditionally have allowed investigators to remove the documents to an off-site location to review the documents to determine which documents fall within the scope of the warrant. See Santarelli, 778 F.2d at 616; United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (upholding seizure of an entire file cabinet when such seizure was motivated by the impracticability of on-site sorting); United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982).

For similar reasons, courts have approved removal of computers to an off-site location for review. See United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (the "narrowest definable search and seizure reasonably likely to obtain" the evidence described in a warrant is, in most instances, "the seizure and subsequent off-premises search of the computer and all available disks"); United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (seizure of entire computer reasonable because affidavit "justified taking the entire system off site because of the time, expertise, and controlled environment required for a proper analysis"); Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001) ("[b]ecause of the technical difficulties of conducting a computer search in a suspect's home, the seizure of the computers, including their content, was reasonable in these cases to allow police to locate the offending files"); cf. United States v. Giberson, 527 F.3d 882, 886 (9th Cir. 2008) (holding that a warrant that "clearly limited the types of documents and

records that were seizable" permitted the seizure of an entire computer); United States v. Grimmett, 439 F.3d 1263, 1269 (10th Cir. 2006) ("we have adopted a somewhat forgiving stance when faced with a 'particularity' challenge to a warrant authorizing the seizure of computers"). Moreover, attempting to search storage media on-site may even risk damaging the evidence itself in some cases. Modern operating systems continually read from and write to the hard disk, changing some of the information recorded there; thus, the simple act of using a computer might alter the evidence recorded on the hard drive. Internet-connected computers are additionally vulnerable, because someone at a remote location might be able to access the computer and delete data while investigators are examining it on-site. Thus, the best strategy will generally be to review storage media off-site where forensic examiners can ensure the integrity of the data.

In many cases, rather than seize an entire computer for off-site review, agents can instead create a digital copy of the hard drive that is identical to the original in every relevant respect. This copy is called an "image copy"a copy that "duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original." United States v. Vilar, 2007 WL 1075041, *35 n.22 (S.D.N.Y. Apr. 4, 2007), quoting Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L. Rev. 531 (2005); see also United States v. Stierhoff, 477 F. Supp. 2d 423, 439 & n.8 (D.R.I. 2007). An image copy cannot be created by simply dragging and dropping icons or running conventional backup programs; the process of making one usually involves opening the computer case and connecting the investigator's own hardware directly to the hard drive. In some cases, investigators will make the image copy on-site; in others, investigators will seize the computer hardware from the premises and make the image copy off-site.

To justify the possible imaging and/or removal for off-site review of a computer or other storage media, the Ninth Circuit requires the affidavit to explain why practical constraints might require the seizure of the entire computer system for off-site examination. See United States v. Hill, 459 F.3d 966, 975-76 (9th Cir. 2006) (stating that the affidavit must "demonstrate to the magistrate factually why such a broad search and seizure authority is reasonable in the case at hand"). As imaging and/or removal is necessary in nearly every computer search warrant case, it is doubtful that failure to include such a statement in the affidavit constitutes a Fourth Amendment violation. Nevertheless, although explicitly required only by the Ninth Circuit, it is a good practice for every search warrant affidavit to explain why it is necessary to image an entire hard drive (or physically seize it) and later examine it for responsive records. Including these facts in the affidavit provides a considerable degree of reassurance that the Fourth Amendment will be satisfied. See United States v. Hill, 459 F.3d 966, 976 (9th Cir. 2006); United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) ("the affidavit explained why it was necessary to seize the entire computer system" and "justified taking the entire system off site because of the time, expertise, and controlled environment required for a proper analysis"); United States v. Adjani, 452 F.3d 1140, 1149 n.7 (9th Cir. 2006). As noted below, these facts justifying removal of storage media for off-site review should *not* commit the agents to any particular "protocol" for reviewing the media to find evidence that falls within the scope of the warrant. Instead, the affidavit will simply note that off-site review might be required.

4. Do Not Place Limitations on the Forensic Techniques That May Be Used To Search

Limitations on search methodologies have the potential to seriously impair the government's ability to uncover electronic evidence. "[A] search can be as much an art as a science," United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005), and the forensic process can require detective work, including intuition and on-the-spot judgment in deciding, based on what the examiner has just seen, what is the best step to take next. One particularly burdensome restriction that could be placed on a forensic investigator is the requirement that the investigator limit the search to files containing particular keywords. Forensic analysis may include keyword searches, but a properly performed forensic analysis will rarely end there, because keyword searches will fail to find many kinds of files that fall within the scope of a warrant. For example, at the time of this writing, a number of file types, such as TIFF files and some PDF files, cannot be searched for keywords. See, e.g., United States v. Evanson, 2007 WL 4299191, at *5 (D. Utah Dec. 5, 2007) (noting that in the search at issue some files "were in 'tiff' format," a "'digital picture of a hard copy document' that has been scanned," and that these files "had numbers as file names, rather than recognizable file names that purportedly described the data in the files"). In addition, keyword searches can also be thwarted through the use of code words or even unintentional misspellings. Law and investment firmsnot to mention individuals involved in criminal activityoften 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. Every Westlaw or LEXIS user is familiar with the difficulty of crafting search terms that find the correct case on the first try; requiring a forensic investigator to find crucial evidence with a keyword search specified prior to forensic analysis is just as impractical.

Court-mandated forensic protocols are also unnecessary because investigators already operate under significant constitutional restrictions. As with any search, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." Dalia v. United States, 441 U.S. 238, 258 (1979); United States v. Ramirez, 523 U.S. 65, 71 (1998) ("The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant."); Hill, 459 F.3d at 978 ("reasonableness of the officer's acts both in executing the warrant and in performing a subsequent search of seized materials remains subject to judicial review"). Unreasonable conduct can be remedied after the fact, including, as a "last resort," with suppression of evidence. Hudson v. Michigan, 547 U.S. 586, 591 (2006).

A few magistrate judges issue warrants to search computers only subject to limitations on the way that the seized media may later be examined. For example, some magistrates require that the forensic analysis of the computer be completed within a set time period; issues related to the timing of forensic analysis are discussed in Section D.5 below. In addition, some magistrates may refuse to sign a warrant that does not include a protocol specifying how the government will examine seized media to find evidence that falls within the scope of the warrant. See, e.g., *In re Search of 3817 W. West End,* 321 F. Supp. 2d 953, 962-63 (N.D. Ill. 2004). Neither Rule 41 nor the Fourth Amendment requires magistrates to impose such restrictions, and prosecutors should oppose such restrictions whenever they significantly interfere with the government's ability to obtain evidence that falls within the scope of the warrant. While it might be helpful for the affidavit to contain background information that might justify particular steps taken during the searchsuch as describing the ease with which evidence can be concealed in a computer, explaining the need to search off-site, or justifying the seizure of commingled recordsneither the

search warrant application nor the affidavit need contain special restrictions on how agents search for the things described in the warrant.

Any significant limitation (such as a restriction to keyword searches) on the techniques the government may use to find evidence that falls within the scope of a warrant is inconsistent with Supreme Court precedent. The Supreme Court has held that "[n]othing in the language of the Constitution or in [the Supreme Court's] decisions interpreting that language suggests that, in addition to the requirements set forth in the text [of the Fourth Amendment], search warrants also must include a specification of the precise manner in which they are to be executed." United States v. Grubbs, 547 U.S. 90, 98 (2006) (quoting Dalia, 441 U.S. at 255). "It would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth Amendment rights may be affected in more than one way, the court must set forth precisely the procedures to be followed by the executing officers." Dalia, 441 U.S. at 258. Furthermore, any limitation on the government's ability to find evidence that falls within the scope of a warrant is inconsistent with the rule that "[a] container that may conceal the object of a search authorized by a warrant may be opened immediately; the individual's interest in privacy must give way to the magistrate's official determination of probable cause." United States v. Ross, 456 U.S. 798, 823 (1982).

Magistrates requiring the government to set forth a protocol for forensic analysis have typically cited the Supreme Court's decision in Andresen v. Maryland, 427 U.S. 463 (1976), in which the Court noted that when search warrants authorize the seizure of documents, "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy." Id. at 482 n.11. Under *Andresen*, it is surely appropriate for magistrates to strictly enforce the Particularity Clause in computer cases involving commingled records. However, nothing in *Andresen* authorizes magistrates to control the manner in which a warrant is *executed*, and such control was rejected by the Court in *Dalia* and *Grubbs*. In addition, the *Andresen* Court recognized that it is necessary to look at "innocuous documents . . . in order to determine whether they are, in fact, among those papers authorized to be seized." Andresen, 427 U.S. at 482 n.11.

Circuit courts have upheld computer search warrants that included neither a protocol (a list of steps the investigator is required to undertake in examining the computer) nor an explanation for the lack of a protocol. In United States v. Giberson, 527 F.3d 882 (9th Cir. 2008), the court upheld a seizure of a computer and a search through it for particularly described records, even though the records were intermingled with other files, without requiring any protocol. The court held that "the potential intermingling of materials does not justify an exception or heightened procedural protections for computers beyond the Fourth Amendment's reasonableness requirement." Id. at 889. In United States v. Hill, 459 F.3d 966 (9th Cir. 2006), the defendant challenged the search of his computer, arguing, among other things, that the warrant was invalid because "it did not include a search protocol to limit the officer's discretion as to what they could examine when searching the defendant's computer media." Id. at 977. The court held that no search protocol was necessary, and that it also was not necessary to explain the absence of a search protocol in the warrant application. Id. at 978. The Tenth Circuit emphasized in United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005), that while warrants must describe "with particularity the objects of their search," the methodology used to find those objects need not be

described: "This court has never required warrants to contain a particularized computer search strategy." Id. at 1251. In United States v. Khanani, 502 F.3d 1281, 1290-91 (11th Cir. 2007), the Eleventh Circuit rejected the argument that a warrant should have included a search protocol, pointing in part to the careful steps agents took to ensure compliance with the warrant. See also United States v. Cartier, 543 F.3d 442, 447-48 (8th Cir. 2008) ("While we acknowledge that there may be times that a search methodology or strategy may be useful or necessary, we decline to make a blanket finding that the absence of a search methodology or strategy renders a search warrant invalid per se"); United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) ("The warrant process is primarily concerned with identifying what may be searched or seizednot how"). But see United States v. Payton, ___ F.3d ___, 2009 WL 2151348, at *3-5 (9th Cir. July 21, 2009) (holding that search of computer without explicit authorization violated Fourth Amendment where nothing present at the residence searched suggested that records falling within the scope of the warrant would be found on the computer, and suggesting in dicta that judges issuing computer search warrants "may place conditions on the manner and extent of such searches").

If a search strategy is described in the affidavit, the affidavit should clearly state that the strategy is an illustration of a likely strategy that will be employed, but not "a specification of the precise manner in which [the warrant is] to be executed." Grubbs, 547 U.S. at 98. Indeed, one court has held that "search protocols and keywords are not 'material' for purposes of Rule 16(a)(1)(E)," and thus are not discoverable. United States v. Fumo, 2007 WL 3232112, at *7 (E.D. Pa. Oct. 30, 2007).

Finally, if a magistrate judge refuses to issue a warrant without conditioning its execution on certain requirements, and if law enforcement officials choose to execute the warrant anyway, the officials should not ignore the requirements. See, e.g., United States v. Brunette, 76 F. Supp. 2d 30, 42 (D. Maine 1999), *aff'd*, 256 F.3d 14 (1st Cir. 2001) (suppression appropriate because the government failed to comply with time limits for reviewing seized computers when those time limits were required by the warrant). Instead, law enforcement officials should follow the requirements of the warrant unless they obtain relief from the issuing magistrate or an appropriate higher court. Prosecutors encountering such issues should contact CCIPS at (202) 514-1026 for further assistance.

5. Seeking Authorization for Delayed Notification Search Warrants

If certain conditions are met, a court may authorize so-called "surreptitious entry" or "sneak-and-peek" warrants that excuse agents from having to notify at the time of the search the person whose premises are searched. Neither the Fourth Amendment nor Rule 41 requires an officer executing a search warrant to present the property owner with a copy of the warrant before conducting his search. United States v. Grubbs, 547 U.S. 90, 98-99 (2006). In addition, under 18 U.S.C. § 3103a, 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 (except for unduly delaying a trial): endangering the life or physical safety of an individual, flight from prosecution, evidence tampering, witness intimidation, or otherwise seriously jeopardizing an investigation.

Under § 3103a, law enforcement authorities must provide delayed notice within a "reasonable period not to exceed 30 days after the date of [the warrant's] execution" or, alternatively, "on a later date certain if the facts of the case justify a longer period of delay." 18 U.S.C. § 3103a(b)(3). This initial period can be extended "for good cause" upon "an updated showing of the need for further delay;" such extensions are "limited to periods of 90 days or less, unless the facts of the case justify a longer period of delay." 18 U.S.C. § 3103a(c).

Section 3103a 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. For more information regarding section 3103a, prosecutors and investigators should contact the Office of Enforcement Operations ("OEO") at (202) 514-6809.

6. 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." Rule 41 defines "property" to include "information," see Fed. R. Crim. P. 41(a)(2)(A), and 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. 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.

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); cf. Herring v. United States, 129 S. Ct. 695, 702 (2009) (exclusionary rule is applied in Fourth Amendment cases only if police conduct is "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system"). 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.").

D. Forensic Analysis

1. The Two-Stage Search

In the vast majority of cases, forensic analysis of a hard drive (or other computer media) takes too long to perform on-site during the initial execution of a search warrant. Thus, as discussed in Section C.3 above, investigators generally must remove storage media for off-site analysis to determine the information that falls within the scope of the warrant. This process has two steps: *imaging*, in which the entire hard drive is copied, and *analysis,* in which the copy of the hard drive is culled for records that are responsive to the warrant.

Imaging is described in Section C.3 above. It results in the creation of an "image copy" of the hard drivea copy that "duplicates every bit and byte on the target drive including all files, the slack space, Master File Table, and metadata in exactly the order they appear on the original." United States v. Vilar, 2007 WL 1075041, at *35 n.22 (S.D.N.Y. Apr. 4, 2007), quoting Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harv. L. Rev. 531 (2005).

After imaging, the second step of the forensic review process begins: the hard drive image is examined, and data that falls within the scope of the warrant is identified. In computer search cases, where the purpose for the off-site analysis is to determine whether information stored on computer media falls within the scope of a warrant, courts have treated the off-site forensic analysis of computer media seized pursuant to a warrant as a continuation of the search, still bound by the Fourth Amendment. See United States v. Syphers, 426 F.3d 461, 468 (1st Cir. 2005) (referring to a forensic review of a seized computer as a "search"); United States v. Mutschelknaus, 564 F. Supp. 2d 1072, 1076 (D.N.D. 2008) (referring to forensic analysis as a "subsequent search"); United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 66 (D. Conn. 2002) (referring to an examination of a hard drive image as a "search").

Once a computer seized pursuant to a warrant has been reviewed and items within the computer determined to fall within the scope of the warrant, subsequent review of those items should not implicate the Fourth Amendment. As the Ninth Circuit has explained, "once an item in an individual's possession has been lawfully seized and searched, subsequent searches of that item, so long as it remains in the legitimate uninterrupted possession of the police, may be conducted without a warrant." United States v. Turner, 28 F.3d 981, 983 (9th Cir. 1994) (quoting United States v. Burnette, 698 F.2d 1038, 1049 (1983)).

2. Searching Among Commingled Records

Few computers are dedicated to a single purpose; rather, computers can perform many functions, such as "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more." United States v. Andrus, 483 F.3d 711, 718 (10th Cir. 2007). Thus, almost every hard drive encountered by law enforcement will contain records that have nothing to do with the investigation. The Fourth Amendment governs how investigators may search among the commingled records to isolate those records that are called for by the warrant.

The Supreme Court has noted that in a search of commingled records, "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." Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976). Therefore, "responsible officials, including judicial officials, must take care to assure that [these searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy." Id.

Following on the acknowledgement in *Andresen* that "innocuous" documents can be "cursorily" examined, courts have set forth guidelines for agents review of commingled records to find documents that fall within the scope of a warrant. The leading case is United States v. Heldt, which allows a "brief perusal" of each document, and requires that "the perusal must cease at the point of which the warrant's inapplicability to each document is clear." United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1982); see also United States v. Rude, 88 F.3d 1538, 1552 (9th Cir. 1996); United States v. Giannetta, 909 F.2d 571, 577 (1st Cir. 1990) ("the police may look through . . . file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the documentary items to be seized"); United States v. Slocum, 708 F.2d 587, 604 (11th Cir. 1983); United States v. Ochs, 595 F.2d 1247, 1258 (2d. Cir. 1979) ("some perusal, generally fairly brief."). If a document falls outside the warrant but nonetheless is incriminating, *Heldt* allows that document's "seizure" only if during that brief perusal the document's "otherwise incriminating character becomes obvious." Heldt, 668 F.2d at 1267.

Similar reasoning has been applied to computer searches. See United States v. Khanani, 502 F.3d 1281, 1290 (11th Cir. 2007) (endorsing a search in which "a computer examiner eliminated files that were unlikely to contain material within the warrants' scope"); Manno v. Christie, 2008 WL 4058016, at *4 (D.N.J. Aug. 22, 2008) (finding it "reasonable for [Agent] to briefly review each electronic document to determine if it is among the materials authorized by the warrant, just as he could if the search was only of paper files"); United States v. Potts, 559 F. Supp. 2d 1162, 1175-76 (D. Kan. 2008) (warrant did not authorize an overbroad search when it allowed the investigator "to search the computer by . . . opening or cursorily reviewing the first few 'pages' of such files in order to determine the precise content" (internal quotation marks removed)); United States v. Fumo, 2007 WL 3232112, at *6 (E.D. Pa. Oct. 30, 2007) ("search protocols and keywords do not mark the outer bounds of a lawful search; to the contrary, because of the nature of computer files, the government may legally open and briefly examine each file when searching a computer pursuant to a valid warrant"); United States v. Scarfo, 180 F. Supp. 2d 572, 578 (D.N.J. 2001) (in holding that a key stroke logger could be used to obtain a passphrase even though it would capture other keystrokes, noting that "law enforcement officers must be afforded the leeway to wade through a potential morass of information in the target location to find the particular evidence which is properly specified in the warrant"). When it becomes necessary for an investigator to personally examine a computer file to determine whether it falls within the scope of the warrant, the investigator should take all necessary steps to analyze the file thoroughly, but the investigator should cease the examination of that file as soon as it becomes clear that the warrant does not apply to that file.

Some older cases appear to suggest that when agents executing a search encounter commingled records, they should seize the records, and then seek additional approval from the magistrate before proceeding. For example, the Ninth Circuit, writing about a search of paper files in an age before computer searches were common, suggested that in the "comparatively rare instances" where "documents are so intermingled that they cannot feasibly be sorted on site," law

enforcement "can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search." United States v. Tamura, 694 F.2d 591, 595-596 (9th Cir. 1982). The Tenth Circuit suggested in dicta that the same procedure might be followed for computer searches. See United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) ("the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents"). Both courts, however, have subsequently clarified that a procedure in which the initial warrant establishes the criteria for off-site review is sufficient. See United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (affidavit that establishes "why it was necessary to seize the entire computer system" and "justified taking the entire system off site," with magistrate approval, "makes inapposite United States v. Tamura"); United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005) ("we have not required a specific prior authorization along the lines suggested in Carey in every computer search").

3. Analysis Using Forensic Software

Provided the forensic examiner is attempting to find data that is responsive to the warrant, the Fourth Amendment does not limit the techniques an examiner may use to examine a hard drive.

"[A] computer search may be as extensive as reasonably required to locate the items described in the warrant." United States v. Grimmett, 439 F.3d 1263, 1270 (10th Cir. 2006). So long as the forensic examiner is attempting to find data that is responsive to the warrant, the Fourth Amendment does not restrain the techniques an examiner uses. The use of forensic software, no matter how "sophisticated," also does not affect Fourth Amendment analysis. Cf. United States v. Long, 425 F.3d 482, 487 (7th Cir. 2005) (noting in consent search case that "it is impossible to search computer hardware or software without using some type of software," and "[t]he fact that the Encase search engine [is] sophisticated is of no importance.").

Even if a defendant has taken steps to conceal evidence on a hard drive, a forensic review that nonetheless uncovers it does not invade a reasonable expectation of privacy so long as the warrant permitted a search of the hard drive for that evidence. For example, reading the contents of deleted files by examining unallocated space on the disk has been upheld. See United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) ("recovery [by law enforcement of unlawful images] after attempted destruction, is no different than decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note").

4. Changes of Focus and the Need for New Warrants

A single computer can be involved in several types of crimes, so a computer hard drive might contain evidence of several different crimes. When an agent searches a computer under the authority of a warrant, however, the warrant will often authorize a search of the computer only for evidence of certain specified crimes. If the agent comes across evidence of a crime that is not identified by the warrant, it may be a 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), *and* 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).

The Tenth Circuit has subsequently characterized *Carey* as "simply stand[ing] for the proposition that law enforcement may not expand the scope of a search beyond its original justification." United States v. Grimmett, 439 F.3d 1263, 1268 (10th Cir. 2006). *Grimmett*, then, shifts the analysis away from the agent's subjective intent and toward what the warrant justified. Notably, *Carey*'s focus on the agent's subjective intent reflects a somewhat outdated view of the Fourth Amendment. The Supreme Court has declined to examine an agent's subjective intent and instead has focused on whether the circumstances, viewed objectively, justified the agent's conduct. See, e.g., Brigham City v. Stuart, 547 U.S. 398, 404 (2006) ("An action is 'reasonable' under the Fourth Amendment, regardless of the individual officer's state of mind, as long as the circumstances, viewed objectively, justify the action.") (internal quotation marks removed); 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.

Under an objective standard for agents' conduct, there is inherent tension between *Carey* and cases such as Hill, 322 F. Supp. 2d at 1090, which recognized that "[t]here is no way to know what is in a file without examining its contents." This fact, combined with the principle that "[a] container that may conceal the object of a search authorized by a warrant may be opened immediately," United States v. Ross, 456 U.S. 798, 823 (1982), suggests that it should not be necessary to seek a second warrant after discovering evidence of a separate crime. As the court explained in Gray, 78 F. Supp. 2d at 531 n.11, "[a]rguably, [the agent] could have continued his systematic search of defendant's computer files pursuant to the first search warrant, and, as long as he was searching for the items listed in the warrant, any child pornography discovered in the course of that search could have been seized under the 'plain view' doctrine." Nevertheless,

Carey has not been overruled, so it remains prudent to seek a second warrant upon discovering evidence of an additional crime not identified in the initial warrant.

5. Permissible Time Period for Examining Seized Media

Neither the Fourth Amendment nor Rule 41 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, subject only to the reasonableness requirement of the Fourth Amendment, and the reasonableness of the government's search is determined primarily by whether probable cause for the search has dissipated. The absence of a specific time frame for forensic examination is confirmed by a new amendment to Rule 41(e), which is scheduled to take effect (assuming no contrary congressional action) on December 1, 2009:

A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Courts have agreed that neither the Fourth Amendment nor Rule 41 places explicit limits on the duration of any of forensic analysis, and courts have upheld forensic analyses begun months after investigators acquire a computer or data. See United States v. Burns, 2008 WL 4542990, at *8-9 (N.D. Ill. Apr. 29, 2008) (ten month delay); United States v. Gorrell, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (ten month delay); United States v. Hernandez, 183 F. 3d 468, 480 (D.P.R. 2002) (six week delay); United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 66 (D. Conn. 2002); cf. United States v. New York Tel. Co., 434 U.S. 159, 169 n.16 (1977) (applying Fourth Amendment standards to pen registers before the enactment of the pen register act, holding that "the requirement that the search be conducted within 10 days of its issuance does not mean that the duration of a pen register surveillance may not exceed 10 days").

The Fourth Amendment does require that forensic analysis of a computer be conducted within a reasonable time. See United States v. Mutschelknaus, 564 F. Supp. 2d 1072, 1077 (D.N.D. 2008) ("[T]he Federal Rules of Criminal Procedure do not require that the forensic analysis of computers and other electronic equipment take place within a specific time limit. Any subsequent search only needs to be conducted within a reasonable time."); *Burns*, 2008 WL 4542990, at *8 ("A delay must be reasonable, but there is no constitutional upper limit on reasonableness."); United States v. Grimmett, 2004 WL 3171788, at *5 (D. Kan. Aug. 10, 2004), *aff'd* 439 F.3d 1263 (10th Cir. 2006). In judging the reasonableness of time for forensic analysis, courts may recognize that analysis of computers is a difficult and time-consuming process. See Triumph Capital Group, Inc., 211 F.R.D. at 66 (finding that time to complete search reasonable because "computer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation and a greater degree of care in their execution").

Importantly, courts usually treat the dissipation of probable cause as the chief measure of the "reasonableness" of a search's length under the Fourth Amendment. For example, in United States v. Syphers, 426 F.3d 461 (1st Cir. 2005), the First Circuit stated that the Fourth Amendment "contains no requirements about *when* the search or seizure is to occur or the *duration*," but cautioned that "unreasonable delay in the execution of a warrant that results in the lapse of probable cause will invalidate a warrant." Id. at 469 (quotations omitted). See *Burns*, 2008 WL 4542990 at *9 (upholding search despite "lengthy" delay because "Burns does not assert that the time lapse affected the probable cause to search the computer (nor could he, given that suspected child pornography had already been found on the hard drive), that the government has acted in bad faith, or that he has been prejudiced in any way by the delay"). Significantly, dissipation of probable cause is unlikely in computer search cases because evidence is "frozen in time" when storage media is imaged or seized. Triumph Capital Group, Inc., 211 F.R.D. at 66.

A few magistrate judges have taken a different view, however, and 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.[1]

Prosecutors should oppose such limitations. The law does not expressly authorize magistrate judges to issue warrants that impose time limits on law enforcement's examination of seized evidence, and the authority of magistrates to impose such limits is open to question, especially in light of the forthcoming amendment to Rule 41 stating that the time for executing a warrant "refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." 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 encountering this issue may contact CCIPS at (202) 514-1026 for further assistance.

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.). Similarly, the Fourth Amendment requires only reasonableness, and courts have rejected challenges based on claims of delay, as discussed above. This incongruity is especially true when the hardware to be searched is a container of contraband child pornography, and it is therefore subject to forfeiture and will not be returned.

The use of the exclusionary rule to police delays by forensic examiners is even more questionable after Hudson v. Michigan, 547 U.S. 586 (2006). In Hudson, in which the Supreme Court rejected a suppression remedy for violation of the knock-and-announce rule, the Court held that "but-for causality is only a necessary, not a sufficient, condition for suppression." Id. at 592. In rejecting suppression, the Court also relied on the conclusion that suppression would not "vindicate the interests protected by the [constitutional] requirement [at issue]," id. at 593, and that "the exclusionary rule has never been applied" when its "substantial social costs" outweigh its deterrent benefits. Id. (citation omitted).

6. Contents of Rule 41(f) Inventory Filed With the Court

Officers should file inventories with returns that simply indicate the hardware devices that were seized.

Rule 41(f) requires an officer executing a warrant to "prepare and verify an inventory of any property seized," and to "return [the warrant]together with a copy of the inventoryto the magistrate judge designated on the warrant," Fed. R. Crim. P. 41(f)(1)(B), (D). Currently, "[t]he Rules do not dictate a requisite level of specificity for inventories of seized items," and whether an inventory is sufficiently specific is a question of fact. In re Searches of Semtex Indus. Corp., 876 F. Supp. 426, 429 (E.D.N.Y. 1995). When documents are seized, an inventory listing each of them is not required; such "specificity and particularization would not seem to be called for even under an extreme construction of Rule 41" in light of its requirement that an inventory be "promptly" filed with the magistrate. United States v. Birrell, 269 F. Supp. 716, 722 (S.D.N.Y. 1967).

Thus, in computer cases, officers have typically filed inventories with returns that simply indicate the information or hardware devices that were seized, such as "image of one Maxtor 500 gigabyte hard drive." This approach has been adopted in a new amendment to Rule 41(f), which is scheduled to take effect (assuming no contrary congressional action) on December 1, 2009.

The new rule specifies that "[i]n a case involving the seizure of electronic storage media or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied."

Courts have also held that when the government seizes documents or data, providing defendants with "a copy of everything seized" has been held to "obviate[] the need for a detailed inventory." United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 66 (D. Conn. 2002); United States v. Ogden, 2008 WL 2247074, at *13 (W.D. Tenn. May 28, 2008) (rejecting suppression motion based on failure to provide a timely inventory of a computer search "[b]ecause the Defendant has had access to the seized files, has personal knowledge of the files, and was recently given a list of the files"). Providing defendants with "access" to paper records seized from an office also "obviates the need for a more detailed inventory" beyond one that simply identifies which file cabinets were seized. Semtex, 876 F. Supp. at 429-30.

E. Challenges to the Search Process

1. Challenges Based on "Flagrant Disregard"

Defense counsel will sometimes attempt to use the seizure of storage media or commingled information 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. Khanani, 502 F.3d 1281, 1289 (11th Cir. 2007); 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).

As discussed above in Section C.3, for practical and technical reasons, agents executing computer searches frequently must seize hardware or files beyond those described in the warrant. Defense lawyers sometimes 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. Gawrysiak, 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 an attempt 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 they routinely approve off-site searches despite the incidental seizure of additional property. See, e.g., United States v. Hill, 459

F.3d 966, 974-75 (9th Cir. 2006) ("the officers would have to examine every one of what may be thousands of files on a diska process that could take many hours and perhaps days"); 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); = ("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.").

2. Motions for Return of Property

Rule 41(g) allows an "aggrieved" person to move for the property's return. Fed. R. Crim. P. 41(g). This rule 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 State Devices, Inc., 130 F.3d 853, 855-56 (9th Cir. 1997). Rule 41(g) 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(g) 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 email. 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(g) 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 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(g)). 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(g) (quoted in Ramsden, 2 F.3d at 326); see also In re Search of Law Office, 341 F.3d 404, 413-14 (5th Cir. 2003) ("Rule 41(e) does not permit a district court to order complete suppression of seized evidence absent, at the very least, a substantial showing of irreparable harm").

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, e.g., In re Search of 5444 Westheimer Road, 2006 WL 1881370, at *2 (S.D. Tex. Jul. 6, 2006) (declining to exercise jurisdiction over a claim for pre-indictment return of property when government had provided copies of seized computer data); 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. Aug. 25, 1999) (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(g) 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").

Legal Limitations on the Use of Search Warrants to Search Computers

In general, so long as the proper procedures are followed, the government may execute a search warrant against any individualincluding individuals not themselves suspected of crimes--if there is probable cause to believe that the search will reveal contraband or evidence of a crime. See Zurcher v. Stanford Daily, 436 U.S. 547 (1978); Warden v. Hayden, 387 U.S. 294, 309 (1967). Yet in a few circumstances, Congress and the Attorney General have limited the situations in which criminal investigators can use search warrants to obtain evidence. Three of these limitations apply with special force to the field of computer searches.

1. Journalists and Authors: 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 Internet, 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 materials that relate to the freedom of expression. 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

When deciphering the inscrutable text of the PPA, it can be helpful to understand the context in which it was enacted. 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 the "mental impressions, conclusions, or theories" of their 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).

In these situations, the government is required to use a subpoena or other compulsory process rather than use a search warrant, unless a PPA exception applies.

The PPA protects a broad set of actors. It is not limited to journalists: it has been used by a publisher of role-playing games, see Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), and a publisher of an "internet-based journal," although the latter's claim was dismissed on other grounds. See Mink v. Suthers, 482 F.3d 1244, 1257-58 (10th Cir. 2007).

The PPA contains several important exceptions:

Contraband. The PPA does not apply to "contraband or the fruits of a crime or things otherwise criminally possessed, or property designed or intended for use, or which is or has been used as, the means of committing a criminal offense." 42 U.S.C. § 2000aa-7(a), (b).

Criminal suspect. The PPA does not apply if "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," although the statute sets forth a further exception to this exception in certain circumstances where the offense "consists of the receipt, possession, communication, or withholding" of the targeted materials. See 42 U.S.C. §§ 2000aa(a)(1), 2000aa(b)(1); Guest v. Leis, 255 F.3d 325, 342 (6th Cir. 2001); DePugh v. Sutton, 917 F. Supp. 690, 696 (W.D. Mo. 1996) ("The P.P.A. clearly allows the government to depart from the requirements of the Act in those instances in which the person suspected of a crime is in possession of documents related to the crime."). Materials may "relate" to an offense even when the relations are somewhat remote. For example, in S.H.A.R.K. v. Metro Parks Serving Summit County, 499 F.3d 553 (6th Cir. 2007), animal rights activists placed hidden cameras on trees to document planned extermination of deer. The removal (and seizure) of those cameras did not violate the PPA, because the cameras were "related" to the crime of trespass necessary to place them there in the first place. Id. at 567.

Emergency. The PPA does not apply if 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).

Subpoena would be inadequate. The PPA does not apply in a search for or seizure of "documentary materials" as defined by §2000aa-7(a), if 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). One court held this exception was met when an incriminating videotape was in the possession of a person who was friends with the person whom the tape would incriminate. See Berglund v. City of Maplewood, 173 F. Supp. 2d 935, 949-50 (D. Minn. 2001).

Importantly, these exceptions are exceptions to the PPA only, not to Fourth Amendment protections in general. When a PPA exception applies, it means only that the government may apply for a warrant it does not mean that the government may proceed to search without a warrant. See DePugh v. Sutton, 917 F. Supp. 690, 696 (W.D. Mo. 1996).

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 would have been difficult to foresee when Congress enacted it in 1980. First, the use of personal computers for publishing and the Internet 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 Zurcher v. Stanford Daily, 436 U.S. 547 (1978). For example, the "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 might 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 S.H.A.R.K. v. Metro Parks Serving Summit County, 499 F.3d 553, 567 (6th Cir. 2007) (seizure of video cameras placed by trespassers did not violate PPA because cameras were related to the crime of trespass);

Carpa v. Smith, 2000 WL 189678, at *1 (9th Cir. Feb. 15, 2000) ("[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).[2] 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 email, 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 the SCA 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. 1994) (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 from a non-suspect 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 CHIP in their district (see Introduction, p. xii) for more specific guidance.

2. 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 Third Party 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 Attorneys' Manual, and should consult OEO at (202) 514-6809. See generally United States Attorneys' 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 examine the computer to determine which files contain privileged material. After reviewing the files, the third party will offer those files that are not privileged 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 "filter team" or "taint team" to help execute the search and review the files afterwards. The filter team sets up a so-called "ethical wall" between the evidence and the prosecution team, permitting only unprivileged files to pass over 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 filter team and a special master. Most prosecutors will prefer to use a filter team if the court consents. A filter team can usually review 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 filter teams. See In re Grand Jury Subpoenas, 454 F.3d 511, 522-23 (6th Cir. 2006) (approving of use of filter teams in connection with search warrants while disapproving of their use in connection with grand jury subpoenas); 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 filter 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 filter 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 filter 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 material is provided to the prosecution team.

In unusual circumstances, the court may conclude that a filter 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 neutral technical expert to assist in sorting, identifying, and analyzing digital evidence for the reviewing process.

3. Other Disinterested Third Parties

In addition to the more specific restrictions on using a search warrant to obtain information from disinterested publishers, lawyers, physicians, and clergymen, Department of Justice policy favors the use of a subpoena or other less intrusive means to obtain evidence from disinterested third parties, unless use of those less intrusive means would substantially jeopardize the availability or usefulness of the materials sought. See 28 C.F.R. §59.4(a)(1); United States Attorneys' Manual, §9-19.210. Except in emergencies, the application for such a warrant must be authorized by an attorney for the government. See 28 C.F.R. §59.4(a)(2); United States Attorneys' Manual, §9-19.210. Importantly, however, failure to comply with this policy "may not be litigated, and a court may not entertain such an issue as the basis for the suppression or exclusion of evidence." 28 C.F.R. §59.5(b).

4. Communications Service Providers: the SCA

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.

One category of disinterested third party often encountered in the computer context is Internet service providers. The Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712, governs law enforcement access to the contents of electronic communications stored by third-party service providers. See Chapter 3, *infra* (discussing the SCA). In most cases, law enforcement officials should use the compulsory process provisions of § 2703 to compel a service provider to disclose information; when possible, law enforcement officials should avoid physical execution of a Rule 41 search warrant on service providers. When law enforcement officers execute a Rule 41 search warrant on an Internet service provider and seize the accounts of customers and subscribers, those customers and subscribers may bring civil actions claiming that the search violated the SCA. In addition, the SCA 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 text of the SCA does not appear to contemplate civil liability for searches and seizures authorized by valid Rule 41 search warrants: the SCA 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). Nonetheless, Steve Jackson Games, Inc. v. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), raised the concern that a search executed pursuant to a valid warrant might violate the SCA. In Steve Jackson Games, the district court held the Secret Service liable under the SCA 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 the SCA requires that search warrants also comply with 18 U.S.C. § 2703(b)(1)(A) and the various notice requirements of § 2703. See id. In fact, the SCA makes quite clear that § 2703(d) and the notice requirements of § 2703 are implicated only when law enforcement does not obtain a search warrant.[3] Compare 18 U.S.C. §2703(b)(1)(A), with 18 U.S.C. §2703(b)(1)(B). Further, objectively reasonable good faith reliance on a warrant, court order, or statutory authorization is a complete defense to an SCA violation. See 18 U.S.C. §2707(e). Compare Gracey, 111 F.3d at 1484 (applying good faith defense because seizure of stored communications incidental to a valid search was objectively reasonable), with 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 the SCA 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 every computer search, agents should strive to avoid unwarranted intrusions into private areas, and searches of service providers are no different. See Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) ("responsible officials, including judicial officials, must take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy."). In most cases, investigators will want to avoid a wholesale search and seizure of the provider's computers by relying instead on compulsory process served on the provider consistent with the SCA. When investigators have no choice but to execute the search, such as where the service provider lacks the ability or will to comply with compulsory process or is suspected of involvement in the criminal conduct, agents must search the provider's computers themselves. Because each of the provider's computers might contain records relating to users who are wholly unrelated to the criminal investigation, special procedures designed to uphold those users' privacy interests may be appropriate. For example, agents might inform the magistrate judge in the search warrant affidavit that they will take steps to ensure the confidentiality of the accounts and not expose their contents to human inspection. 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 SCA 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 SCA 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").

1 When the computer does not contain contraband (such as child pornography), this specific concern can usually be addressed by imaging the computer, returning it promptly, and later taking as much time as necessary to conduct the forensic exam on the image copy.

2 The Steve Jackson Games litigation raised many important issues involving the PPA and the SCA 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*.

3 This raises a fundamental distinction overlooked in Steve Jackson Games: the difference between a search warrant issued under Rule 41 that law enforcement executes with a physical search, and a search warrant issued under the SCA that law enforcement executes by compelling a provider of electronic communication service or remote computing service to disclose the contents of a subscriber's network account. Although both are search warrants, they are different in practice. This distinction is especially important when a court concludes that the SCA was violated and then must determine the remedy because there is no statutory suppression for nonconstitutional violations of the SCA. See 18 U.S.C. § 2708; Chapter 3.I, *infra* (discussing remedies for violations of the SCA).

Chapter 3

The Stored Communications Act

A. Introduction

The SCA regulates how the government can obtain stored account information from network service providers such as ISPs. Whenever agents or prosecutors seek stored email, account records, or subscriber information from a network service provider, they must comply with the SCA. The SCA's classifications are summarized in the chart that appears in Section F of this chapter.

The Stored Communications Act, 18 U.S.C. §§ 2701-2712 ("SCA"), sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers.[1] There are three main substantive components to this system, which serves to protect and regulate the privacy interests of network users with respect to government, network service providers, and the world at large. First, § 2703 creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications from network service providers. Second, § 2702 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-government entities. Third, § 2701 prohibits unlawful access to certain stored communications; anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties.

The structure of the SCA 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 the content of stored emails 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, the SCA 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 subpoena; other information requires a special court order; and still other information requires a search warrant. In addition, some types of legal process require notice to the subscriber, while other types do not.

Agents and prosecutors must apply the various classifications devised by the SCA'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 service 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 non-content record pertaining to a subscriber, or other information enumerated by the SCA). 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 Section F of this chapter provides a useful way to apply these distinctions in practice.

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

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

The SCA protects communications held by two defined classes of network service providers: providers of "electronic communication service," see 18 U.S.C. § 2510(15), and providers of "remote computing service," see 18 U.S.C. § 2711(2). Careful examination of the definitions of these two terms is necessary to understand how to apply the SCA.

1. 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.D.2.) For example, "telephone companies and electronic mail companies" generally act as ECS providers. See S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568; Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900-03 (9th Cir. 2008) (text messaging service provider is an ECS); In re Application of United States, 509 F. Supp. 2d 76, 79 (D. Mass. 2007) (cell phone service provider is an ECS); Kaufman v. Nest Seekers, LLC, 2006 WL 2807177, at *5 (S.D.N.Y. Sept. 26, 2006) (host of electronic bulletin board is ECS); Freedman v. America Online, Inc., 325 F. Supp. 2d 638, 643 n.4 (E.D. Va. 2004) (AOL is an ECS).

Any company or government entity that provides others with the means to communicate electronically can be a "provider of electronic communication service" relating to the communications it provides, regardless of the entity's primary business or function. See Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114-15 (3d Cir. 2004) (insurance company that provided email service to employees is an ECS); Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (city providing pager service to its police officers was a provider of ECS); 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 ECS). In In re Application of United States, 349 F.3d 1132, 1138-41 (9th Cir. 2003), the Ninth Circuit held that a company operating a system that enabled drivers to communicate with designated call centers over a cellular telephone network was an ECS, though it also noted that the situation would have been entirely different "if the Company merely used wire communication as an incident to providing some other service, as is the case with a street-front shop that requires potential customers to speak into an intercom device before permitting entry, or a 'drive-thru' restaurant that allows customers to place orders via a two-way intercom located beside the drive-up lane." Id. at 1141 n.19.

A provider 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 email of users of another company's bulletin board service was not a provider of electronic communication service); State Wide Photocopy, Corp. 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 a provider of ECS. For example, a commercial website is not a provider of ECS, 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. See also United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) (a home computer connected to the Internet is not an ECS); In re Jetblue Airways Corp. Privacy Litigation, 379 F. Supp. 2d 299, 309-10 (E.D.N.Y. 2005) (airline that operated website that enabled it to communicate with customers was not an ECS); Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) (ECS "does not encompass businesses selling traditional products or services online"); In re Doubleclick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 508-09 (S.D.N.Y. 2001) (distinguishing ISPs that provide ECS from websites that are users of ECS). However, "an online business or retailer may be considered an electronic communication service provider if the business has a website that offers customers the ability to send messages or communications to third parties." Becker v. Toca, 2008 WL 4443050, at *4 (E.D. La. Sept. 26, 2008).

2. Remote Computing Service

The term "remote computing service" ("RCS") is defined by 18 U.S.C. § 2711(2) as "the 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 allows customers to use its computing facilities in "essentially a time-sharing arrangement" provides an RCS. H.R. Rep. No. 99-647, at 23 (1986). A server that allows users to store data for future retrieval also provides an RCS. See Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432, 442-43 (W.D. Tex. 1993) (provider of bulletin board services was a remote computing service), aff'd on other grounds, 36 F.3d 457 (5th Cir. 1994). Importantly, an entity that operates a website and its associated servers is not an RCS, unless of course the entity offers a storage or processing service through the website. For example, an airline may compile and store passenger information and itineraries through its website, but these functions are incidental to providing airline reservation service, not data storage and processing service; they do not convert the airline into an RCS. See In re Jetblue Airways Corp. Privacy Litigation, 379 F. Supp. 2d at 310; see also United States v. Standefer, 2007 WL 2301760, at *5 (S.D. Cal. Aug. 8, 2007) (holding that e-gold payment website was not an RCS because e-gold customers did not use the website "to simply store electronic data" or to "outsource tasks," but instead used e-gold "to transfer gold ownership to other users").

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, Verizon is a provider to the public: anyone can obtain a Verizon account. (It may seem odd at first that a service can charge a fee but still be considered available "to the public," but this approach 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 available only to those with a special relationship with the provider do not provide service to the public. For example, an employer that provides email accounts to its employees will not be an RCS with respect to those employees, because such email accounts are not available to the public. See Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (interpreting the "to the public" clause in § 2702(a) to exclude an internal email system that was made available to a hired contractor but was not available to "any member of the community at large").

In Quon v. Arch Wireless Operating Co., the Ninth Circuit held that a text messaging service provider was an ECS and therefore not an RCS. See Quon, 529 F.3d at 902-03. However, this "either/or" approach to ECS and RCS is contrary to the language of the statute and its legislative history. The definitions of ECS and RCS are independent of each other, and therefore nothing prevents a service provider from providing both forms of service to a single customer. In addition, an email service provider is certainly an ECS, but the House report on the SCA also stated that an email stored after transmission would be protected by a provision of the SCA that protects contents of communications stored by an RCS. See H.R. Rep. No. 99-647, at 65 (1986). One subsequent court has rejected the Ninth Circuit's analysis in Quon and stated that a provider "may be deemed to provide both an ECS and an RCS to the same customer." Flagg, v. City of Detroit, 252 F.R.D. 346, 362 (E.D. Mich. 2008). The key to determining whether the provider is an ECS or RCS is to ask what role the provider has played and is playing with respect to the communication in question.

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 range of information that an ISP may typically store regarding one of its customers. It may have the customer's subscriber information, such as name, address, and credit card number. It may have logs revealing when the customer logged on and off the service, the IP addresses assigned to the customer, and other more detailed logs pertaining to what the customer did while online. The ISP may also have the customer's opened, unopened, draft, and sent emails.

When agents and prosecutors wish to obtain such records, they must be able to classify these types of information using the language of the SCA. The SCA breaks the information down into three categories: (1) contents; (2) non-content records and other information pertaining to a subscriber or customer; and (3) basic subscriber and session information, which is a subset of non-content records and is specifically enumerated in 18 U.S.C. § 2703(c)(2). See 18 U.S.C. §§ 2510(8), 2703. In addition, as described below, the SCA creates substantially different protections for contents in "electronic storage" in an ECS and contents stored by a provider of RCS.

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

Section 2703(c)(2) lists the categories of basic subscriber and session 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. In the Internet context, "any temporarily assigned network address" includes the IP address used by a customer for a particular session. For example, for a webmail service, the IP address used by a customer accessing her email account constitutes a "temporarily assigned network address." This list does not include other, more extensive transaction-related records, such as logging information revealing the email addresses of persons with whom a customer corresponded.

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

Section 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 and session information described in the previous section. As one court explained, "a record means something stored or archived. The term information is synonymous with data." In re United States, 509 F. Supp. 2d 76, 80 (D. Mass. 2007).

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 email 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. See also In re Application of United States, 509 F. Supp. 76, 80 (D. Mass. 2007) (historical cell-site information fall within scope of § 2703(c)(1)); 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 the SCA); Hill v. MCI WorldCom Commc'ns, Inc., 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," not contents, for a telephone account); Jessup-Morgan v. America Online, Inc., 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (holding that a customer's identification information is a "record or other information pertaining to a subscriber" rather than contents). According to the legislative history of the 1994 amendments to § 2703(c), the purpose of separating the basic subscriber and session information from other non-content records was to distinguish basic subscriber and session information from more revealing transactional information that could contain a "person's entire on-line profile." H.R. Rep. No. 103-827, at 17, 31-32 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3497, 3511-12.

3. Contents and "Electronic Storage"

The contents of a network account are the actual files (including email) 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 emails or voice mails are "contents," as are word processing files stored in employee network accounts. The subject lines of emails are also contents. Cf. Brown v. Waddell, 50 F.3d 285, 292 (4th Cir. 1995) (noting that numerical pager messages allow "an unlimited range of number-coded substantive messages" in the course of holding that the interception of pager messages requires compliance with Title III).

The SCA further divides contents into two categories: contents in "electronic storage" held by a provider of electronic communication service, and contents stored by a remote computing service. (In addition, contents that fall outside of these two categories are not protected by the SCA.) Importantly, "electronic storage" is a statutorily defined term. It does *not* simply mean storage of information by electronic means. Instead, "electronic storage" is "(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." 18 U.S.C. § 2510(17). Moreover, the definition of "electronic storage" is important because, as explained in Section D below, contents in "electronic storage" for less than 181 days can be obtained only with a warrant.

Unfortunately, as a result of the Ninth Circuit's decision in Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004), there is now a split between two interpretations of "electronic storage"--a traditional narrow interpretation and an expansive interpretation supplied by the Ninth Circuit.

Both interpretations are discussed below. As a practical matter, federal law enforcement within the Ninth Circuit is bound by the Ninth Circuit's decision in Theofel, but law enforcement elsewhere may continue to apply the traditional interpretation of "electronic storage."

As traditionally understood, "electronic storage" refers only to temporary storage made in the course of transmission by a service provider and to backups of such intermediate communications made by the service provider to ensure system integrity. It does not include post-transmission storage of communications. For example, email 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 communication is stored as a temporary and intermediate measure pending the recipient's retrieval of the communication from the service provider. Once the recipient retrieves the email, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the accessed communication, the copy will not be in "temporary, intermediate storage" and is not stored incident to transmission. See Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2004) (stating that email in post-transmission storage was not in "temporary, intermediate storage"). By the same reasoning, if the sender of an email maintains a copy of the sent email, the copy will not be in "electronic storage." Messages posted to an electronic "bulletin board" or similar service are also not in "electronic storage" because the website on which they are posted is the final destination for the information. See Snow v. DirecTV, Inc., 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005), adopted by 2005 WL 1266435 (M.D. Fla. May 27, 2005), aff'd on other grounds, 450 F.3d 1314 (11th Cir. 2006).

Furthermore, the "backup" component of the definition of "electronic storage" refers to copies made by an ISP to ensure system integrity. As one district court explained, the backup component "protects the communication in the event the system crashes before transmission is complete. The phrase 'for purposes of backup protection of such communication' in the statutory definition makes clear that messages that are in post-transmission storage, after transmission is complete, are not covered by part (B) of the definition of 'electronic storage.'" Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), aff'd in part on other grounds, 352 F.3d 107, 114 (3d Cir. 2004) (affirming the SCA portion of the district court's ruling on other grounds); see also United States v. Weaver, 2009 WL 2163478, at *4 (C.D. Ill. July 15, 2009) (interpreting "electronic storage" to exclude previously sent email stored by web-based email service provider); In re Doubleclick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 511-13 (S.D.N.Y. 2001) (emphasizing that "electronic storage" should have a narrow interpretation based on statutory language and legislative intent and holding that cookies fall outside of the definition of "electronic storage" because of their "long-term residence on plaintiffs' hard drives"); H.R. Rep. No. 99-647, at 65 (1986) (noting congressional intent that opened email left on a provider's system be covered by provisions of the SCA relating to remote computing services, rather than provisions relating to communications in "electronic storage").

This narrow interpretation of "electronic storage" was rejected by the Ninth Circuit in Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004), in which the court held that email messages were in "electronic storage" regardless of whether they had been previously accessed, because it concluded that retrieved email fell within the backup portion of the definition of "electronic

storage." Id. at 1075-77. Although the Ninth Circuit did not dispute that previously accessed email was not in temporary, intermediate storage within the meaning of § 2510(17)(A), it insisted that a previously accessed email message fell within the scope of the "backup" portion of the definition of "electronic storage," because such a message "functions as a 'backup' for the user." Id. at 1075. However, CCIPS has consistently argued that the Ninth Circuit's broad interpretation of the "backup" portion of the definition of "electronic storage" should be rejected. There is no way for a service provider to determine whether a previously opened email on its servers is a backup for a copy of the email stored by a user on his computer, as the service provider simply cannot know whether the underlying email remains stored on the user's computer. Essentially, the Ninth Circuit's reasoning in Theofel confuses "backup protection" with ordinary storage of a file.

Although prosecutors within the Ninth Circuit are bound by Theofel, law enforcement elsewhere may continue to apply the traditional narrow interpretation of "electronic storage," even when the data sought is within the Ninth Circuit. Recent lower court decisions addressing the scope of "electronic storage" have split between the traditional interpretation and the Theofel approach. Compare United States v. Weaver, 2009 WL 2163478, at *4 (C.D. Ill. July 15, 2009) (rejecting Theofel), and Bansal v. Russ, 513 F. Supp. 2d 264, 276 (E.D. Pa. 2007) (holding that access to opened email in account held by non-public service provider did not violate the SCA), with Bailey v. Bailey, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (endorsing Theofel), and Cardinal Health 414, Inc. v. Adams, 482 F. Supp. 2d 967, 976 n.2 (M.D. Tenn. 2008) (same). Prosecutors confronted with Theofel-related issues should consult CCIPS at (202) 514-1026 for further assistance.

4. Illustration of the SCA's Classifications in the Email Context

An example illustrates how the SCA's categories work in practice outside the Ninth Circuit, where Theofel does not apply. Imagine that Joe sends an email from his account at work ("joe@goodcompany.com") to the personal account of his friend Jane ("jane@localisp.com"). The email 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 email is in "electronic storage." Once Jane retrieves Joe's email, she can either delete the message from LocalISP's server or else leave the message stored there. If Jane chooses to store the email with LocalISP, LocalISP is now a provider of RCS (and not ECS) with respect to the email sent by Joe. The role of LocalISP has changed from a transmitter of Joe's email to a storage facility for a file stored remotely for Jane by a provider of RCS.

Next imagine that Jane responds to Joe's email. Jane's return email to Joe will stream across the Internet to the servers of Joe's employer, Good Company. Before Joe retrieves the email from Good Company's servers, Good Company is a provider of ECS with respect to Jane's email (just like LocalISP was with respect to Joe's original email before Jane accessed it). When Joe accesses Jane's email message and the communication reaches its destination (Joe), Good Company ceases to be a provider of ECS with respect to that email (just as LocalISP ceased to be a provider of ECS with respect to Joe's original email when Jane accessed it). Unlike LocalISP, however, Good Company does not become a provider of RCS if Joe decides to store the opened

email 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 email in Joe's account, the SCA no longer regulates access to this email, and such access is governed solely by the Fourth Amendment. Functionally speaking, the opened email in Joe's account drops out of the SCA.

Finally, consider the status of the other copies of the emails in this scenario: Jane has downloaded a copy of Joe's email from LocalISP's server to her personal computer at home, and Joe has downloaded a copy of Jane's email from Good Company's server to his office desktop computer at work. The SCA governs neither. Although these computers contain copies of emails, these copies are not stored on the server of a third-party provider of RCS or ECS, and therefore the SCA 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. A chart illustrating these issues appears in Section F of this chapter. Sample language that agents may use appears in Appendices B, E, and F.

D. Compelled Disclosure Under the SCA

Section 2703 articulates the steps that the government must take to compel providers to disclose the contents of stored wire or electronic communications (including email and voice mail) and other information such as account records and basic subscriber and session 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 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 the SCA is that greater process generally includes access to information that cannot 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 because it can authorize a broader disclosure. Note, however, the notice requirement must be considered separately 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.

Two circumstances allow the government to compel disclosure of information under the SCA without a subpoena. First, 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). Second, the government may compel a service provider to disclose non-content information pertaining to a customer or subscriber when the government has obtained the customer or subscriber's consent. See 18 U.S.C. § 2703(c)(1)(C).

1. Subpoena

The SCA permits the government to compel disclosure of the basic subscriber and session information (discussed above in Section C.1) listed in 18 U.S.C. § 2703(c)(2) using a subpoena:

(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 the SCA. The hypothetical email exchange between Jane and Joe discussed in Section C of this chapter provides a useful example: Good Company provided neither "remote computing service" nor "electronic communication service" with respect to the opened email on Good Company's server. 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 the SCA did not exist. Similarly, information relating or belonging to a person who is neither a "customer" nor a "subscriber" is not protected by the SCA and may be obtained using a subpoena according to the same rationale. Cf. Organizacion JD Ltda. v. United States Dep't of Justice, 124 F.3d 354, 359-61 (2d Cir. 1997) (discussing the scope of the word "customer" as used in the SCA).

The legal threshold for issuing a subpoena is low. See United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950). Investigators may obtain disclosure pursuant to § 2703(c)(2) using any federal or state grand jury or trial subpoena or an administrative subpoena authorized by a federal or state statute. See 18 U.S.C. § 2703(c)(2). For example, subpoenas authorized by the Inspector General Act may be used. See 5 U.S.C. app. 3 § 6(a)(4). 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). 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 Commc'ns Corp., 196 F.R.D. 559, 561 (N.D. Cal. 2000) (holding that civil 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

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 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); and

3) "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).

Outside the Ninth Circuit (which is now governed by Theofel), this third category will include opened and sent email. Agents outside of the Ninth Circuit can therefore obtain such email (and other stored electronic or wire communications in "electronic storage" more than 180 days) using a subpoena, provided they comply with the SCA's notice provisions. However, in light of Theofel, some service providers may be reluctant to produce opened or sent email less than 181 days old without a warrant. Prosecutors moving to compel compliance with a subpoena for such email should contact CCIPS at (202) 514-1026 for assistance. In the Ninth Circuit, agents can continue to subpoena communications that have been in "electronic storage" over 180 days.

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) permits 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 18 U.S.C. § 2705(a)(2) (defining "adverse result"); 18 U.S.C. § 2705(a)(6) (defining "supervisory official"). This provision of the SCA provides a permissible way for the government to delay notice to the customer or subscriber when notice would jeopardize a pending investigation or endanger the life or physical safety of an individual. The government may extend the delay of notice for additional 90-day periods through additional certifications that meet the "adverse result" standard of section 2705(b). See 18 U.S.C. § 2705(a)(4). Upon expiration of the delayed notice period, 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).

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,

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.

18 U.S.C. § 2703(d).

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, 1109-10 (D. Kan. 2000) (concluding that a conclusory application for a 2703(d) order "did not meet the requirements of the statute."). As the Tenth Circuit has noted, the "specific and articulable facts" standard of 2703(d) "derives from the Supreme Court's decision in [Terry v. Ohio, 392 U.S. 1 (1968)]." United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008). The House Report accompanying the 1994 amendment to section 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 31-32 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3511-12 (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. The SCA 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"); 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 that State to enter orders authorizing the use of a pen register or a trap and trace device"). However, the statute provides that when a state governmental entity seeks a 2703(d) order, the order "shall not issue if prohibited by the law of such State." 18 U.S.C. § 2703(d). Moreover, although the statute explicitly allows federal courts to issue 2703(d) orders to providers outside of the court's district, it is silent on whether state courts have such authority.

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

Investigators can obtain everything associated with an account except for unopened email 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 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); and

3) "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).

As a practical matter, except in the Ninth Circuit, this means that the government can use a 2703(d) order that complies with the prior notice provisions of § 2703(b)(1)(B) to obtain the full contents of a subscriber's account except unopened email and voicemail that have been in the account for 180 days or less. In the Ninth Circuit, which is governed by Theofel, agents can continue to use 2703(d) orders to obtain communications in "electronic storage" over 180 days. Following Theofel, some providers have resisted producing email content less than 181 days old in response to a 2703(d) order, even when the 2703(d) order is issued by a court outside the Ninth Circuit. Prosecutors encountering this problem should contact CCIPS at (202) 514-1026 for assistance.

As an alternative to giving prior notice, law enforcement 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, prosecutors generally will obtain this order by including an appropriate request in the 2703(d) application and proposed order; sample language appears in Appendix B. Prosecutors may also apply to the court for extensions of the delay. See 18 U.S.C. § 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 Section 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). The applicant must satisfy this standard anew in every application for an extension of the delayed notice.

5. Search Warrant

Investigators can obtain everything associated with an account with a search warrant. The SCA 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 § 2703 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 any content or non-content information pertaining to an account by obtaining a search warrant "issued using the procedures described in" Fed. R. Crim. P. 41. 18 U.S.C. § 2703(a).

Search warrants issued under § 2703 have several noteworthy procedural features. First, 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 may be issued by a federal "court with jurisdiction over the offense under investigation," even for records held in another district. See United States v. Berkos, 543 F.3d 392, 396-98 (7th Cir. 2008); In re Search of Yahoo, Inc., 2007 WL 1539971, at *6 (D. Ariz. May 21, 2007); In re Search Warrant, 2005 WL 3844032, at *5-6 (M.D. Fla. 2006) ("Congress intended 'jurisdiction' to mean something akin to territorial jurisdiction"). State courts may also issue warrants under § 2703, but the statute does not give these warrants effect outside the limits of the courts' territorial jurisdiction. Second, obtaining a search warrant obviates the need to give notice to the subscriber. See 18 U.S.C. § 2703(b)(1)(A); Fed. R. Crim. P. 41(f)(1)(C).

Third, 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 specified in the warrant. See 18 U.S.C. § 2703(g) (stating that the presence of an officer is not required for

service or execution of a § 2703 warrant); United States v. Bach, 310 F.3d 1063, 1068 (8th Cir. 2002) (finding search of email by ISP without presence of law enforcement did not violate Fourth Amendment).

Fourth, a two-step process is often used to obtain the content of communications under a § 2703 warrant. First, the warrant directs the service provider to produce all email from within the specified account or accounts. Second, the warrant authorizes law enforcement to review the information produced to identify and copy information that falls within the scope of the particularized "items to be seized" under the warrant.

Otherwise, as a practical matter, § 2703 search warrants are obtained much 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.

E. Voluntary Disclosure

Providers of services not available "to the public" may freely disclose both contents and other records relating to stored communications. The SCA 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 the SCA 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 is whether the relevant service offered by the provider is available "to the public." See Section B, above. If the provider does not provide the applicable service "to the public," then the SCA does not place any restrictions on disclosure. See 18 U.S.C. § 2702(a). For example, in Andersen Consulting LLP 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* emails that Andersen employees had left on the UOP network. Andersen sued, claiming that the disclosure of its contents by the provider UOP had violated the SCA. 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, the SCA did not prohibit disclosure of contents belonging to UOP's "subscribers." See id.

If the services offered by the provider *are* available to the public, then the SCA 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. 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)(6). Section 2702(b) contains exceptions for disclosure of contents, and § 2702(c) contains exceptions for disclosure of other customer records.

The SCA allows the voluntary disclosure of contents when:

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

2) in the case of a remote computing service, the disclosure is made with the consent of a subscriber, § 2702(b)(3);[2]

3) 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);

4) the disclosure is submitted "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A," § 2702(b)(6);

5) 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)(7); or

6) the disclosure is made to a governmental entity, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." § 2702(b)(8).

The SCA provides for the voluntary disclosure of non-content customer records by a provider to a governmental entity when:

1) the disclosure is made "with the lawful consent of the customer or subscriber," or "as otherwise authorized in section 2703," § 2702(c)(1)-(2);

2) 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);

3) the disclosure is made to a governmental entity, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," § 2702(c)(4); or

4) the disclosure is made "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A." § 2702(c)(5).

In general, these exceptions permit disclosure by a provider to the public when the needs of public safety and of service providers themselves 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?		How to Compel Disclosure	
	Public Provider	**Non-Public**	**Public Provider**	**Non-Public**
Basic subscriber, session, and billing information•	No, unless 2702(c) exception applies 2702(a)(3)	Yes 2702(a)(3)	Subpoena; 2703(d) order; or search warrant 2703(c)(2)	Subpoena; 2703(d) order; or search warrant 2703(c)(2)
Other transactional and account records	No, 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)
Retrieved communications and the content of 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; SCA does not apply* 2711(2)
Unretrieved communications, including email and voice mail (in electronic storage more 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 communications, including email 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)

• See 18 U.S.C. § 2703(c)(2) for listing of information covered. This information includes local and long distance telephone connection records and records of session times and durations as well as IP addresses assigned to the user during the Internet connections.

† Includes the content of voice communications.

* For investigations occurring in the Ninth Circuit, Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004), requires use of a search warrant unless the communications have been in storage for more than 180 days. Some providers follow Theofel even outside the Ninth Circuit; contact CCIPS at (202) 514-1026 if you have an appropriate case to litigate this issue.

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

Law enforcement officials who procure records under the SCA quickly learn the importance of communicating with network service providers. Communication is necessary 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, it is often advisable for agents to communicate with a network service provider (or review the provider's law enforcement compliance guide) to learn how the provider operates *before* obtaining a legal order that compels the provider to act.

The SCA 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 result, some evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. For example, suppose that a crime occurs on Day 1, agents learn of the crime on Day 28, begin work on a search warrant on Day 29, and obtain the warrant on Day 32, only to learn that the network service provider deleted the records in the ordinary course of business on Day 30. To minimize the risk that evidence will be lost, the SCA 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 services 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 be adequate, a fax or an email is safer practice because it both provides a paper record and guards against misunderstanding. 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, § 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should 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, or they may be unable to comply without taking actions that potentially could alert a suspect. In such a situation, the agent must weigh the benefit of preservation against the risk of alerting the subscriber. The key here is effective communication: agents should communicate with the network service provider before ordering the provider to take steps that may have unintended adverse effects. Investigators with questions about a provider's practices may also contact CCIPS at (202) 514-1026 for further assistance.

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

Section § 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 legal 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 warrant, agents can simply include appropriate language in the application and proposed order or warrant. If agents instead seek to compel the disclosure of 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. § 521 *et seq.* Originally, 47 U.S.C. § 551 set 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).

After 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 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 USA-PATRIOT Act § 211, 115 Stat. 272, 283-84 (2001). In particular, cable operators may disclose subscriber information to the government pursuant to the SCA, Title III, and the Pen/Trap 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).[3]

4. Reimbursement

When a government entity obtains information pursuant to the SCA, the network provider may be entitled to reimbursement for its reasonable costs incurred in supplying the information.

In general, persons and entities are not entitled to reimbursement for complying with federal legal process unless there is specific federal statutory authorization. See Blair v. United States, 250 U.S. 273, 281 (1919) (discussing possibility of reimbursement for grand jury testimony). "It is beyond dispute that there is in fact a public obligation to provide evidence . . . and that this obligation persists no matter how financially burdensome it may be." Hurtado v. United States, 410 U.S. 578, 589 (1973) (stating that the Fifth Amendment does not require compensation for the performance of a public duty). However, in many (but not all) circumstances, the SCA

requires government entities obtaining the contents of communications, records, or other information pursuant to the SCA to reimburse the disclosing person or entity. See 18 U.S.C. § 2706.

Section 2706 generally obligates government entities "obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704" to pay the service provider "a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information." 18 U.S.C. § 2706(a). Significantly, this section only requires reimbursement when the government actually obtains communication content, records, or other information. Thus, the government is not required to pay for costs incurred by a provider in responding to a 2703(f) preservation letter unless the government later obtains the preserved records.

The amount of the fee required under § 2706(a) "shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court." 18 U.S.C. § 2706(b). In practice, if the service provider seeks what appears to be unreasonably high reimbursement costs, the government should demand a detailed accounting of costs incurred by activity. A cost accounting will help ensure that the provider is not seeking reimbursement for indirect costs or activities that were not reasonably necessary to the production.

In addition, the SCA contains a reimbursement exception that precludes reimbursement in specific circumstances. The reimbursement requirement "does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703," unless a court determines that the information sought by the government is "unusually voluminous" or "caused an undue burden on the provider." 18 U.S.C. § 2706(c).

The reimbursement exception of § 2706(c) applies only to records and other information "maintained by" a communications common carrier. In Ameritech Corp. v. McCann, 403 F.3d 908, 912 (7th Cir. 2005), the Seventh Circuit held that reports of who placed calls to a specified customer were not "maintained by" Ameritech. Ameritech's computer system recorded calls made by a customer, but it did not automatically keep or generate a list of the calls made to a customer. Compiling such a list required substantial computation time. According to the court, Ameritech "maintains" bills and equivalent statements, and the government can therefore get such "raw information" for free. However, when the government requires Ameritech to create a report, the government must provide compensation. Prosecutors outside the Seventh Circuit are not bound by Ameritech, and there is a reasonably strong argument that its interpretation of § 2706(c) is flawed. Under this alternative interpretation, any information stored by a carrier is "maintained by" the carrier, and questions regarding the difficulty of producing information can be evaluated under the "undue burden" standard of § 2706(c).

H. Constitutional Considerations

Defendants sometimes raise constitutional challenges to compelled disclosure of information from communication service providers. They typically argue that use of a 2703(d) order or a

subpoena (rather than a warrant) to compel disclosure of information violated the Fourth Amendment. These claims fail for two reasons. First, the defendant may have no reasonable expectation of privacy in the information obtained from the service provider. Second, the Fourth Amendment generally permits the government to compel a provider to disclose information in an account when the provider has access to and control over the targeted information, regardless of whether the account user has a reasonable expectation of privacy in the targeted information.

It is now well established that a customer or subscriber has no reasonable expectation of privacy in her subscriber information or transactional records. In United States v. Miller, 425 U.S. 435 (1976), the Supreme Court held that a defendant had no reasonable expectation of privacy in his bank records because the records were not his "private papers" but were "the business records of the banks" in which the defendant could "assert neither ownership nor possession." Id. at 440. The Court explained that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." Id. at 443 (citing Hoffa v. United States, 385 U.S. 293, 302 (1966)). The Court relied upon the principles of Miller in Smith v. Maryland, 442 U.S. 735 (1979), in which it held that a defendant had no reasonable expectation of privacy in dialed telephone numbers obtained from the phone company. Id. at 745-46.

Courts have now extended this Miller/Smith analysis to network accounts, holding that individuals retain no Fourth Amendment privacy interest in subscriber information and transactional records. See United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (email and Internet users have no reasonable expectation of privacy in source or destination addresses of email or the IP addresses of websites visited); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (finding no Fourth Amendment protection for network account holders' subscriber information obtained from communication service provider).

In contrast, whether a user has a reasonable expectation of privacy in the contents of communications stored in her account will depend on the facts and circumstances associated with the account. In Quon v. Arch Wireless Operating Co., 529 F.3d 892, 906 (9th Cir. 2008), the Ninth Circuit rejected "a monolithic view of text message users' reasonable expectation of privacy," explaining that "this is necessarily a context-sensitive inquiry." Compare Quon, 529 F.3d at 906-08 (finding reasonable expectation of privacy in pager messages based on an "informal policy that the text messages would not be audited"), and Wilson v. Moreau, 440 F. Supp. 2d 81, 108 (D.R.I. 2006) (finding reasonable expectation of privacy in content of Yahoo! email account), aff'd, 492 F.3d 50 (1st Cir. 2007), with Biby v. Board of Regents, 419 F.3d 845, 850-51 (8th Cir. 2005) (university policy stating that computer files and emails may be searched in response to litigation discovery requests eliminated computer user's reasonable expectation of privacy) and Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (finding that disclaimer on private bulletin board service defeated expectation of privacy in postings). See also United States v. Young, 350 F.3d 1302, 1307-08 (11th Cir. 2003) (Federal Express customer had no reasonable expectation of privacy in the contents of a package based on terms of service authorizing Federal Express to inspect packages).

Critically, however, even if a user has a reasonable expectation of privacy in an item, a subpoena may be used to compel the production of the item, provided the subpoena is reasonable. See United States v. Palmer, 536 F.2d 1278, 1281-82 (9th Cir. 1976). The Fourth Amendment imposes a probable cause requirement *only* on the issuance of warrants. See U.S. Const. amend.-IV ("and no Warrants shall issue, but upon probable cause"). A century of Supreme Court case law demonstrates that reasonable subpoenas comply with the Fourth Amendment. See Wilson v. United States, 221 U.S. 361, 376 (1911) ("there is no unreasonable search and seizure when a [subpoena], suitably specific and properly limited in its scope, calls for the production of documents which, as against their lawful owner to whom the writ is directed, the party procuring its issuance is entitled to have produced"); Oklahoma Press Publ'g Co. v. Walling, 327 U.S. 186, 208 (1946); United States v. Dionisio, 410 U.S. 1, 9-12 (1973); Donovan v. Lone Steer, Inc., 464 U.S. 408, 414-15 (1984). The rule for when a subpoena is reasonable and thus complies with the Fourth Amendment is also well-established: "the Fourth Amendment requires that the subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome." Donovan, 464 U.S. at 415 (quoting See v. City of Seattle, 387 U.S. 541, 549 (1967)). Finally, the Fourth Amendment does not require that notice be given to the target of an investigation in third-party subpoena cases. See SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743, 749-51 (1984).

In general, the cases indicate that the government may compel an entity to disclose any item that is within its control and that it may access. 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 mail in the third party's possession); Schwimmer v. United States, 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). This rule is supported both by the rule that a party with "joint access or control for most purposes" may consent to a search, see United States v. Matlock, 415 U.S. 164, 171 n.7 (1974), and also by the rule that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." Miller, 425 U.S. at 443.

As a practical matter, there is good reason to believe that network service providers will typically have sufficient access to and control over stored communications on their networks to produce the communications in response to compulsory process. Terms of service used by network service providers often establish that the provider has authority to access and disclose subscriber email. For example, at the time of this writing, Yahoo!'s terms of service confirm its right in its "sole discretion to pre-screen, refuse, or remove any Content that is available via the Yahoo! Services," as well as to access and disclose email to comply with legal process. Terms of service similar to Yahoo!'s were sufficient to establish Federal Express's common authority over the contents of a package in Young: the Eleventh Circuit concluded that because Federal Express retained the right to inspect packages, it had authority to consent to a government request to search the package without a warrant. Young, 350 F.3d at 1309. See generally Warshak v. United States, 532 F.3d 521, 527 (6th Cir. 2008) (en banc) (noting the range of terms of service used by different providers). In addition, service providers typically exercise actual authority to access the content of communications stored on their networks. Major providers regularly screen

for spam, malicious code, and child pornography. Some, such as Gmail, screen the content of email in order to target advertising at the account holder.

CCIPS has assisted many prosecutors facing constitutional challenges to the SCA, and prosecutors confronted with such challenges are encouraged to consult with CCIPS at (202) 514-1026 for further assistance.

I. Remedies

Suppression is not a remedy for nonconstitutional SCA violations. However, the SCA does create a cause of action for civil damages.

1. Suppression

The SCA 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 the SCA do not result in suppression of the evidence. See United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008) ("[V]iolations of the ECPA do not warrant exclusion of evidence."); United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); 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. Ferguson, 508 F. Supp. 2d 7, 10 (D.D.C. 2007); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005); 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) (unpublished); 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.").

As discussed previously in Section H, defendants occasionally have claimed that section 2703's procedures for compelled disclosure violate the Fourth Amendment. However, even if a court were to hold section 2703 unconstitutional in some circumstances, suppression would likely not be a proper remedy. In Illinois v. Krull, 480 U.S. 340, 349 (1987), the Supreme Court held that the exclusionary rule did not apply to evidence obtained in "objectively reasonable reliance on a statute." Reliance on section 2703 likely satisfies this standard, as the only decision thus far to have held section 2703 unconstitutional was reversed on appeal. See Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (en banc). In addition, when a defendant moves to suppress based on a claim that the SCA's procedures are unconstitutional, the court may conclude that the government's reliance on the SCA was objectively reasonable and deny the suppression motion without ruling on the constitutionality of the SCA. See Krull, 480 U.S. at 357 n.13; United States v. Vanness, 342 F.3d 1093, 1098 (10th Cir. 2003). Courts have adopted this approach in two cases in which the defendants argued that the SCA was unconstitutional. See United States v. Warshak, 2007 WL 4410237, at *5 (S.D. Ohio Dec. 13, 2007); United States v. Ferguson, 508 F. Supp. 2d 7, 9-10 (D.D.C. 2007).

2. Civil Actions and Disclosures

Although the SCA 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. See, e.g., Freedman v. American Online, Inc., 303 F. Supp. 2d 121 (D. Conn. 2004) (granting summary judgment on liability under the SCA against police officers who served on AOL a purported search warrant that had not been signed by a judge). The Ninth Circuit has held that the SCA does not impose secondary liability for aiding and abetting an SCA violation or conspiring to violate the SCA. See Freeman v. DirecTV, Inc., 457 F.3d 1001, 1006 (9th Cir. 2006). Thus, liability under the SCA for a violation of the voluntary disclosure provisions of section 2702 is limited to service providers. See id. at 1006.

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 SCA-related information. Information that is obtained pursuant to § 2703 and that qualifies as a "record" under 5 U.S.C. § 552a(a) can be disclosed by an officer or governmental entity only "in the proper performance of the official functions of the officer or governmental entity making the disclosure." 18 U.S.C. § 2707(g). Other disclosures of such information by an officer or governmental entity are unlawful unless the information has been previously and lawfully disclosed to the public. See id.

The SCA includes separate provisions for suits against the United States and suits against any other person or entity. Section 2707 permits a "person aggrieved" by SCA violations that result from knowing or intentional conduct 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. 18 U.S.C. § 2707(b), (c). Willful or intentional violations can also result in punitive damages, see § 2707(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 civil or criminal action brought under the SCA. See § 2707(e). Qualified immunity may also be available. See Chapter 4.E.2.

Suits against the United States may be brought under 18 U.S.C. § 2712 for willful violations of the SCA, Title III, or specified sections of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.* 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 adversely affect a related investigation or criminal prosecution. See 18 U.S.C. § 2712 (b), (e).

1 The SCA is sometimes referred to as the Electronic Communications Privacy Act. The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), but ECPA itself also included amendments to the Wiretap Act and created the Pen Register and Trap and Trace Devices statute addressed in Chapter 4. See Pub. L. No. 99-508, 100 Stat. 1848 (1986). Although 18 U.S.C. § 2701-2712 is referred to as the "Stored Communications Act" here and elsewhere, the phrase "Stored Communications Act" appears nowhere in the language of the statute.

2 See also Quon, 529 F.3d at 900-03 (holding that text messaging service provider did not provide remote computing service and thus could not disclose users' communications to the city that subscribed to its service).

3 The Satellite Home Viewer Extension and Reauthorization Act of 2004 (SHVERA) was based on the original Cable Act and contains nearly identical provisions governing disclosure of customer records by satellite television providers. See 47 U.S.C. § 338(i).

Chapter 4

Electronic Surveillance in Communications Networks

A. Introduction

Criminal investigations often involve real-time 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" email account to monitor a suspect sending or receiving child pornography. In cases involving cellular telephones, agents may wish to obtain "cell-site" location information for a suspect's cellular telephone to determine the suspect's approximate location at the time of a call. Agents may wish to wiretap a suspect's telephone or learn whom the suspect has called. This chapter explains how the electronic surveillance statutes apply to criminal investigations involving computers and also discusses how to obtain cell-site location information for cellular phones.

Real-time electronic surveillance in federal criminal investigations is governed primarily by two statutes. The first is the federal Wiretap Act, 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, first passed as part of the Electronic Communications Privacy Act of 1986. 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 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(2)(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, 453-54 (D.C. Cir. 2000) (contrasting pen registers and Title III intercept devices); Brown v. Waddell, 50 F.3d 285, 289-94 (4th Cir. 1995) (same).

The difference between addressing information and content is clear for telephone calls. The addressing information is the phone numbers of the originating and receiving telephones. 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 on 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 payload of the packet, which contains the contents (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, collecting the entire packet ordinarily implicates Title III. The primary difference between an Internet pen/trap device and an Internet Title III intercept device is that the former is designed to capture and retain only addressing information, while the latter is designed to capture and retain the entire packet.

The same distinction applies to Internet email. Every Internet email 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 email 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). See United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (email to/from addresses and IP addresses constitute addressing information). The Pen/Trap statute permits law enforcement to obtain the header information of Internet emails (except for 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 email contents, including the subject line, requires compliance with the strict dictates of Title III.

In some circumstances, questions may arise regarding whether particular components of network communications contain content. See In re Application of United States, 396 F. Supp. 2d 45, 49 (D. Mass. 2005) (asserting that uniform resource locators ("URLs") may contain content); In re Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9, 16 (1st Cir. 2003) (noting that user-entered search terms are sometimes appended to the query string of the URL for the search results page). Because of these and other issues, the United States Attorneys' Manual currently requires prior consultation with CCIPS before a pen/trap may be used to collect all or part of a URL. See United States Attorneys' Manual § 9-7.500. Prosecutors who have other questions about whether a particular type of information constitutes contents may contact CCIPS for assistance at (202) 514-1026.

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 if "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). The Pen/Trap statute applies to a wide range of communication technologies, including computer network communications. See In re Application of United States, 416 F. Supp. 2d 13, 16 (D.D.C. 2006).

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, 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.

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 email headers) is both a pen register and a trap and trace device, and it is commonly referred to 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 non-mobile telephone, a cellular telephone, an Internet user account, an email account, or an IP address. Second, the definitions' inclusion of all "dialing, routing, addressing, [and/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 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 CCIPS at (202) 514-1026, OEO at (202) 514-6809, or their local CHIP (see Introduction, p. xii)

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 have jurisdiction over the offense being investigated. See 18 U.S.C. § 3122(a); 18 U.S.C. § 3127(2)(A). So long as the application contains these elements, the statute obligates the court to 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 United States, 846 F. Supp. 1555, 1559 (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 can 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) in the United States through whom calls are placed to the target telephone. Similarly, in the Internet context, a federal prosecutor may obtain an order to trace communications sent 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 United States in the chain from the victim to the source of the communications.

The Pen/Trap statute does not require an applicant for a pen/trap order to describe precisely what types of "dialing, routing, addressing, [and/or] signaling information" he or she seeks to obtain. Although one magistrate has ruled that an Internet pen/trap order should contain a list of categories of information that may not be collected, such as email subject lines, see In re Application of United States, 396 F. Supp. 2d 45, 49 (D. Mass. 2005), this requirement is not supported by the statute. One later district court held that such a "do not collect" list is unnecessary. See In re Application of United States, 416 F. Supp. 2d 13, 18 (D.D.C. 2006) (approving Internet pen/trap order seeking specified non-content information, such as originating IP addresses).

The government must also use "technology reasonably available to it" to avoid recording or decoding the contents of any wire or electronic communications. 18 U.S.C. § 3121(c). When there is no way to avoid the inadvertent collection of content through the use of reasonably available technology, DOJ policy requires that the government may not use any inadvertently collected content in its investigation. However, a few courts have gone beyond the statute's requirement that the government use technology reasonable available to it to avoid collecting content. Citing the exclusion of contents from the definitions of pen register and trap and trace device, these courts have stated or implied that the government cannot use pen/trap devices that might collect any content at all. See In re Application of the United States, 2007 WL 3036849, at *8-9 (S. D. Tex. 2007) ("[T]he Pen Register Statute does not permit the Government simply to minimize the effects of its collection of unauthorized content, but instead prohibits the collection of content in the first place."); In re Application of United States, 416 F. Supp. 2d 13, 17 (D.D.C. 2006) ("[T]he Government must ensure that the process used to obtain information about email communications excludes the contents of those communications."). Courts have been particularly likely to take this position in the context of phone pen/trap devices that would collect "post-cut-through dialed digits" because this data can include content that cannot be separated out using reasonably available technology.[1] See In re Applications of United States, 515 F. Supp. 2d 325, 339 (E.D.N.Y. 2007); In re Application of United States, 441 F. Supp. 2d 816, 827 (S.D. Tex. 2006); In re Application of United States, 2007 WL 3036849, at *8-*9 (S. D. Tex. 2007). Because this area of the law is developing rapidly, prosecutors or agents may have

questions about current trends, and they may direct any such questions to Mark Eckenwiler, Associate Director, of OEO at (202) 514-6809, CCIPS at (202) 514-1026, or their local CHIP (see Introduction, p. xii)

A pen/trap order may authorize the installation and 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 order should direct the provider not to disclose the existence of the pen/trap or the investigation "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 all "information, facilities, and technical assistance" necessary to install pen/trap devices unobtrusively and with a minimum of interference with services. 18 U.S.C. § 3124(a), (b). Providers and other persons 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 pen/trap 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 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 identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied." 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.

The Pen/Trap statute requires record keeping and reporting when law enforcement officers install their own pen/trap device on a packet-switched data network of a provider of electronic communications service to the public. See 18 U.S.C. § 3123(a)(3). In such cases, the agency must maintain a record that identifies: (1) the identity of the officers who installed the device or accessed it to obtain information; (2) the dates and times the device was installed, uninstalled, and accessed to obtain information; (3) the configuration of the device at the time of installation and any subsequent modifications thereof; and (4) the information collected by the device. See 18 U.S.C. § 3123(a)(3)(A). This record must be provided to the court within thirty days after termination of the pen/trap order (including any extensions thereof). See 18 U.S.C. § 3123(a)(3)(B).

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 United States, 846 F. Supp. 1555, 1559 (M.D. Fla. 1994).

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).

3. Emergency Pen/Traps

The Pen/Trap statute authorizes the installation and use of a pen/trap without a court order in emergency situations involving: (1) immediate danger of death or serious bodily injury to any person; (2) conspiratorial activities characteristic of organized crime; (3) an immediate threat to a national security interest; or (4) an ongoing attack on a protected computer (as defined in 18 U.S.C. § 1030(e)(2)) that constitutes a crime punishable by a term of imprisonment greater than one year. See 18 U.S.C. § 3125(a)(1). The installation and use of an emergency pen/trap requires approval at least at the Deputy Assistant Attorney General level, or by the principal prosecuting attorney of any state or subdivision thereof who is acting pursuant to a state statute. See 18 U.S.C. § 3125(a). In order to authorize an emergency pen/trap, the relevant official must reasonably determine that (1) a specified emergency situation requires the installation and use of the pen/trap device before an order authorizing such installation and use can, with due diligence, be obtained, and (2) there are grounds upon which a pen/trap order could be entered to authorize the installation and use. See 18 U.S.C. § 3125(a). For assistance in seeking an emergency pen/trap authorization during regular business hours, contact OEO at (202) 514-6809 and ask to speak to a supervisor in the electronic surveillance unit. Outside of regular business hours, contact the DOJ Command Center at (202) 514-5000.

A court order authorizing the installation and use of the emergency pen/trap device must be sought within 48 hours after its installation and use. See 18 U.S.C. § 3125(a), (c). In the absence

of such an order, the use of the emergency pen/trap device must immediately terminate when the earliest of these events occurs: (i) the information sought is obtained, (ii) the application for the order is denied, or (iii) 48 hours have lapsed since the installation of the pen/trap device. 18 U.S.C. § 3125(b).

4. The Pen/Trap Statute and Cell-Site Information

Cell-site data identifies the antenna tower and, in some cases, the 120-degree face of the tower to which a cell phone is connected at the beginning and end of each call made or received by a cell phone. "These towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas." In re Application of United States, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005). Thus, at best, this data reveals the neighborhood in which a cell phone user is located at the time a call starts and at the time it terminates; it does not provide continuous tracking and is not a virtual map of a cell phone user's movements. Despite its relative lack of precision, cell-site information is an important investigatory tool that can help law enforcement determine where to establish physical surveillance and locate kidnapping victims, fugitives, and targets of criminal investigations. This section discusses using the combined authority of the Pen/Trap statute and 18 U.S.C. § 2703(d) to obtain prospective cell-site data. For a discussion of how to obtain *historical* cell-site data, see Chapter 3.

In most districts, investigators may obtain prospective cell-site information through an application that satisfies both the Pen/Trap statute and 18 U.S.C. § 2703(d). The rationale behind this "hybrid" use of the Pen/Trap statute and § 2703(d) is as follows. Cell-site data is "dialing, routing, addressing, or signaling information," and therefore 18 U.S.C. § 3121(a) requires the government to obtain a pen/trap order to acquire this information. However, the Communications Assistance for Law Enforcement Act of 1994 ("CALEA") precludes the government from relying "solely" on the authority of the Pen/Trap statute to obtain cell-site data for a cell phone subscriber. 47 U.S.C. § 1002(a). Thus, some additional authority is required to obtain prospective cell-site information. Section 2703(d) provides this authority because, as discussed in Chapter 3, *supra*, it authorizes the government to use a court order to obtain all non-content information pertaining to a customer or subscriber of an electronic communication service.

When seeking a hybrid order for prospective cell-site information, prosecutors must satisfy the requirements of both the Pen/Trap statute and 18 U.S.C. § 2703(d). This application should contain: (i) a government attorney's affirmation "that the information likely to be obtained is relevant to an ongoing criminal investigation," 18 U.S.C. § 3122, and (ii) a further demonstration by the government attorney of "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." 18 U.S.C. § 2703(d). Hybrid orders otherwise generally follow the procedures for pen/trap orders.

District courts and magistrate judges have split on whether hybrid orders may be used to compel disclosure of prospective cell-site information. Compare In re Application of United States, 2008 WL 5082506 (E.D.N.Y. 2008) (upholding hybrid orders for cell-site information), In re Application of United States, 460 F. Supp. 2d. 448, 462 (S.D.N.Y. 2006) (same), and In re Application of United States, 433 F. Supp. 2d 804, 806 (S.D. Tex. 2006) (same), with In re

Application of United States, 416 F. Supp. 2d 390, 396-97 (D. Md. 2006) (rejecting hybrid orders), and In re Application of United States, 396 F. Supp. 2d 294, 327 (E.D.N.Y. 2005) (same). Courts that have rejected hybrid orders for prospective cell-site information have generally required the government to obtain a warrant to compel its disclosure. See, e.g., In re Application of United States, 416 F. Supp. 2d at 397. Most of these courts have not held that a warrant is constitutionally required to obtain prospective cell-site information. Instead, they have held that as a matter of statutory construction, the Pen/Trap statute and 18 U.S.C. § 2703(d) cannot be used to obtain prospective cell-site information, and that Rule 41 can be used because it "governs any matter in which the government seeks judicial authorization to engage in certain investigative activities." In re Application of United States, 396 F. Supp. 2d at 322. Because this area of the law is developing rapidly, prosecutors or agents may have questions about current trends in different districts, and they should direct any such questions to John Lynch, Deputy Chief for Computer Crime, of CCIPS at (202) 514-1026, Mark Eckenwiler, Associate Director, of OEO at (202) 514-6809, or their local CHIP (see Introduction, p. xii)

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, monitor 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 exchange between two participating parties, such as a telephone call between A and B. At a fundamental level, the statute prohibits using an electronic, mechanical, or other device to intercept private wire, oral, or electronic communications between the parties unless one of several statutory exceptions applies. See 18 U.S.C. §§ 2510(4), 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 a home, at a workplace, in government offices, in prison, or on the Internet, they must almost invariably 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 18 U.S.C. §§ 2510(1), (2), (4), (12). 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 OEO at (202) 514-6809.

"Wire communication"

In general, telephone conversations are wire communications.

Title III defines "wire communication" as

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.

18 U.S.C. § 2510(1).

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 the point of reception"). If a communication does not contain a human voice, either alone or in a group conversation, then it is not 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. See In re Application of United States, 349 F.3d 1132, 1138 n.12 (9th Cir. 2003) (cell phone communications are considered wire communications under Title III). Importantly, the presence

of wires 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. H.R. Rep. No. 99-647, at 35 (1986).

"Electronic communication"

Most Internet communications (including email) are electronic communications.

Title III originally covered only wire and oral communications, but Congress amended it in 1986 to include "electronic communications," defined 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.

18 U.S.C. § 2510(12).

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 qualify as electronic communications. See, e.g., Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002) ("document" transmitted from web server); In re Application of United States, 416 F. Supp. 2d 13, 16 (D.D.C. 2006) ("there can be no doubt that [§ 2510(12)] is broad enough to encompass email communications and other similar signals transmitted over the Internet").

However, at least one district court has held that transmissions that occur within a single computer--such as the transmission of keystrokes from the keyboard to the central processing unit--are not "electronic communications" within the meaning of Title III. See United States v. Ropp, 347 F. Supp. 2d 831 (C.D. Cal. 2004). In Ropp, the defendant placed a piece of hardware between the victim's computer and her keyboard that recorded the signals transmitted between the two. Id. at 831. The court found that the acquired communications were not "electronic communications" because "the communications in question involved preparation of emails and

other communications, but were not themselves emails or any other communication at the time of the interception." Id. at 835 n.1. Because the court found that the typing was a communication within the victim's own computer, it reasoned that "[a]t the time of interception, [the communications] no more affected interstate commerce than a letter, placed in a stamped envelope, that has not yet been mailed." Id. The court further stated that the acquired keystrokes could not be an "electronic communication" under Title III because these transmissions were not made by a "system that affects interstate or foreign commerce." Id. at 837. In the court's view, a computer is not a "system that affects interstate or foreign commerce" simply by virtue of the fact that it is connected to the Internet or to another external network at the time of the electronic transmission; rather, the relevant inquiry is whether the computer's network connection was involved in the transmission. See id. at 837-38. At least one court has criticized Ropp on the ground that it "seems to read the statute as requiring the communication to be traveling in interstate commerce, rather than merely 'affecting' interstate commerce." Potter v. Havlicek, 2007 WL 539534, at *8 (S.D. Ohio Feb. 14, 2007). The court explained that "keystrokes that send a message off into interstate commerce 'affect' interstate commerce." Id.

Notwithstanding the Ropp decision, investigators should use caution whenever they acquire the contents of communications on computers or internal networks in real time. For additional discussion of the statute and relevant legislative history as it relates to the meaning of "electronic communication," see U.S. Department of Justice, *Prosecuting Computer Crimes* (Office of Legal Education 2007), section II.A.4. Agents and prosecutors may call CCIPS at (202) 514-1026, OEO at (202) 514-6809, or the CHIP within their district (see Introduction, p. xii) for additional guidance in specific cases.

"Intercept"

The structure and language of the SCA and Title III require that the term "intercept" be applied only to communications acquired contemporaneously with their transmission.

Title III 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." 18 U.S.C. § 2510(4). The statutory definition of "intercept" does not explicitly require that the "acquisition" of the communication be contemporaneous with the transmission of the communication. However, a contemporaneity requirement is necessary to maintain the proper relationship between Title III and the SCA's restrictions on access to stored communications. Otherwise, for example, a Title III order could be required to obtain unretrieved email from a service provider.

Most courts have held that both wire and electronic communications are "intercepted" within the meaning of Title III only when such communications are acquired contemporaneously with their transmission. An individual who 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 email communications); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-14 (3d Cir. 2003) (same); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876-79 (9th Cir. 2002) (website); United States v. Steiger, 318 F.3d 1039, 1047-50 (11th Cir. 2003) (files stored on hard drive); United States v. Mercado-Nava, 486

F. Supp. 2d 1271, 1279 (D. Kan. 2007) (numbers stored in cell phone); United States v. Jones, 451 F. Supp. 2d 71, 75 (D.D.C. 2006) (text messages); United States v. Reyes, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (pager communications); Bohach v. City of Reno, 932 F. Supp. 1232, 1235-36 (D. Nev. 1996) (same). However, the First Circuit has suggested that the contemporaneity requirement, which was developed during the era of telephone wiretaps, "may not be apt to address issues involving the application of the Wiretap Act to electronic communications." United States v. Councilman, 418 F.3d 67, 79-80 (1st Cir. 2005) (en banc) (citing In re Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9, 21 (1st Cir. 2003)); see also Potter v. Havlicek, 2007 WL 539534, at *6-7 (S.D. Ohio Feb. 14, 2007) (finding "substantial likelihood" that the Sixth Circuit will find the contemporaneity requirement does not apply to electronic communications).

Notably, there is some disagreement between circuits about whether a computer communication is "intercepted" within the meaning of Title III if it is acquired while in "electronic storage," as defined in 18 U.S.C. § 2510(17). The Ninth Circuit has held that in order for a communication to be "intercepted" within the meaning of Title III, "it must be acquired during transmission, not while it is in electronic storage." See Konop, 302 F.3d at 878. The unstated implication of this holding is that communications in electronic storage are necessarily not in transmission. The First Circuit has held, however, that email messages are intercepted within the meaning of Title III when they are acquired while in "transient electronic storage that is intrinsic to the communication process." United States v. Councilman, 418 F.3d 67, 85 (1st Cir. 2005) (en banc). In so holding, the court suggested that an electronic communication can be in "electronic storage" and in transmission at the same time. See id. at 79. Exactly how close in time an acquisition must be to a transmission remains an open question. It is clear that "contemporaneous" does not mean "simultaneous." However, the Eleventh Circuit suggested that "contemporaneous" must equate with a communication "in flight." United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003). By contrast, the First Circuit held the contemporaneity requirement could be read simply to exclude acquisitions "made a substantial amount of time after material was put into electronic storage." In re Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9, 21 (1st Cir. 2003).

3. Exceptions to Title III's Prohibition

Title III broadly prohibits the intentional interception, use, or disclosure[2] of wire and electronic communications unless a statutory exception applies. See 18 U.S.C. § 2511(1). In general, this prohibition 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 the applicability of a statutory exception. Title III contains dozens of exceptions that may or may not apply in hundreds of different situations. In cases involving computer crimes or computer evidence, however, seven exceptions are especially pertinent:

a. interception pursuant to a § 2518 court order;

b. the 'consent' exceptions, § 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).

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, see 18 U.S.C. § 2516(1), and by Justice Department policy in the case of electronic communications (except for numeric pagers). See United States Attorneys' Manual § 9-7.100. 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 18 U.S.C. § 2518(5).

Title III imposes several formidable requirements that must be satisfied before investigators can obtain a Title III order. See 18 U.S.C. §§ 2516-2518. 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)-(s) 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 reasonably appear to be unlikely to succeed or to be too dangerous, see § 2518(1)(c); and (2) 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 Electronic Surveillance Unit of OEO at (202) 514-6809.

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

The consent exceptions under paragraphs 2511(2)(c) and (d) are perhaps the most frequently used exceptions to Title III's general prohibition on intercepting communications. The first consent exception applies to those acting under color of law:

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.

18 U.S.C. § 2511(2)(c). Under Title III, government employees are not "acting under color of law" merely because they are government employees. See Thomas v. Pearl, 998 F.2d 447, 451 (7th Cir. 1993). Whether a person is acting under color of law under Title III depends on whether the individual was acting at the government's direction when conducting the interception. See United States v. Andreas, 216 F.3d 645, 660 (7th Cir. 2000); United States v. Craig, 573 F.2d 455, 476 (7th Cir. 1977); see also Obron Atlantic Corp. v. Barr, 990 F.2d 861, 864 (6th Cir. 1993); United States v. Tousant, 619 F.2d 810, 813 (9th Cir. 1980).

The second consent exception applies more generally:

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.

18 U.S.C. § 2511(2)(d). A criminal or tortious purpose must be a purpose other than merely to intercept the communication to which the individual is a party. See Roberts v. Americable Int'l, Inc., 883 F. Supp. 499, 503 (E.D. Cal. 1995).

In general, both of these provisions authorize the interception of communications when one of the parties to the communication consents to the interception.[3] For example, if an undercover government agent or informant records a telephone conversation between herself and a suspect, her consent to the recording authorizes the interception.[4] See, *e.g.*, Obron Atlantic Corp. v. Barr, 990 F.2d 861, 863-64 (6th Cir. 1993) (relying on § 2511(2)(c)). Similarly, if a private person records her own telephone conversations with others, her consent authorizes the interception unless the commission of a criminal or tortious act was at least a determinative factor in her motivation for intercepting the communication. See United States v. Cassiere, 4 F.3d 1006, 1021 (1st Cir. 1993) (interpreting § 2511(2)(d)).

Courts have provided additional guidance about who constitutes a "party." For example, a police officer executing a warrant who answers the phone and pretends to be the defendant is a party to the communication. See United States v. Campagnuolo, 592 F.2d 852, 863 (5th Cir. 1979). At least one court has held that someone whose presence is known to other communicants may be a party, even if the communicants do not address her, nor she them. See United States v. Tzakis, 736 F.2d 867, 871-72 (2d Cir. 1984).

Consent under subsections 2511(2)(c) and (d) may be express or implied. See United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987). The key to establishing implied consent in most cases is showing that the consenting party received actual notice of the monitoring and used the monitored system anyway. See United States v. Workman, 80 F.3d 688, 693 (2d Cir. 1996); Griggs-Ryan v. Smith, 904 F.2d 112, 116-17 (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); Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) ("Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception.")

(internal quotation marks omitted). However, consent must be "actual" rather than "constructive." See In re Pharmatrak, Inc. Privacy Litigation, 329 F.3d 9, 19-20 (1st Cir. 2003) (citing cases). Proof of notice to the party generally supports the conclusion that the party knew of the monitoring. See Workman, 80 F.3d. at 693; but see Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) (finding lack of consent despite notice of possibility of monitoring). 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), abrogated on other grounds by United States v. Watts, 519 U.S. 148 (1997). Mere knowledge of the capability of monitoring does not imply consent. Watkins v. L. M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983).

i. Bannering and 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, a network banner alerting the user that communications on the network are monitored and intercepted may be used to demonstrate that a user consented to intercepting communications on that network. 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 constitutes consent to the monitoring. Often, a user must click to consent to the terms of the banner before gaining further access to the system; such a user has explicitly consented to the monitoring of her communications. Even if no clicking is required, a 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). Numerous courts have held that explicit notices that prison telephones would be monitored generated consent to monitor inmates' calls. See United States v. Conley, 531 F.3d 56, 58-59 (1st Cir. 2008); United States v. Verdin-Garcia, 516 F.3d 884, 894-95 (10th Cir. 2008); United States v. Workman, 80 F.3d 688, 693-94 (2d Cir. 1996); United States v. Amen, 831 F.2d 373, 379 (2d Cir. 1987). In the computer context, one court rejected an employee's challenge to his employer's remote monitoring of his Internet activity based on a banner authorizing the employer to "monitor communications transmitted" by the employee. United States v. Greiner, 2007 WL 2261642, at *1 (9th Cir. 2007).

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. 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.

In addition to banners, there are also other ways to show that a computer user has impliedly consented to monitoring of network activity. For example, terms of service agreements and computer use policies may contain language showing that network users have consented to monitoring. See, e.g., United States v. Angevine, 281 F.3d 1130, 1132-34 (10th Cir. 2002) (university's computer use policy stated, *inter alia*, that the university would periodically monitor

network traffic); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (government employer's Internet usage policy stated that employer would periodically monitor users' Internet access as deemed appropriate); Borninski v. Williamson, 2005 WL 1206872, at *13 (N.D. Tex. May 17, 2005) (employee signed Application for Internet Access, which stated that use of system implied consent to 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, 1016 (10th Cir. 1993). In a computer network environment, by contrast, the simple framework of a two-way communication between two parties may break 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 times, the ultimate destination of the hacker's communications may be unclear. Finding a "person" who is a "party to the communication"--other than the hacker himself, of course--can therefore be difficult. 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.

The owner of a computer system may satisfy the "party to the communication" language when a user sends a command or 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).

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 surer basis for monitoring by law enforcement.

Title III permits

an operator of a switchboard, or 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, 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.

18 U.S.C. § 2511(2)(a)(i).

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 or invasions of privacy. For example, system administrators can track intruders within their networks in order to prevent further damage. See Mullins, 992 F.2d at 1478 (need to monitor misuse of computer system justified interception of electronic communications pursuant to § 2511(2)(a)(i)).

Importantly, the rights and property clause of the provider exception does not permit providers to conduct unlimited monitoring. See United States v. Auler, 539 F.2d 642, 646 (7th Cir. 1976). 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, 1351 (8th Cir. 1976) ("The federal courts . . . have construed the statute to impose a standard of reasonableness upon the investigating communication carrier."); United States v. Councilman, 418 F.3d 67, 82 (1st Cir. 2005) ("indisputable" that provider exception did not permit provider to read customer email when done in the hope of gaining a commercial advantage).

Thus, providers investigating unauthorized use of their systems have broad authority to monitor and disclose evidence of unauthorized use under § 2511(2)(a)(i), but should attempt to tailor their monitoring and disclosure to that which is reasonably related to the purpose of the monitoring. See, *e.g.*, United States v. Freeman, 524 F.2d 337, 341 (7th Cir. 1975) (phone company investigating use of illegal devices designed to steal long-distance service acted permissibly under § 2511(2)(a)(i) when it intercepted the first two minutes of every illegal conversation but did not intercept legitimately authorized communications). Expressed another way, there should 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); see also 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 should refrain from using the provider exception to satisfy law enforcement needs that lack a substantial nexus with the protection of the provider's rights and property. 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. Where a service provider supplies a communication to law enforcement that was intercepted pursuant to the rights and property exception, courts have scrutinized whether the service provider was acting as an agent of the government when intercepting communications. For example, in McClelland v. McGrath, 31 F. Supp. 2d 616 (N.D. Ill. 1998), a user of a cloned cellular telephone sued police officers for allegedly violating Title III by asking the telephone company to intercept his calls in connection with a kidnapping investigation. In denying in part the officers' motion for summary judgment, the district court found that a genuine issue of material fact existed as to whether the phone company was impermissibly acting as the government's agent when it intercepted the plaintiff's call. See id. at 618-19. The court held that the officers were not free to ask or direct the service provider to intercept any phone calls or disclose their contents without complying with the judicial authorization provisions of Title III, regardless of whether the service provider was entitled to intercept those calls on its own initiative. See id.; see also United States v. McLaren, 957 F. Supp. at 218-19. However, if the provider's interception of communications pursuant to the rights and property clause preceded law enforcement's involvement in the matter, no agency existed at the time of the interception, and the provider exception applies. See United States v. Pervaz, 118 F.3d 1, 5-6 (1st Cir. 1997).

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, the cautious approach is to only accept the fruits of a provider's monitoring if certain criteria have been met that indicate that the provider is monitoring and disclosing to protect its rights or property. These criteria are: (1) the provider's rights and property are clearly implicated, and the provider affirmatively wishes both to intercept and to disclose to protect its 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 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 recommended 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 CHIP or CCIPS attorney 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 under the rights and property exception. 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 special 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 united in having their agency's best interests in mind, it is possible that law enforcement agents will consider relying upon provider monitoring, justifying it under 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., United States v. Savage, 564 F.2d 728, 731 (5th Cir. 1977); 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 CHIP within their district (see Introduction, p. xii) for additional guidance in specific cases.

The "normal course of his employment" and "necessary to the rendition of his service" clauses of § 2511(2)(a)(i) provide additional contexts in which the provider exception applies. Courts have held that the first of these exceptions authorizes a business to receive email sent to an account provided by the business to a former employee or to an account associated with a newly acquired business. See Freedom Calls Found. v. Bukstel, 2006 WL 845509, at *27 (E.D.N.Y. 2006) (employer entitled in the normal course of business to intercept emails sent to account of former employee because, *inter alia*, "monitoring is necessary to ensure that . . . email messages are answered in a timely fashion"); Ideal Aerosmith, Inc. v. Acutronic USA, Inc., 2007 WL 4394447, at *5-6 (E.D. Pa. 2007) (corporation entitled in the normal course of business to intercept emails sent to business it acquired). The "necessary to the rendition of his service" clause 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). These cases generally arose when analog phone lines were in use. For example, a switchboard operator may briefly overhear conversations

when connecting calls. See, e.g., Savage, 564 F.2d at 731-32; Adams v. Sumner, 39 F.3d 933, 935 (9th Cir. 1994). Similarly, repairmen may overhear snippets of conversations in the course of repairs. See United States v. Ross, 713 F.2d 389, 392 (8th Cir. 1983). These cases concerning wire communications suggest that the "necessary incident to the rendition of his service" language would likewise permit a system administrator to intercept communications in the course of repairing or maintaining a computer network.

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

Title III allows victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. Specifically, the computer trespasser exception provides:

It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.

18 U.S.C. § 2511(2)(i).

A "computer trespasser" is defined in 18 U.S.C. § 2510(21) to include any person who accesses a "protected computer" without authorization, provided the person is not "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer."

Under this exception, law enforcement--or a private party acting at the direction of law enforcement--may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before interception can occur, the four requirements found in § 2511(2)(i)(I)-(IV) must be met. Under the first of these requirements, the owner or operator of the computer must authorize the interception. In general, although not specifically required by Title III, 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. Under § 2511(2)(i)(IV), investigators may not invoke the computer trespasser exception unless they are able to avoid intercepting communications of authorized users. Critically, however, the computer trespasser exception may be used in combination with other authorities, such as the consent exception of § 2511(2)(d) and the provider exception of § 2511(2)(a)(I), and in such cases it may

be permissible for investigators to also intercept communications of authorized users. For example, if all non-trespassing users of a network have consented to the monitoring their communications by law enforcement, and if the computer trespasser exception can be used to monitor the communications of all trespassers on the network, then law enforcement will be able to monitor all network communications. Similarly, 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 of trespassers 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)

As a result of Title III's "extension telephone" exception, the statute 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.

18 U.S.C. § 2510(5)(a). Congress intended this exception to have a fairly narrow application: the exception 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. Am. 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), overruled in 11th Cir. by Glazner v. Glazner, 347 F.3d 1212, 1214-16 (11th Cir. 2003); 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, e.g., Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001) ("[M]onitoring in the ordinary course of business requires notice to the person or

persons being monitored."); Kempf v. Kempf, 868 F.2d 970, 973 (8th Cir. 1989) (holding that Title III prohibits all wiretapping activities unless specifically excepted and that the Act does not have an 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).

There is also some ambiguity as to whether and how the extension telephone exception would apply in the computer context because the provision's reference to "any telephone or telegraph instrument, equipment or facility" is not entirely clear. 18 U.S.C. § 2510(5)(a). Specifically, it is not obvious from the text of the statute whether "telephone or telegraph" modifies all three objects--*i.e.*, "instrument, equipment or facility"--or only "instruments." The former reading suggests that the exception could apply only to providers of telephone or telegraph services, while the latter reading supports the conclusion that the exception could apply to a computer service provider. The Second Circuit has resolved this ambiguity in favor of the more expansive interpretation in Hall v. EarthLink Network, Inc., 396 F.3d 500, 504-05 (2d Cir. 2005), in which it held that an ISP acted in its ordinary course of business when it continued to receive and store messages sent to the account of a terminated customer.

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 also a common source of confusion. This language does *not* permit agents to intercept the private communications of the targets of a criminal investigation on the theory that a law enforcement agent may need to intercept communications "in the ordinary course of his duties." As Chief Judge Posner 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 or prison may fall within this law enforcement exception, but non-routine taping designed to target a particular suspect ordinarily would not. See id.; accord Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001) ("Congress most likely carved out an exception for law enforcement officials to make clear that

the routine and almost universal recording of phone lines by police departments and prisons, as well as other law enforcement institutions, is exempt from the statute."); United States v. Lewis, 406 F.3d 11, 18-19 (1st Cir. 2005) (concluding that routine monitoring of calls made from prison falls within law enforcement exception); United States v. Hammond, 286 F.3d 189, 192 (4th Cir. 2002) (same); 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)

Section 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)(7)(A) (creating an analogous rule for stored communications).

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

Section 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." Congress intended this language 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). This exception may apply even if users are required to register and agree to terms of use in order to access the communication. See Snow v. DirecTV, Inc., 450 F.3d 1314, 1321-22 (11th Cir. 2006) (electronic bulletin board that required visitors to register, obtain a password, and certify that they were not associated with DirecTV was accessible to the public).

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

Agents and prosecutors must comply with Title III and the Pen/Trap statute when planning electronic surveillance. Violations can result in criminal penalties, civil liability, and (in the case of certain Title III violations) suppression of the evidence obtained. See 18 U.S.C. § 2511(4) (criminal penalties for Title III violations); 18 U.S.C. § 2520 (civil action for Title III violations); 18 U.S.C. § 3121(d) (criminal penalties for Pen/Trap statute violations); 18 U.S.C. § 2707(a), (g) (civil action for certain Pen/Trap statute 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 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. Accordingly, 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 also result in suppression of the evidence wrongfully obtained.

a. No Statutory Suppression for Interception of Electronic Communications

The statutes that govern electronic surveillance grant statutory suppression remedies to defendants only in a specific set of cases. 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, or when the intercepted oral or wire communications occurred on his premises. 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). An "aggrieved person" is defined in 18 U.S.C. § 2510(11) to mean "a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed." In Alderman v. United States, 394 U.S. 165, 176 (1969), the Supreme Court held that a defendant has standing under the Fourth Amendment to challenge intercepted conversations if he was a party to the conversations or if the conversations occurred "on his premises, whether or not he was present or participating in those conversations."

Notably, Title III does not provide a statutory suppression remedy for unlawful interceptions of electronic communications. See, e.g., United States v. Jones, 364 F. Supp. 2d 1303, 1306-09 (D. Utah 2005); United States v. Steiger, 318 F.3d 1039, 1050-52 (11th Cir. 2003); 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). There is one minor exception to this rule: electronic communications intercepted pursuant to a Title III court order may be suppressed for failure to seal the intercepted communications as required by 18 U.S.C. § 2518(8)(a). See United States v. Suarez, 906 F.2d 977, 982 n.11 (4th Cir. 1990). In addition, the Pen/Trap statute does not provide a statutory suppression remedy for violations. See United States v. Forrester, 512 F.3d 500, 512 (9th Cir. 2008); 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).

b. Suppression Following Interception with a Defective Title III Order

Under section 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 to intercept wire or oral communications 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 (suppression required for failure to receive authorization from Justice Department official listed in § 2516(1) for wire interception order in light of importance of such authorization to statutory scheme) with United States v. Radcliff, 331 F.3d 1153, 1162-63 (10th Cir. 2003) (suppression not required for wiretap orders' failure to specifically identify the Justice Department officials who authorized the applications because, *inter alia*, this defect did not subvert statutory scheme). 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).

c. The "Clean Hands" Exception in the Sixth Circuit

Section 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. Five circuit courts have so held. See United States v. Crabtree, 565 F.3d 887, 889-92 (4th Cir. 2009); 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) 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 in turn 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.

After the Sixth Circuit decided Murdock, several circuits rejected the "clean hands" exception and instead 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 United States v. Crabtree, 565 F.3d 887, 889-92 (4th Cir. 2009); 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).

d. 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 at least two 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. 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). The Ninth Circuit recently confirmed that this holding applies equally to computer surveillance techniques that reveal the "to" and "from" addresses of email messages, the IP addresses of websites visited, and the total amount of data transmitted to or from an account. See United States v. Forrester, 512 F.3d 500, 510-11 (9th Cir. 2008). 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 also 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 United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978), 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." Id.. at 160. 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. Hernandez-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, 581 (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. § 3124(e) (good-faith defense for Title III violations). See also 18 U.S.C. § 3124(e) (good-faith defense for Pen/Trap statute violations). These defenses are most commonly applicable to law enforcement officers executing legal process and service providers complying with legal process, even if the process later turns out to be deficient in some way. Similarly, Title III protects a person acting under color of law when that person believes in good faith that interception is warranted by the computer trespasser exception. See 18 U.S.C. § 2520(d)(3) (creating a defense for good faith reliance on a good faith determination that, *inter alia*, § 2511(2)(i) permitted the interception).

The 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). The defense is also available to providers and other private parties who conduct surveillance in good faith reliance on a court order obtained by law enforcement. See Jacobson v. Rose, 592 F.2d 515, 522-23 (9th Cir. 1978) (Congress established good-faith defense for Title III violations in part "to protect telephone companies and other persons who cooperate under court order with law enforcement officials") (citation omitted). In contrast, 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 majority of courts have recognized a qualified immunity defense to Title III civil suits in addition to the statutory good-faith defense. See, e.g., Lonegan v. Hasty, 436 F. Supp. 2d 419, 430 n.5 (E.D.N.Y. 2006) (noting that courts in Second Circuit have "routinely" allowed defendants to raise the qualified immunity defense in Title III cases); 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) ("a defendant may claim qualified immunity in response to a Title III claim"); 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). But see Berry v. Funk, 146 F.3d 1003, 1013-14 (D.C. Cir. 1998) (concluding that qualified immunity does not apply to Title III violations because the statutory good-faith defense exists); Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 1009 (N.D. Cal. 2006) (disagreeing with Tapley and Blake and holding that providers who assist the government are not entitled to qualified immunity from Title III suits).

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 kidnapper who used a cloned cellular phone when the police asked the cellular provider to intercept the kidnapper's unauthorized communications to help locate the kidnapper, and adding that the kidnapper's right to be free from monitoring was "crystal clear" despite § 2511(2)(a)(i)).

---

1 "Post-cut-through dialed digits" are digits dialed after the initial call set-up is complete. Such digits can be non-content telephone numbers, "such as when a subject places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is 'cut through,' dialing the telephone number of the destination party." United States Telecom Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000). Such digits can also be content. "For example, subjects calling automated banking services enter account numbers. When calling voicemail systems, they enter passwords. When calling pagers, they dial digits that convey actual messages." Id.

2 As the focus of this manual is obtaining electronic evidence, prohibited "use" and "disclosure" are beyond the scope of this manual. Use and disclosure of intercepted communications are discussed in chapter 2 of CCIPS's Prosecuting Computer Crimes (Office of Legal Education 2007) and part XI of OEO's Electronic Surveillance Manual (2005 ed.).

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

4 DOJ policy sets forth certain approval requirements for consensual interception of oral communications. See United States Attorneys' Manual § 9-7.302 (citing 2002 Attorney General Guidelines). Approval from OEO is required in certain sensitive circumstances; AUSA approval is required at a minimum.

Chapter 5

Evidence

A. Introduction

Although the primary concern of this manual is obtaining computer records in criminal investigations, prosecutors must also bear in mind the admissibility of that evidence in court proceedings. Computer evidence can present novel challenges. A complete guide to offering computer records into evidence is beyond the scope of this manual. However, this chapter addresses some of the more important evidentiary issues arising when the government seeks to admit computer records in court, including hearsay and the foundation to establish the authenticity of computer records.

B. Hearsay

Hearsay is "a *statement*, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." Fed. R. Evid. 801(c) (emphasis added). "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." Fed. R. Evid. 801(a) (emphasis added). The Rules of Evidence do not define an "assertion." However, courts have held that "the term has the connotation of a positive declaration." See, e.g., United States v. Lewis, 902 F.2d 1176, 1179 (5th Cir. 1990); Lexington Ins. Co. v. W. Penn. Hosp., 423 F.3d 318, 330 (3d Cir. 2005).

Many courts have categorically determined that computer records are admissible under Federal Rule of Evidence 803(6), the hearsay exception for "records of regularly conducted activity"--or more commonly, the "business records" exception--without first asking whether the records are hearsay. See, e.g., Haag v. United States, 485 F.3d 1, 3 (1st Cir. 2007); United States v. Fujii, 301 F.3d 535, 539 (7th Cir. 2002); United States v. Briscoe, 896 F.2d 1476, 1494 (7th Cir. 1990).

Increasingly, however, courts have recognized that many computer records result from a process and are not statements of persons--they are thus not hearsay at all. See United States v. Washington, 498 F.3d 225, 230-31 (4th Cir. 2007) (printed result of computer-based test was not the statement of a person and thus would not be excluded as hearsay); United States v. Hamilton, 413 F.3d 1138, 1142-43 (10th Cir. 2005) (computer-generated header information was not hearsay as "there was neither a 'statement' nor a 'declarant' involved here within the meaning of Rule 801"); United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003) ("nothing 'said' by a machine . . . is hearsay") (quoting 4 Mueller & Kirkpatrick, Federal Evidence§ 380, at 65 (2d ed. 1994)).

This section addresses hearsay issues associated with three categories of computer records: (1) those that record assertions of persons (hearsay); (2) records resulting from a process (non-hearsay); and (3) records that combine the first two categories and thus are partially hearsay. This section also addresses Confrontation Clause issues that may arise when seeking admission of computer records. However, this section does not address in detail more general questions

regarding the admission of hearsay, which are thoroughly addressed by other resources. See, e.g., Courtroom Evidence, 2nd, Article VIII, United States Department of Justice, OLE (2001); Steven Goode and Olin G. Welborn, *Courtroom Evidence Handbook*, Ch. 2, pp. 226-280 (2005-2006).

1. Hearsay vs. Non-Hearsay Computer Records

Records stored in computers can be divided into three categories: non-hearsay, hearsay, and records that include both hearsay and non-hearsay. First, non-hearsay records are created by a process that does not involve a human assertion, such as: telephone toll records; cell tower information; email header information; electronic banking records; Global Positioning System (GPS) data; and log-in records from an ISP or internet newsgroup. Although human input triggers some of theses processes--dialing a phone number or a punching in a PIN--this conduct is a command to a system, not an *assertion*, and thus is not hearsay. Second, hearsay records contain assertions by people, such as: a personal letter; a memo; bookkeeping records; and records of business transactions inputted by persons. Third, mixed hearsay and non-hearsay records are a combination of the first two categories, such as: email containing both content and header information; a file containing both written text and file creation, last written, and last access dates; chat room logs that identify the participants and note the time and date of "chat"; and spreadsheets with figures that have been typed in by a person, but the columns of which are automatically calculated by the computer program.

Non-Hearsay Records

Hearsay rules apply to statements made by persons, not to logs or records that result from computer processes. Computer-generated records that do not contain statements of persons therefore do not implicate the hearsay rules. This principle applies both to records generated by a computer without the involvement of a person (*e.g.*, GPS tracking records) and to computer records that are the result of human conduct other than assertions (*e.g.*, dialing a phone number or punching in a PIN at an ATM). For example, pressing "send" on an email is a command to a system (send this message to the person with this email address) and is thus non-assertive conduct. See United States v. Bellomo, 176 F.3d 580, 586 (2d Cir. 1999) ("Statements offered as evidence of commands or threats or rules . . . are not hearsay.").

Two cases illustrate this point. In United States v. Washington, 498 F.3d 225 (4th Cir. 2007), lab technicians ran a blood sample taken from the defendant through a gas chromatograph connected to a computer. The test results, signed by the lab director, indicated that the defendant had been driving under the influence of both alcohol and PCP. The lab director, who did not participate in testing the sample, testified at trial. The Fourth Circuit rejected a hearsay objection to this evidence. The court noted that the computer-generated test result was "data generated by" a machine and observed that hearsay must be a "statement" made by a "declarant." Id. at 231. Further, "[o]nly a *person* may be a declarant and make a statement." Id. Since "nothing 'said' by a machine . . . is hearsay," the Fourth Circuit concluded that the test results were not excludable based upon the hearsay rules. Id. (citation omitted).

Similarly, in United States v. Hamilton, 413 F.3d 1138 (10th Cir. 2005), the defendant made a hearsay objection to the admission of header information associated with approximately forty-

four images introduced in his child pornography trial. The header information circumstantially identified Hamilton as the person who had posted the child pornography images to a "newsgroup." Specifically, the header information consisted of the subject of the posting, the date the images were posted, and Hamilton's screen name and IP address. See id. at 1142. The Tenth Circuit noted that the header information was "automatically generated by the computer hosting the newsgroup" when images were uploaded to the newsgroup. Id. Since the information was independently generated by the computer process, there was no "statement" by a "declarant" and thus the header information was "outside of Rule 801(c)'s definition of 'hearsay.'" Id. (citing United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003) (header information automatically generated by a fax machine was not hearsay as "nothing 'said' by a machine . . . is hearsay.")).

Occasionally, courts have mistakenly assumed that computer-generated records are hearsay without recognizing that they do not contain the statement of a person. 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 it concluded that the printout was an admissible business record according to Rule 803(6). On appeal following conviction, the Seventh Circuit also assumed that the printout was hearsay, but agreed with the defendant that the printout should not have been admitted as a business record. See id. at 670. Nevertheless, the court held that the computer printout was sufficiently reliable that it could have been admitted under Rule 807, the residual hearsay exception. See id. at 672. However, the court should instead 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 (or on Confrontation Clause grounds--see Section B.2 *infra*) because it contained no human "statements."

Hearsay Records

Some computer records are wholly hearsay (*e.g.*, a printed text document describing observations of fact where the underlying file data is not introduced). Other computer records contain both hearsay and non-hearsay components (*e.g.*, an email with both header information and content that includes factual assertions). In each instance, the proponent must lay a foundation that establishes both the admissibility of the hearsay statement and the authenticity of the computer-generated record.

A number of courts permit computer-stored business records to be admitted as records of a regularly conducted activity under Rule 803(6). Where business records include hearsay, one must show through testing or by a certification complying with Rule 902(11) or 18 US.C. § 3505 that the records were contemporaneously made and kept in the normal and ordinary course of business by a person with knowledge. Different circuits have articulated slightly different standards for the admissibility of computer-stored business records. Some courts simply apply the direct language of Rule 803(6). 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.") (internal quotation marks and citation omitted); 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 [it] was the regular practice of that business activity to make records, as shown by the testimony of the custodian or other qualified witness."). 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. Fujii, 301 F.3d 535, 539 (7th Cir. 2002); United States v. Sanders, 749 F.2d 195, 198 (5th Cir. 1984).

In addition to the business records exception, other hearsay exceptions may apply in appropriate cases, such as the public records exception of Rule 803(8). See, e.g., United States v. Smith, 973 F.2d 603, 605 (8th Cir. 1992) (police computer printouts are admissible as evidence); Hughes v. United States, 953 F.2d 531, 540 (9th Cir. 1992) (computerized IRS printouts are admissible). Computer records, particularly emails or chat logs, may also include admissions or adopted admissions, which are not hearsay under Rule 801(d)(2). For example, in United States v. Burt, 495 F.3d 733, 738-39 (7th Cir. 2007), the court found that logs of chat conversations between the defendant and a witness were not hearsay--the defendant's half of the conversation constituted "admissions" while the witness's half was admissible as context for those admissions. Similarly, in United States v. Safavian, 435 F. Supp. 2d 36, 43-44 (D.D.C. 2006), the full text of some emails forwarded by the defendant to others were admitted as "adoptive admissions" when their context clearly manifested the defendant's belief in the truth of the authors' statements.

2. Confrontation Clause

In Crawford v. Washington, 541 U.S. 36, 68 (2004), the Supreme Court held that the Confrontation Clause of the Sixth Amendment bars the government from introducing pre-trial "testimonial statements" of an unavailable witness unless the defendant had a prior opportunity to cross examine the declarant. Id. at 68. The Crawford Court declined to define "testimonial statements," but the courts of appeals have subsequently interpreted "testimonial" to mean those statements where the "declarant reasonably expected the statement to be used prosecutorially." United States v. Ellis, 460 F.3d 920, 925 (7th Cir. 2006) (collecting cases).

In Melendez-Diaz v. Massachusetts, 129 S.Ct. 2527, 2532 (2009), the Supreme Court recently held that "certificates of analysis" --affidavits from the state's forensic examiners--identifying substances found on a defendant as cocaine were testimonial statements under Crawford. At trial, the prosecution introduced the certificates to prove that the substance found on the defendant was in fact cocaine, and the affidavits themselves "contained only the bare-bones statement that '[t]he substance was found to contain: Cocaine.'" Id. at 2532. There was no dispute that the "certificates" at issue represented statements of persons. Rather, the respondents had argued, *inter alia*, that testimony concerning "neutral scientific testing" was more reliable and trustworthy than testimony concerning historical events and thus was not the type of testimonial statement that fell within the ambit of the Confrontation Clause. See id. at 2536-37. The Court

rejected this distinction in favor of uniform treatment of all testimonial statements for Confrontation Clause purposes. See id. at 2532.

Although Confrontation Clause analysis is distinct from hearsay analysis, records that are the output of a computer-generated process do not implicate the Confrontation Clause for the same reason that computer-generated records are not hearsay: they are not statements of persons. In United States v. Washington, 498 F.3d 225 (4th Cir. 2007), as described above, computer-generated lab results indicated that the defendant had been driving under the influence of both alcohol and PCP. Washington argued that the computer-generated lab results were "testimonial hearsay" and thus violated his right to confront witnesses against him--namely, the lab technicians who actually ran the lab test. The Fourth Circuit rejected the Confrontation Clause argument, holding that the computer-generated test results were not statements "made by the technicians who tested the blood." Id. at 229. Rather, the "machine printout is the only source of the statement, and no *person* viewed a blood sample and concluded that it contained PCP and alcohol." Id. The Sixth Amendment guarantees the right to confront witnesses; machines, not being persons, are not witnesses. Since the technicians, independent from the machine, could not have affirmed or denied the test results, the admission of the gas chromatography printout did not implicate the defendant's Sixth Amendment rights. In sum, the Fourth Circuit held that the "raw data generated by the diagnostic machines are 'statements' *of the machines* themselves, not their operators. But 'statements' made by machines are not out-of-court statements made by declarants that are subject to the Confrontation Clause." Id.

The Fourth Circuit's analysis in Washington is distinguishable from Melendez-Diaz. The document at issue in Washington was raw, computer-generated data, whereas the "certificates" at issue in Melendez-Diaz were plainly witness statements. Moreover, in Washington, the forensic scientist who interpreted the raw data testified as an expert, and thus the defendant had a full and fair opportunity to call into question the judgment and skills upon which his interpretation of any underlying data was based. See Washington, 498 F.3d at 228. The Fourth Circuit in Washington did not rely on the reliability of "neutral" scientific testing, but on the fact that the machine generating the data was not a person. Consequently, the Fourth Circuit's reasoning in Washington likely remains good law.

C. Authentication

Before a party moves for admission of an electronic record or any other evidence, the proponent must show that it is authentic. That is, the proponent must offer evidence "sufficient to support a finding that the matter in question is what its proponent claims." Fed. R. Evid. 901(a). See United States v. Salcido, 506 F.3d 729, 733 (9th Cir. 2007) (data from defendant's computer was properly introduced under Rule 901(a) based on "chain of custody"); United States v. Meienberg, 263 F.3d 1177, 1181 (10th Cir. 2001) (district court correctly found that sufficient evidence existed under Rule 901(a) to admit computer printout of firearms sold through defendant's business). The proponent need not prove beyond all doubt that the evidence is authentic and has not been altered. United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007). Instead, authentication requirements are "threshold preliminary standard[s] to test the reliability of the evidence, subject to later review by an opponent's cross-examination." Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 544 (D. Md. 2007) (citing Jack B. Weinstein & Margaret A.

Berger, *Weinstein's Federal Evidence* § 900.06 [3] (Joseph M. McLaughlin ed., Matthew Bender 2d ed.1997)); see also United States v. Tin Yat Chin, 371 F.3d 31, 37-38 (2d Cir. 2004). Once evidence has met this low admissibility threshold, it is up to the fact finder to evaluate what weight to give the evidence. United States v. Ladd, 885 F.2d 954, 956 (1st Cir. 1989).

1. Authentication of Computer-Stored Records

The standard for authenticating computer records is the same as for authenticating other records. Although some litigants have argued for more stringent authenticity standards for electronic evidence, courts have resisted those arguments. See, e.g., United States v. Simpson, 152 F.3d 1241, 1249-50 (10th Cir. 1998) (applying general rule 901(a) standard to transcript of chat room discussions); In re F.P., 878 A.2d 91, 95-96 (Pa. Super. Ct. 2005) ("We see no justification for constructing unique rules for admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.").

Generally, witnesses who testify to the authenticity of computer records need not have special qualifications. In most cases, the witness does not need to have programmed the computer himself or even understand the maintenance and technical operation of the computer. See United States v. Salgado, 250 F.3d 438, 453 (6th Cir. 2001) ("[I]t is not necessary that the computer programmer testify in order to authenticate computer-generated records."); United States v. Moore, 923 F.2d 910, 914-15 (1st Cir. 1991) (holding that head of bank's consumer loan department could authenticate computerized loan data). Instead, the witness simply must have first-hand knowledge of the relevant facts, such as what the data is and how it was obtained from the computer or whether and how the witness's business relies upon the data. See generally United States v. Whitaker, 127 F.3d 595, 601 (7th Cir. 1997) (holding that FBI agent who was present when the defendant's computer was seized appropriately authenticated seized files).

Federal Rule of Evidence 901(b) offers a non-exhaustive list of authentication methods. Several of these illustrations are useful in cases involving computer records. For example, Rule 901(b)(1) provides that evidence may be authenticated by a person with knowledge "that a matter is what it is claimed to be." See United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007) (witness and undercover agent sufficiently authenticated emails and chat log exhibits by testifying that the exhibits were accurate records of communications they had had with the defendant); United States v. Kassimu, 2006 WL 1880335 (5th Cir. Jul. 7, 2006) (district court correctly found that computer records were authenticated based on the Postal Inspector's description of the procedure employed to generate the records).

Rule 901(b)(3) allows authentication of the item where the trier of fact or an expert compares it "with specimens which have been authenticated." See United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (emails that were not clearly identifiable on their own could be authenticated by comparison to other emails that had been independently authenticated). Rule 901(b)(4) indicates that evidence can be authenticated based upon distinctive characteristics such as "contents, substance, internal patterns, or other distinctive characteristics." See United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (email was appropriately authenticated

based entirely on circumstantial evidence, including presence of the defendant's work email address, information within the email with which the defendant was familiar, and use of the defendant's nickname); Safavian, 435 F. Supp. 2d at 40 (distinctive characteristics for email included the "@" symbol, email addresses containing the name of the person connected with the email, and the name of the sender or recipient in the "To," "From," or signature block areas).

Rule 901(b)(4) is helpful to prosecutors who seek to introduce electronic records obtained from seized storage media. For example, a prosecutor introducing a hard drive seized from a defendant's home and data from that hard drive may employ a two-step process. First, the prosecutor may introduce the hard drive based on chain of custody testimony or its unique characteristics (*e.g.*, the hard drive serial number). Second, prosecutors may consider using the "hash value" or similar forensic identifier assigned to the data on the drive to authenticate a copy of that data as a forensically sound copy of the previously admitted hard drive. Similarly, prosecutors may authenticate a computer record using its "metadata" (information "describing the history, tracking, or management of the electronic document"). See Lorraine v. Markel American Ins. Co., 241 F.R.D. at 547-48.

When computer-stored records are records of regularly conducted business activity, Rule 902(11) (domestic records) and 18 U.S.C. § 3505 (foreign records) permit the use of a written certification to establish the authenticity of the record. Some have questioned whether such certifications constitute testimonial hearsay barred by Crawford v. Washington, 541 U.S. 36 (2004), which is discussed in Section B.2 above. See, e.g., United States v. Jimenez, 513 F.3d 62, 78 (3d Cir. 2008) ("Even assuming, without deciding, that the Rule 902(11) declarations are testimonial and subject to the Confrontation Clause, their admission in this case for the purpose of authenticating the bank statements was harmless."). In dicta in Melendez-Diaz, the Supreme Court noted that under common law, "[a] clerk could by affidavit *authenticate* or provide a copy of an otherwise admissible record." Melendez-Diaz v. Massachusetts, 129 S. Ct. 2527, 2539 (2009). Lower courts may follow this statement from Melendez-Diaz and hold that the Confrontation Clause allows the introduction of certificates of authenticity at trial. Moreover, even if the Confrontation Clause did bar the introduction of certificates of authenticity at trial, the certificates likely could still be used to establish the authenticity of the records under Rule 104(a), which specifies that "[p]reliminary questions concerning . . . the admissibility of evidence shall be determined by the court," and that in making admissibility determinations, the court "is not bound by the rules of evidence except those with respect to privileges." See United States v. Collins, 966 F.2d 1214, 1223 (7th Cir. 1992) ("In Bourjaily v. United States, 483 U.S. 171, 175-76 (1987), the Supreme Court held that a judge can, without offending the Sixth Amendment's Confrontation Clause, consider another person's out-of-court statements in determining whether these statements are admissible as coconspirator statements.").

2. Authentication of Records Created by a Computer Process

Records that are not just stored in a computer but rather result, in whole or part, from a computer process will often require a more developed foundation. To demonstrate authenticity for computer-generated records, or any records generated by a process, the proponent should introduce "[e]vidence describing a process or a system used to produce a result and showing that the process or system produces an accurate result." Fed. R. Evid. 901(b)(9). See also United

States v. Briscoe, 896 F.2d 1476, 1494-95 (7th Cir. 1990) (the government satisfied its burden where it provided sufficient facts to warrant a finding that the records were trustworthy and the opposing party was afforded an opportunity to inquire into the accuracy thereof). Moreover, in addition to the obvious benefit of getting the records into evidence, a developed foundation will explain what the computer or program does, thereby enabling the finder of fact to understand the soundness and relevance of the records.

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.[1] See, e.g., United States v. Salgado, 250 F.3d 438, 453 (6th Cir. 2001) ("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."). While expert testimony may be helpful in demonstrating the reliability of a technology or computer process, such testimony is often unnecessary. See Salgado, 250 F.3d at 453 ("The government is not required to present expert testimony as to the mechanical accuracy of the computer where it presented evidence that the computer was sufficiently accurate that the company relied upon it in conducting its business."); Brown v. Texas, 163 S.W.3d 818, 824 (Tex. App. 2005) (holding that witness who used global positioning system technology daily could testify about technology's reliability).

When the computer program is not used on a regular basis and the proponent cannot establish reliability based on its use in the ordinary course of business, the proponent 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 (2d Cir. 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); see also United States v. Tank, 200 F.3d 627, 630 (9th Cir. 2000).

3. Common Challenges to Authenticity

Alterations

Because electronic records can be altered easily, opposing parties often allege that computer records lack authenticity because they have been tampered with or changed after they were created. Importantly, courts have rejected arguments that electronic evidence is inherently unreliable because of its potential for manipulation. As with paper documents, the mere possibility of alteration is not sufficient to exclude electronic evidence. Absent specific evidence of alteration, such possibilities go only to the evidence's weight, not admissibility. See United States v. Safavian, 435 F. Supp. 2d 36, 41 (D.D.C. 2006). See also United States v. Whitaker, 127 F.3d 595, 602 (7th Cir. 1997); 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.").

Nevertheless, prosecutors and investigators should be wary of situations in which evidence has been edited or is captured using methods subject to human error. In United States v. Jackson, 488 F. Supp. 2d 866 (D. Neb. 2007), an undercover agent had recorded chat sessions with the defendant by "cutting and pasting" the log of each conversation into a word processing document. After his investigation ended, the agent's computer was wiped clean, leaving the "cut and paste" document as the only record of the chat conversations. Despite the agent's testimony at trial that he had been careful to avoid errors in cutting and pasting, the court excluded the "cut and paste" document based on defense expert testimony that suggested errors in the agent's transcript. Id. at 869-71. The court's analysis relied, in part, on the defense expert's testimony that there were several more reliable methods that the agent could have used to accurately capture the chat logs, including creating a forensic image of the agent's computer's hard drive, using software to save the chats, or using a basic "print screen" function. Id. Still, the ruling in Jackson is at odds with the prevailing standard for authenticity, particularly given the agent's testimony that no errors were made and the defense's inability to demonstrate any actual, as opposed to hypothetical, errors. Under the prevailing standard, courts should admit even "cut and paste" documents in many contexts. Cf. United States v. Gagliardi, 506 F.3d 140, 151 (2d Cir. 2007) (transcript of instant message conversations that were cut and pasted into word processing documents were sufficiently authenticated by testimony of a participant in the conversation).

Authorship

Although handwritten records may be penned in a distinctive handwriting style, computer-stored records do not necessarily identify their author. This is a particular problem with Internet communications, which can offer their authors an unusual degree of anonymity. For example, Internet technologies permit users to send effectively anonymous emails, 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 of a computer record. In particular, distinctive characteristics like email addresses, nicknames, signature blocks, and message contents can prove authorship, at least sufficiently to meet the threshold for authenticity. 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. 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. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) (emails between defendant government official and lobbyist were authenticated by distinctive characteristics under Rule 901(b)(4) including email addresses which bore the sender's and recipient's names; "the name of the sender or recipient in the bodies of the email, in the signature blocks at the end of the email, in the 'To:' and 'From:' headings, and by signature of the sender"; and the contents); United States v. Tank, 200 F.3d 627, 630-31 (9th Cir. 2000) (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) (email messages were properly authenticated where messages included defendant's email address, defendant's nickname, and where defendant followed up messages with phone calls).

Authenticating Contents and Appearance of Websites

Several cases have considered what foundation is necessary to authenticate the contents and appearance of a website at a particular time. Print-outs of web pages, even those bearing the URL and date stamp, are not self-authenticating. See In re Homestore.com, Inc. Securities Lit., 347 F. Supp. 2d 769, 782-83 (C.D. Cal. 2004). Thus, courts typically require the testimony of a person with knowledge of the website's appearance to authenticate images of that website. See id. ("To be authenticated, some statement or affidavit from someone with knowledge is required; for example, Homestore's web master or someone else with personal knowledge would be sufficient."); Victaulic Co. v. Tieman, 499 F.3d 227, 236 (3d Cir. 2007) (court cannot assume that a website belonged to a particular business based solely on the site's URL); United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (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). Testimony of an agent who viewed a website at a particular date and time should be sufficient to authenticate a print-out of that website.

Some litigants have attempted to introduce content from web pages stored by the Internet Archive, a non-profit organization attempting to create a "library" of web pages by using automated web crawlers to periodically capture web page contents. Internet Archive provides a service called the "Wayback Machine" that enables users to view historical versions of captured web pages on a given date. The various courts that have considered information obtained through the Wayback Machine have differed over whether testimony about the Internet Archive's operation is sufficient or whether proponents must provide testimony from someone with personal knowledge of the particular web pages' contents. Compare St. Luke's Cataract and Laser Institute v. Sanderson, 2006 WL 1320242, at *2 (M.D. Fla. May 12, 2006) (Internet Archive employee with personal knowledge of the Archive's database could authenticate web pages retrieved from the Archive), and Telewizja Polska USA, Inc. v. Echostar Satellite Corp., 2004 WL 2367740, at *6 (N.D. Ill. Oct. 15, 2004) (affidavit from an Internet Archive employee would

be sufficient to authenticate web pages retrieved from the Internet Archive's database if the employee had personal knowledge of the Archive's contents), with Novak v. Tucows, Inc., 2007 WL 922306, at *5 (E.D.N.Y. Mar. 26, 2007) (requiring testimony from the host of a web page, rather than from the Internet Archive, to authenticate the page's contents).

D. Other Issues

The authentication requirement and the hearsay rule usually constitute 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. For example, in United States v. Bennett, 363 F.3d 947, 953 (9th Cir. 2004), in an effort to prove that the defendant had imported drugs from international waters, an agent testified about information he viewed on the screen of the global positioning system (GPS) on the defendant's boat. The Ninth Circuit found that the agent's testimony violated the best evidence rule. The agent had only observed a graphical representation of data recorded by the GPS system; he had not actually observed the boat following the purported path. Because the United States sought to prove the contents of the GPS data, the best evidence rule required the government to introduce the GPS data itself or the printout of that data, rather than merely the agent's testimony about the data. See id. Alternatively, the government could have sought to demonstrate that the original GPS data was lost, destroyed, or otherwise unobtainable under Fed. R. Evid. 1004, but the court ruled that the government had failed to do. See id. at 954.

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.

The Federal Rules of Evidence have expressly addressed this concern. The 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). 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).

However, as with demonstrating authenticity, a proponent might need to demonstrate that the print out does *accurately* reflect the stored data in order to satisfy the best evidence rule. Compare Laughner v. State, 769 N.E. 2d 1147, 1159 (Ind. Ct. App. 2002) (AOL Instant Message logs that police had cut-and-pasted into a word-processing file satisfied best evidence rule) (abrogated on other grounds by Fajardo v. State, 859 N.E. 2d 1201 (Ind. 2007)), with United States v. Jackson, 488 F. Supp. 2d 866, 871 (D. Neb. 2007) (word-processing document into which chat logs were cut-and-pasted was not the "best evidence" because it did not accurately reflect the entire conversation).

Similarly, properly copied electronic data is just as admissible as the original data. Rule 1003 states that a "duplicate is admissible to the same extent as an original" unless there is a genuine question about the original's authenticity or there is some other reason why admitting the duplicate would be unfair. A "duplicate" is defined, by Rule 1001(4), as "a counterpart produced by the same impression as the original . . . or by mechanical or electronic re-recording . . . or by other equivalent techniques which accurately reproduces the original." Thus, a proponent can introduce, for instance, an image of a seized hard drive, where the proponent can demonstrate that the imaging process accurately copied the data on the original hard drive. This demonstration is often accomplished through testimony showing that the hash value of the copy matches that of the original.

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 United States v. Moon, 513 F.3d 527, 544-45 (6th Cir. 2008); United States v. Catabran, 836 F.2d 453, 456-57 (9th Cir. 1988); United States v. Sanders, 749 F.2d 195, 199 (5th Cir. 1984); 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).

---

1 As discussed in the hearsay section of this chapter, federal courts that evaluate the authenticity of computer-generated records sometimes 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). Although this analysis is technically incorrect when the records do not contain statements of a person, as a practical matter, 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 under 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).

Appendices

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 eliminate any Fourth Amendment "reasonable expectation of privacy" that users might otherwise retain in their use of the network. Second, banners may generate consent to real-time monitoring under Title III. Third, banners may generate consent to the retrieval of stored files and records pursuant to the SCA. Fourth, in the case of a non-government network, banners may establish the network owner's common authority to consent to a law enforcement search.

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. 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 to consider when evaluating a banner:

a) Does the banner state that a user of the network shall have no reasonable expectation of privacy in the network? A user who lacks a reasonable expectation of privacy in a network will not be able to claim that any search of the network violates his Fourth Amendment rights. See Rakas v. Illinois, 439 U.S. 128, 143 (1978).

b) 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).

c) 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) and 2702(c)(2).

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 to 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 which 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.

Broad Banners

Here are three examples of broad banners:

(1) You are accessing a U.S. Government information system, which includes this computer, this computer network, all computers connected to this network, and all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following: you have no reasonable expectation of privacy regarding communications or data transiting or stored on this information system; at any time, and for any lawful government purpose, the Government may monitor, intercept, search, and seize any communication or data transiting or stored on this information system; and any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

(2) 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.

(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.

Narrower Banners

In other cases, network providers may wish to establish a more limited policy. Here are three examples of relatively narrow banners that will generate consent to access in some situations but not others:

(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 that this sample 2703(d) application and order are for the disclosure of both content and non-content information associated with an email account at an ISP.

When using a 2703(d) order to compel disclosure of content, the government is required either to give prior notice to the subscriber or customer or to comply with the procedures for delayed notice in 18 U.S.C. § 2705(a). This order authorizes the delay of notice to the account holder under 18 U.S.C. § 2705(a). A 2703(d) order can be used to compel disclosure of the content of communications not in "electronic storage" or the content of communications in "electronic storage" for more than 180 days. As discussed in Chapter 3.C.3, courts disagree on whether previously retrieved communications fall within the scope of communications in "electronic storage."

When a 2703(d) order is used to compel disclosure only of non-content information, no notice to the customer or subscriber is required.

UNITED STATES DISTRICT COURT

FOR THE [DISTRICT}

)

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)

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this ex parte application for an Order pursuant to 18 U.S.C. § 2703(d) to require ISPCompany, an Internet Service Provider located in City, State, which functions as an electronic communications service provider and/or a remote computing service, to provide records and other information and contents of wire or electronic communications pertaining to the following email account: sample@sample.com. The records and other information requested are set forth as an Attachment to the proposed Order. In support of this application, the United States asserts:

LEGAL AND FACTUAL BACKGROUND

1. The United States government is investigating [crime summary]. The investigation concerns possible violations of, inter alia, [statutes].

2. Investigation to date of these incidents provides reasonable grounds to believe that ISPCompany has records and other information pertaining to certain of its subscribers that are relevant and material to an ongoing criminal investigation. Because ISPCompany functions as an electronic communications service provider (provides its subscribers access to electronic communication services, including email 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.

3. Here, the government seeks to obtain the following categories of information: (1) records and other information (not including the contents of communications) pertaining to certain subscribers of ISPCompany; and (2) the contents of electronic communications held by ISPCompany (but not in electronic storage for less than 181 days).

4. To obtain records and other information (not including the contents of communications) pertaining to subscribers of an electronic communications service provider 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.

5. Under 18 U.S.C. § 2703(a)(1) and 18 U.S.C. § 2703(b)(1), 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), 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 governmental 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.

6. Section 2703(b)(2) states that § 2703(b)(1) applies with respect to any wire or electronic communication that is held or maintained in 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.

7. 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 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 specific and articulable facts showing that there are reasonable grounds to believe that the materials sought are relevant and material to an ongoing criminal investigation.

THE RELEVANT FACTS

8. [Factual paragraph(s) here]

9. The conduct described above provides reasonable grounds to believe that the materials sought are relevant and material to an ongoing criminal investigation.

10. Records of customer and subscriber information relating to this investigation that are available from ISPCompany, and the contents of electronic communications that may be found at ISPCompany, will help government investigators to identify the individual(s) who are responsible for the events described above and to determine the nature and scope of their activities. Accordingly, the government requests that ISPCompany be directed to produce all records described in Attachment A to the proposed Order. Part A of the Attachment requests the account name, address, telephone number, email address, billing information, and other identifying information for sample@sample.com.

11. Part B requests the production of records and other information relating to sample@sample.com through the date of this Court's Order. As described in more detail in that section, this information should include connection information, telephone records, non-content information associated with any communication or file stored by or for the account(s), and correspondence and notes of records involving the account.

12. Part C requests the contents of electronic communications (not in electronic storage) in ISPCompany's computer systems in directories or files owned or controlled by the accounts identified in Part A. These stored files, covered by 18 U.S.C. § 2703(b)(2), will help ascertain the scope and nature of the activity conducted by sample@sample.com from ISPCompany's computers. Pursuant to 18 U.S.C. § 2703(a), Part C also requests the contents of electronic communications that have been in electronic storage in ISPCompany's computer systems for more than 180 days.

13. The information requested should be readily accessible to ISPCompany by computer search, and its production should not prove to be burdensome.

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

15. The United States requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), ISPCompany 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 would seriously jeopardize the ongoing investigation. 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.

16. 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 ninety days. Providing prior notice to the subscriber or customer would 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 ISPCompany 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 ISPCompany not to disclose the existence or content of the Order or this investigation, except to the extent necessary to carry out the Order; and (4) directing that the notification by the government otherwise required under 18 U.S.C. § 2703(b) be delayed for ninety days; and (5) directing that three certified copies of this application and Order be provided by the Clerk of this Court to the United States Attorney's Office.

Executed on _____ _____

Assistant United States Attorney

UNITED STATES DISTRICT COURT

FOR THE _____

)

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, which application requests the issuance of an order under Title 18, United States Code, Section 2703(d) directing ISPCompany, an electronic communications service provider and/or a remote computing service, located in City, State, to disclose certain records and other information, as set forth in Attachment A to this Order, 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 and the contents of wire or electronic communications 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 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 ISPCompany will, within seven days of the date of this Order, turn over to the United States 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 ISPCompany 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.

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

ATTACHMENT A

You are to provide the following information, if available, as data files on CD-ROM or other electronic media or by facsimile:

A. The following customer or subscriber account information for each account registered to or associated with sample@sample.com for the time period [date range]:

1. subscriber names, user names, screen names, or other identities;

2. mailing addresses, residential addresses, business addresses, email addresses, and other contact information;

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

B. All records and other information relating to the account(s) and time period in Part A, including:

1. records of user activity for any connections made to or from the account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);

2. telephone records, including caller identification records, cellular site and sector information, GPS data, and cellular network identifying information (such as the IMSI, MSISDN, IMEI, MEID, or ESN);

3. non-content information associated with the contents of any communication or file stored by or for the account(s), such as the source and destination email addresses and IP addresses.

4. correspondence and notes of records related to the account(s).

C. [Before seeking to compel disclosure of content, give prior notice to the customer or subscriber *or* comply with the delayed notice provisions of 18 U.S.C. § 2705(a).] The contents of electronic communications (not in electronic storage) in ISPCompany's systems in directories or files owned or controlled by the accounts identified in Part A at any time from [date range]; and the contents of electronic communications that have been in electronic storage in ISPCompany's electronic communications system for more than 180 days [and within date range].

Appendix C

Sample Language for Preservation Requests under 18 U.S.C. § 2703(f)

ISPCompany

Address

Re: Request for Preservation of Records

Dear ISPCompany:

Pursuant to Title 18, United States Code Section 2703(f), this letter is a formal request for the preservation of all stored communications, records, and other evidence in your possession regarding the following email address pending further legal process: sample@sample.com (hereinafter, "the Account").

I request that you not 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 might result in a permanent or temporary termination of service to the Account, or otherwise alert any user of the Account as to your actions to preserve the information described below, please contact me as soon as possible and before taking action.

I request that you preserve, for a period of 90 days, the information described below currently in your possession in a form that includes the complete record. 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 request applies to the following items, whether in electronic or other form, including information stored on backup media, if available:

1. The contents of any communication or file stored by or for the Account and any associated accounts, and any information associated with those communications or files, such as the source and destination email addresses or IP addresses.

2. All records and other information relating to the Account and any associated accounts including the following:

a. subscriber names, user names, screen names, or other identities;

b. mailing addresses, residential addresses, business addresses, email addresses, and other contact information;

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

d. records of user activity for any connections made to or from the Account, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address(es);

e. telephone records, including local and long distance telephone connection records, caller identification records, cellular site and sector information, GPS data, and cellular network identifying information (such as the IMSI, MSISDN, IMEI, MEID, or ESN);

f. telephone or instrument number or other subscriber number or identity, including temporarily assigned network address;

g. means and source of payment for the Account (including any credit card or bank account numbers) and billing records;

h. correspondence and other records of contact by any person or entity about the Account, such as "Help Desk" notes; and

i. any other records or evidence relating to the Account.

If you have questions regarding this request, please call me at [phone number].

Sincerely,

[NAME]

[GOVERNMENT ENTITY]

Appendix D

Sample Pen Register/Trap and Trace Application and Order

The sample pen/trap application and order below are designed (1) to collect email addresses to which the account owner sends email and from which the account owner receives email and (2) to collect IP addresses associated with the transmission of email and the account owner's access to the email account. Investigators may edit the application in order to remove requests for information that will not be needed in a particular case.

UNITED STATES DISTRICT COURT

FOR THE [DISTRICT]

)

IN RE APPLICATION OF THE)

UNITED STATES OF AMERICA FOR) MISC. NO. ____

AN ORDER AUTHORIZING THE)

INSTALLATION AND USE OF PEN)

REGISTER AND TRAP AND)

TRACE DEVICES)

) Filed Under Seal

APPLICATION

The United States of America, moving by and through [AUSA name], its undersigned counsel, respectfully submits under seal this ex parte application for an Order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen/trap devices") on the [service provider] email account [target email address] whose listed subscriber is [subscriber name]. In support of this application, the United States asserts:

1. This is an application, made under 18 U.S.C. § 3122(a)(1), for an order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and a trap and trace device.

2. Under 18 U.S.C. § 3122(b), such an application must include three elements: (1) "the identity of the attorney for the Government or the State law enforcement or investigative officer making the application"; (2) "the identity of the law enforcement agency conducting the investigation"; and (3) "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b).

3. The attorney for the Government making the application is the undersigned, [AUSA name], who is an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

4. The law enforcement agency conducting the investigation is the [law enforcement agency].

5. The applicant hereby certifies that the information likely to be obtained by the requested pen/trap devices is relevant to an ongoing criminal investigation being conducted by [law enforcement agency].

ADDITIONAL INFORMATION

6. Other than the three elements described above, federal law does not require that an application for an order authorizing the installation and use of pen/trap devices specify any facts. The following additional information is provided to demonstrate that the order requested falls within this Court's authority to authorize the installation and use of a pen register or trap and trace device under 18 U.S.C. § 3123(a)(1).

7. 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." 18 U.S.C. § 3127(3). A "trap and trace device" is "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." 18 U.S.C. § 3127(4).

8. In the traditional telephone context, pen registers captured the destination phone numbers of outgoing calls, while trap and trace devices captured the phone numbers of incoming calls. Similar principles apply to other kinds of wire and electronic communications, as described below.

9. The Internet is a global network of computers and other devices. Every device on the Internet is identified by a unique number called an Internet Protocol, or "IP" address. This number is used to route information between devices. Two computers must know each other's IP addresses to exchange even the smallest amount of information. Accordingly, when one computer requests information from a second computer, the requesting computer specifies its own IP address so that the responding computer knows where to send its response. An IP address is analogous to a telephone number and can be recorded by pen/trap devices, and it indicates the online identity of the communicating device without revealing the communication's content.

10. On the Internet, data transferred between devices is not sent as a continuous stream, but rather it is split into discreet packets. Generally, a single communication is sent as a series of packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a header with routing and control information, and a payload, which generally contains user data. The header contains non-content information such as the packet's source and destination IP addresses and the packet's size.

11. An email message has its own routing header, in addition to the source and destination information associated with all Internet data. The message header of an email contains the message's source and destination(s), expressed as email addresses in "From," "To," "CC" (carbon copy), or "BCC" (blind carbon copy) fields. Multiple destination addresses may be specified in the "To," "CC," and "BCC" fields. The email addresses in an email's message header are like the telephone numbers of both incoming and outgoing calls, because they indicate both origin and destination(s). They can be recorded by pen/trap devices and can be used to identify parties to a communication without revealing the communication's contents.

THE RELEVANT FACTS

12. The United States government, including the [law enforcement agency], is investigating [crime facts]. The investigation concerns possible violations by unknown individuals of, inter alia, [statutes].

13. [***OPTIONALLY INSERT FACTUAL PARAGRAPH(S) HERE. Please note that additional facts are not required by statute, but some districts include them in applications anyway. For example, some districts will include a fact paragraph like this one: "The

investigation relates to the purchase and sale of stolen credit cards and other unauthorized access devices, which are then used to perpetrate mail and wire fraud. Investigators believe that matters relevant to the offenses under investigation have been and continue to be discussed using jjones007992@isp.com. Investigators believe that the listed subscriber for this email address number is John Jones, a target of the investigation, ..."]

14. The conduct being investigated involves use of the email account [target email address]. To further the investigation, investigators need to obtain the dialing, routing, addressing, and signaling information associated with communications sent to or from that email account.

15. The pen/trap devices sought by this application will be installed at location(s) to be determined, and will collect dialing, routing, addressing, and signaling information associated with each communication to or from the [service provider] email account [target email address], including the date, time, and duration of the communication, and the following, without geographic limit:

- IP addresses, including IP addresses associated with access to the account;

- Headers of email messages, including the source and destination network addresses, as well as the routes of transmission and size of the messages, but not content located in headers, such as subject lines;

- the number and size of any attachments.

GOVERNMENT REQUESTS

16. For the reasons stated above, the United States requests that the Court enter an Order authorizing installation and use of pen/trap devices to record, decode, and/or capture the dialing, routing, addressing, and signaling information described above for each communication to or from the [service provider] email account [target email address], along with the date, time, and duration of the communication, without geographic limit. The United States does not request and does not seek to obtain the contents of any communications, as defined in 18 U.S.C. § 2510(8), pursuant to the proposed Order.

17. The United States further requests that the Court authorize the foregoing installation and use for a period of sixty days, pursuant to 18 U.S.C. § 3123(c)(1).

18. The United States further requests, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-(b), that the Court order [service provider] and any other person or entity providing wire or electronic communication service in the United States whose assistance may facilitate execution of this Order to furnish, upon service of the Order, information, facilities, and technical assistance necessary to install the pen/trap devices, including installation and operation of the pen/trap devices unobtrusively and with minimum disruption of normal service. Any entity providing such assistance shall be reasonably compensated by [law enforcement agency], pursuant to 18 U.S.C. § 3124(c), for reasonable expenses incurred in providing facilities and assistance in furtherance of this Order.

19. The United States further requests that the Court order [service provider] and any other person or entity whose assistance may facilitate execution of this Order to notify [law enforcement agency] of any changes relating to the email account [target email address], including changes to subscriber information, and to provide prior notice to the [law enforcement agency] before terminating service to the email account.

20. The United States further requests that the Court order that the [law enforcement agency] and the applicant have access to the information collected by the pen/trap devices as soon as practicable, twenty-four hours per day, or at such other times as may be acceptable to them, for the duration of the Order.

21. The United States further requests, pursuant to 18 U.S.C. § 3123(d)(2), that the Court order [law enforcement agency] and any other person or entity whose assistance facilitates execution of this Order, and their agents and employees, not to disclose in any manner, directly or indirectly, by any action or inaction, the existence of this application and Order, the resulting pen/trap devices, or this investigation, except as necessary to effectuate the Order, unless and until authorized by this Court.

22. The United States further requests that this application and any resulting Order be sealed until otherwise ordered by the Court, pursuant to 18 U.S.C. § 3123(d)(1).

23. The United States further requests that the Clerk of the Court provide the United States Attorney's Office with three certified copies of this application and Order, and provide copies of this Order to [law enforcement agency] and [service provider] upon request.

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

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

Executed on _____.

_____

[AUSA name]

[AUSA title]

[address]

UNITED STATES DISTRICT COURT

FOR THE _____

)

IN RE APPLICATION OF THE)

UNITED STATES OF AMERICA FOR) MISC. NO.

AN ORDER AUTHORIZING THE)

INSTALLATION AND USE OF PEN)

REGISTER AND TRAP AND)

TRACE DEVICES)

) Filed Under Seal

ORDER

[AUSA name], on behalf of the United States, has submitted an application pursuant to 18 U.S.C. §§ 3122 and 3123, requesting that the Court issue an Order pursuant to 18 U.S.C. § 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen/trap devices") on the [service provider] email account [target email address], whose listed subscriber is [subscriber name].

The Court finds that the applicant is an attorney for the government and has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation being conducted by [law enforcement agency] of unknown individuals in connection with possible violations of [statutes].

IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 3123, that pen/trap devices may be installed and used to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the [service provider] email account [target email address], including the date, time, and duration of the communication, and the following, without geographic limit:

- IP addresses, including IP addresses associated with access to the account;

- Headers of email messages, including the source and destination network addresses, as well as the routes of transmission and size of the messages, but not content located in headers, such as subject lines;

- the number and size of any attachments.

IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 3123(c)(1), that the use and installation of the foregoing is authorized for sixty days from the date of this Order;

IT IS FURTHER ORDERED, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-(b), that [service provider] and any other person or entity providing wire or electronic communication service in the United States whose assistance may, pursuant to 18 U.S.C. § 3123(a), facilitate the execution of this Order shall, upon service of this Order, furnish information, facilities, and technical assistance necessary to install the pen/trap devices, including installation and operation of the pen/trap devices unobtrusively and with minimum disruption of normal service;

IT IS FURTHER ORDERED that [law enforcement agency] reasonably compensate [service provider] and any other person or entity whose assistance facilitates execution of this Order for reasonable expenses incurred in complying with this Order;

IT IS FURTHER ORDERED that [service provider] and any other person or entity whose assistance may facilitate execution of this Order notify [law enforcement agency] of any changes relating to the email account [target email account], including changes to subscriber information, and to provide prior notice to [law enforcement agency] before terminating service to the email account;

IT IS FURTHER ORDERED that [law enforcement agency] and the applicant have access to the information collected by the pen/trap devices as soon as practicable, twenty-four hours per day, or at such other times as may be acceptable to [law enforcement agency], for the duration of the Order;

IT IS FURTHER ORDERED, pursuant to 18 U.S.C. § 3123(d)(2), that [service provider] and any other person or entity whose assistance facilitates execution of this Order, and their agents and employees, shall not disclose in any manner, directly or indirectly, by any action or inaction, the existence of the application and this Order, the pen/trap devices, or the investigation to any person, except as necessary to effectuate this Order, unless and until otherwise ordered by the Court;

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three certified copies of this application and Order, and shall provide copies of this Order to [law enforcement agency] and [service provider] upon request;

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court, pursuant to 18 U.S.C. § 3123(d)(1).

_____ _____

Date United States Magistrate Judge

Appendix E

Sample Subpoena Language

The SCA permits the government to compel disclosure of the basic subscriber and session information listed in 18 U.S.C. § 2703(c)(2) using a subpoena. This information is specified in Part A below, and the government is not required to provide notice to the subscriber or customer when using a subpoena to compel disclosure of this information.

When the government either gives prior notice to the customer or subscriber or complies with the delayed notice provisions of 18 U.S.C. § 2705(a), it may use a subpoena to compel disclosure of "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" and "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(a), 2703(b)(1)(B)(i), 2703(b)(2). This information is specified in Part B below. As discussed in Chapter 3.C.3, there is disagreement among courts on whether previously retrieved communications fall within the scope of communications in "electronic storage."

The information requested below can be obtained with the 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 18 U.S.C. §§ 2703(b)(1)(B)(i), 2703(c)(2).

Attachment To Subpoena

All customer or subscriber account information for the [choose one: email account, domain name, IP address, subscriber, username] [specify email account, domain name, IP address, subscriber, username], or for any related accounts, that falls within any of the following categories:

1. Name,

2. Address,

3. Local and long distance telephone toll billing records,

4. Records of session times and durations,

5. Length of service (including start date) and types of service utilized,

6. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as an Internet Protocol address, and

7. Means and source of payment for such service (including any credit card or bank account number).

8. [Before seeking to compel disclosure of content, give prior notice to the customer or subscriber or comply with the delayed notice provisions of 18 U.S.C. § 2705(a).] For each such account, the information shall also include the contents of electronic communications (not in electronic storage) held or maintained by your company for the use of the account at any time, up

through and including the date of this subpoena; and the contents of electronic communications that have been in electronic storage in your company's electronic communications system for more than 180 days.

"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.

You are to provide this information, if available, as data files on CD-ROM or other electronic media or by facsimile to [fax number].

Appendix F

Sample Premises Computer Search Warrant Affidavit

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

UNITED STATES DISTRICT COURT

FOR THE [DISTRICT]

)

In the Matter of the Search of) Case No.

[[Premises Address]])

)

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

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

INTRODUCTION AND AGENT BACKGROUND

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

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

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

PROBABLE CAUSE

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

TECHNICAL TERMS

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

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static--that is, long-term--IP addresses, while other computers have dynamic--that is, frequently changed--IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

COMPUTERS AND ELECTRONIC STORAGE

6. As described above and in Attachment A, this application seeks permission to search and seize records that might be found on the PREMISES, in whatever form they are found. I submit that if a computer or electronic medium is found on the premises, there is probable cause to believe those records will be stored in that computer or electronic medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be

stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using readily available forensics tools. This is so because when a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space--that is, in space on the hard drive that is not currently being used by an active file--for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Similarly, files that have been viewed via the Internet are typically automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

d. [[FOR CHILD PORNOGRAPHY CASES]] I know from training and experience that child pornographers generally prefer to store images of child pornography in electronic form as computer files. The computer's ability to store images in digital form makes a computer an ideal repository for pornography. A small portable disk or computer hard drive can contain many child pornography images. The images can be easily sent to or received from other computer users over the Internet. Further, both individual files of child pornography and the disks that contain the files can be mislabeled or hidden to evade detection. In my training and experience, individuals who view child pornography typically maintain their collections for many years and keep and collect items containing child pornography over long periods of time; in fact, they rarely, if ever, dispose of their sexually explicit materials.

e. [[FOR BUSINESS SEARCH CASES]] Based on actual inspection of [[spreadsheets, financial records, invoices]], I am aware that computer equipment was used to generate, store, and print documents used in the [[tax evasion, money laundering, drug trafficking, etc.]] scheme. There is reason to believe that there is a computer system currently located on the PREMISES.

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

8. [[FOR CHILD PORNOGRAPHY PRODUCTION CASES]] I know from training and experience that it is common for child pornographers to use personal computers to produce both still and moving images. For example, a computer can have a camera built in, or can be connected to a camera and turn the video output into a form that is usable by computer programs. Alternatively, the pornographer can use a digital camera to take photographs or videos and load them directly onto the computer. The output of the camera can be stored, transferred or printed

out directly from the computer. The producers of child pornography can also use a scanner to transfer photographs into a computer-readable format. All of these devices, as well as the computer, constitute instrumentalities of the crime.

9. [[FOR HACKING OR OTHER INSTRUMENTALITY CASES]] I know that when an individual uses a computer to [[obtain unauthorized access to a victim computer over the Internet]], the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage device for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

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

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

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

b. Technical requirements. Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and

to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis.

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

13. Searching computer systems for the evidence described in Attachment A may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, the [[AGENCY]] intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

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

a. Upon arriving at the PREMISES, the agents will attempt to identify a system administrator of the network (or other knowledgeable employee) who will be willing to assist law enforcement by identifying, copying, and printing out paper and electronic copies of the things described in the warrant. The assistance of such an employee might allow agents to place less of a burden on the Company than would otherwise be necessary.

b. If the employees choose not to assist the agents, the agents decide that none are trustworthy, or for some other reason the agents cannot execute the warrant successfully without themselves examining the Company's computers, the agents will attempt to locate the things described in the warrant, and will attempt to make electronic copies of those things. This analysis will focus on things that may contain the evidence and information of the violations under investigation. In

doing this, the agents might be able to copy only those things that are evidence of the offenses described herein, and provide only those things to the case agent. Circumstances might also require the agents to attempt to create an electronic "image" of those parts of the computer that are likely to store the things described in the warrant. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Imaging a computer permits the agents to obtain an exact copy of the computer's stored data without actually seizing the computer hardware. The agents or qualified computer experts will then conduct an off-site search for the things described in the warrant from the "mirror image" copy at a later date. If the agents successfully image the Company's computers, the agents will not conduct any additional search or seizure of the Company's computers.

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

CONCLUSION

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

REQUEST FOR SEALING

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

Respectfully submitted,

[[AGENT NAME]]

Special Agent

[[AGENCY]]

Subscribed and sworn to before me on _____:

_____

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

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

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

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

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

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

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

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

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

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

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

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

4. [[IF CASE INVOLVED THE INTERNET]] Records and things evidencing the use of the Internet Protocol address [[e.g. 10.19.74.69]] to communicate with [[e.g. Yahoo! mail servers or university mathematics department computers]], including:

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

b. records of Internet Protocol addresses used;

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

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies).

Appendix G

Sample Letter for Provider Monitoring

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 relying 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 disclosure 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(b)(5) and 2702(c)(3), [Provider] is also permitted to disclose customer communications, 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 [law enforcement] has not directed, requested, encouraged, or solicited [Provider] to intercept, disclose, or use monitored communications, associated records, or other information for law enforcement purposes.

Accordingly, [Provider] will not engage in monitoring solely or primarily to assist law enforcement absent an appropriate court order or a relevant exception to the Wiretap Act (e.g., 18 U.S.C. § 2511(2)(i)). 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,

General Counsel

Appendix H

Sample Authorization for Monitoring of Computer Trespasser Activity

I am [Name of Owner/Operator or person acting on behalf of Owner/Operator, Title] of [Name and Address of Organization]. I am the [Owner] [Operator] [person acting on behalf of the Owner or Operator], and own or have the authority to supervise, manage, or control operation of the [relevant part of the] [Organization's] computer system or the data and communications on and through the network. An unauthorized user(s), who I understand has no contractual basis for any access to this computer system, has accessed this computer and is a trespasser(s). I hereby

authorize [law enforcement agency] to intercept communications to, through, or from a trespasser(s) transmitted to, through, or from [Organization's] computer system. The general nature of the communications to be monitored are [general description of the identifying characteristics of the communications to be monitored.] [Organization will assist law enforcement agency to conduct such interception under the direction of law enforcement agency.] Such interception may occur at any location on the computer system or network, including at multiple or changed locations, which may facilitate the interception of communications to or from the trespasser.

This authorization does not extend to the interception of communications other than those to, through, or from a trespasser(s). This authorization does not restrict monitoring under any other appropriate exception to the Wiretap Act, 18 U.S.C. § 2510 et seq.

This authorization is valid [for a specified time period] [indefinitely, until withdrawn in writing by me or a person acting for me]. I understand I may withdraw authorization for monitoring at any time, but I agree to do so in writing.

_____ _____

Signature of Owner/Operator Date

Appendix I

Sample Email Account Search Warrant Affidavit

The sample 2703 search warrant affidavit and attachments below are designed (1) to obtain email messages associated with the target email account that relate to the investigation, and (2) to obtain records relating to who created, used, or communicated with the account. Investigators may edit the affidavit and attachments to remove requests for information that will not be needed in a particular case. In addition, please note that while the facts described in the "background" section of the affidavit are true for most email providers, the affiant should be certain that they are true for the particular email provider that is the subject of the affidavit.

Notes: When filling out the search warrant form, write "See Attachment A" in the section that asks for the location of the search and "See Attachment B" in the section that asks for a description of the items to be seized. Fax the warrant, along with both attachments and the "certificate of authenticity," to the service provider. The service provider should then give the

requested data to the agent, who should cull through the data returned by the provider and isolate material that is not called for by the warrant.

UNITED STATES DISTRICT COURT

FOR THE [DISTRICT]

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [[EMAIL ADDRESSES]] THAT IS STORED AT PREMISES CONTROLLED BY [[EMAIL PROVIDER]]	Case No. _____

affidavit IN SUPPORT OF

AN APPLICATION FOR A SEARCH WARRANT

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

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by [EMAIL PROVIDER], an email provider headquartered at [PROVIDER ADDRESS]. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require [EMAIL PROVIDER] to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent with the [AGENCY], and have been since [DATE]. [DESCRIBE TRAINING AND EXPERIENCE TO THE EXTENT IT SHOWS QUALIFICATION TO SPEAK ABOUT THE INTERNET AND OTHER TECHNICAL MATTERS].

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. [Give facts establishing probable cause. At a minimum, establish a connection between the email account and a suspected crime. Also mention whether a preservation request was sent (or other facts suggesting the email is still at the provider)]

TECHNICAL BACKGROUND

5. In my training and experience, I have learned that [EMAIL PROVIDER] provides a variety of on-line services, including electronic mail ("email") access, to the general public. Subscribers obtain an account by registering with [EMAIL PROVIDER]. During the registration process, [EMAIL PROVIDER] asks subscribers to provide basic personal information. Therefore, the computers of [EMAIL PROVIDER] are likely to contain stored electronic communications (including retrieved and unretrieved email for [EMAIL PROVIDER] subscribers) and information concerning subscribers and their use of [EMAIL PROVIDER] services, such as account access information, email transaction information, and account application information.

6. In general, an email that is sent to a [EMAIL PROVIDER] subscriber is stored in the subscriber's "mail box" on [EMAIL PROVIDER] servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on [EMAIL PROVIDER] servers indefinitely.

7. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to [EMAIL PROVIDER]'s servers, and then transmitted to its end destination. [EMAIL PROVIDER] often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the [EMAIL PROVIDER] server, the email can remain on the system indefinitely.

8. An [EMAIL PROVIDER] subscriber can also store files, including emails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by [EMAIL PROVIDER]. [NOTE: Consider consulting the provider's law enforcement guide or contacting the provider to identify other types of stored records or files that may be relevant to the case and available from the provider. If there are such records, specifically describe them in the affidavit and list them in Section I of Attachment B.]

9. Subscribers to [EMAIL PROVIDER] might not store on their home computers copies of the emails stored in their [EMAIL PROVIDER] account. This is particularly true when they access their [EMAIL PROVIDER] account through the web, or if they do not wish to maintain particular emails or files in their residence.

10. In general, email providers like [EMAIL PROVIDER] ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

11. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via [EMAIL PROVIDER]'s website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every

device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

12. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

13. I anticipate executing this warrant under the Stored Communications Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require [EMAIL PROVIDER] to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

14. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of [EMAIL PROVIDER] there exists evidence of a crime [and contraband or fruits of a crime]. Accordingly, a search warrant is requested.

15. This Court has jurisdiction to issue the requested warrant because it is "a court with jurisdiction over the offense under investigation." 18 U.S.C. § 2703(a).

16. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR NONDISCLOSURE AND SEALING

17. [IF APPROPRIATE: The United States requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), [EMAIL PROVIDER] be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant 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 would seriously jeopardize the ongoing investigation. 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. [Note: if using this paragraph, include a nondisclosure order with warrant.]]

18. [IF APPROPRIATE: It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal

organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, e.g., by posting them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.]

Respectfully submitted,

[AGENT NAME]

Special Agent

[AGENCY]

Subscribed and sworn to before me on [date]:

_____

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Place to Be Searched

This warrant applies to information associated with [EMAIL ACCOUNT] that is stored at premises owned, maintained, controlled, or operated by [EMAIL PROVIDER], a company headquartered at [ADDRESS].

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by [EMAIL PROVIDER]

To the extent that the information described in Attachment A is within the possession, custody, or control of [EMAIL PROVIDER], [EMAIL PROVIDER] is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails stored in the account, including copies of emails sent from the account;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service

utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

d. All records pertaining to communications between [EMAIL PROVIDER] and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of the statutes listed on the warrant involving [SUSPECT] since [DATE], including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. [Insert specific descriptions of the electronic mail which your probable cause supports seizure and copying of; examples: "the sale of illegal drugs" "a threat to bomb a laboratory," "communications between John and Mary," "preparatory steps taken in furtherance of the scheme". Tailor the list to items that would be helpful to the investigation.]

b. Records relating to who created, used, or communicated with the account.

Appendix J

Sample Consent Form for Computer Search

CONSENT TO SEARCH COMPUTER/ELECTRONIC EQUIPMENT

I, _____, have been asked to give my consent to the search of my computer/electronic equipment. I have also been informed of my right to refuse to consent to such a search.

I hereby authorize _____ and any other person(s) designated by [insert Agency/Department] to conduct at any time a complete search of:

¤ All computer/electronic equipment located at _____. These persons are authorized by me to take from the above location: any computer hardware and storage media, including internal hard disk drive(s), floppy diskettes, compact disks, scanners, printers, other computer/electronic hardware or software and related manuals; any other electronic storage devices, including but not

limited to, personal digital assistants, cellular telephones, and electronic pagers; and any other media or materials necessary to assist in accessing the stored electronic data.

¤ The following electronic devices:

[Description of computers, data storage devices, cellular telephone, or other devices (makes, models, and serial numbers, if available)]

I certify that I own, possess, control, and/or have a right of access to these devices and all information found in them. I understand that any contraband or evidence on these devices may be used against me in a court of law.

I relinquish any constitutional right to privacy in these electronic devices and any information stored on them. I authorize [insert Agency/Department] to make and keep a copy of any information stored on these devices. I understand that any copy made by [insert Agency/Department] will become the property of [insert Agency/Department] and that I will have no privacy or possessory interest in the copy.

This written permission is given by me voluntarily. I have not been threatened, placed under duress, or promised anything in exchange for my consent. I have read this form; it has been read to me; and I understand it. I understand the _____ language and have been able to communicate with the agents/officers.

I understand that I may withdraw my consent at any time. I may also ask for a receipt for all things turned over.

Signed: _____ Signature of Witnesses: _____

Date and Time:_____ Date and Time:_____