

# Search and Seizure of Computers and Data: Annotated Bibliography

Kenneth J. Withers

June 25, 2004

## Cases

*Davis v. Gracey*, 111 F.3d 1472 (10th Cir. 1997). Seizure of a computer pursuant to a warrant was not invalidated by the incidental, concomitant seizure of the computer's "innocent contents," such as e-mail messages and stored software, where the computer was an "instrumentality of the crime."

*U.S. v. Bach*, 310 F.3d 1063 (8th Cir. 2002), *cert. denied*, 538 U.S. 993 (2003). Internet Service Provider (ISP) technicians searched the defendant's e-mail account for child pornography pursuant to a warrant faxed to them by a government agent. The fact that no government agent was present during the search was not a Fourth Amendment violation because the expertise of the ISP technicians to conduct the search was far superior to that of the agents, the items seized were located on the ISP's property, the search was authorized by a judge, and government agents complied with all provisions of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701.

*U.S. v. Bailey*, 272 F. Supp. 2d 822 (D. Neb. 2003). The defendant's subscription to the "Candyman" e-group, an Internet site that "frequently, obviously, unquestionably and sometimes automatically" distributes child pornography to subscribers, established probable cause for a search of the defendant's computer, even though there was no direct evidence that the defendant actually received child pornography. *See also U.S. v. Shields*, 2004 WL 832937 (M.D. Pa. Apr. 14, 2004) (denying defendant's motion to suppress evidence in a factually similar case and concurring with *Bailey's* reasoning).

*U.S. v. Barth*, 26 F. Supp. 2d 929 (W.D. Tex. 1998). After a repairman inadvertently discovered child pornography stored on the defendant's computer, agents conducted a broader, warrantless search of the computer in order to find additional evidence. The defendant's expectation of privacy in his computer files was not lost by his turning the computer over for repairs; thus, the agents' computer search required a warrant to the extent that it exceeded the scope of the repairman's private search. The defendant's motion to suppress all evidence was granted.

*U.S. v. Brunette*, 76 F. Supp. 2d 30 (D. Me. 1999), *aff'd*, 256 F.3d 14 (1st Cir. 2001). The district court suppressed evidence gathered from the defendant's computer after expiration of a warrant's deadline for completing the search. *But see U.S. v. Hernandez*, 183 F. Supp. 2d 468 (D.P.R. 2002) (evidence obtained by searching a seized computer five weeks after expiration of the search warrant was admissible). On the strength of remaining, admissible evidence, the defendant was convicted of possession of child pornogra-

---

The author gratefully acknowledges the assistance of Judge Jonathan Feldman (W.D.N.Y.), Judge Barbara Major (S.D. Cal.), and Judge Nan Nolan (N.D. Ill.) in preparing this bibliography.

phy. On appeal, the First Circuit held that the original search warrant erroneously relied on the officer's "conclusory assertion" that certain images met the statutory definition of child pornography. Absent independent review of the images by a judge or a more specific description of the images, the warrant lacked probable cause. Nevertheless, evidence seized under the warrant was admissible under the "good faith" exception to the exclusionary rule. The defendant's conviction was affirmed.

*U.S. v. Campos*, 221 F.3d 1143 (10th Cir. 2000). A warrant authorizing seizure of all computer equipment "which may be, or [is] used to depict child pornography" was not overbroad, since the warrant application explained why an on-site search was infeasible, the computer equipment was a probable "instrumentality of the crime," and the warrant limited the scope of a subsequent off-site search to files related to child pornography.

*U.S. v. Carey*, 172 F.3d 1268 (10th Cir. 1999). While conducting an authorized search of the defendant's computer for evidence of drug-related crimes, an agent discovered a file containing child pornography. A subsequent search for more evidence of child pornography exceeded the scope of the warrant and was an unconstitutional "general search." Neither the defendant's consent to a search of his apartment nor the "plain view" doctrine justified the agent's warrantless search for evidence of a non-drug-related crime. *But see U.S. v. Gray*, 78 F. Supp. 2d 524 (E.D. Va. 1999) (child pornography discovered while searching for evidence of computer-hacking crimes was admissible under the "plain view" doctrine); *U.S. v. Wong*, 334 F.3d 831 (9th Cir. 2003) (child pornography discovered while searching for evidence relating to the murder of defendant's girlfriend was admissible under the "plain view" doctrine).

*U.S. v. Caron*, 2004 WL 438685 (D. Me. Mar. 9, 2004). A computer repairman inadvertently found between five and seven images of child pornography while repairing the defendant's computer. An agent asked the repairman to open one such file prior to obtaining a search warrant. The Fourth Amendment was not violated because the agent did not exceed the scope of the repairman's "private search."

*U.S. v. Cervini*, 16 Fed. Appx. 865 (10th Cir. July 31, 2001). The fact that an ISP account registered to the defendant and listing his home address was used to post child pornography on the Internet gave rise to probable cause to search the defendant's home and home computer.

*U.S. v. Charbonneau*, 979 F. Supp. 1177 (S.D. Ohio 1997). The defendant did not have a reasonable expectation of privacy in e-mails related to child pornography that he sent to an on-line chat room. Thus, messages collected from the chat room by government agents were admissible. The defendant's wife did not validly consent to a search of the home when agents interrogated her and her teenage son at length and then threatened to execute their search warrant by breaking down the door to the home if she refused. Nevertheless, since the agents possessed a valid warrant at the time of the search, evidence was admissible under the inevitable discovery exception to the exclusionary rule.

*U.S. v. Fantauzzi*, 260 F. Supp. 2d 561 (E.D.N.Y. 2003). In a case stemming from the defendant's membership in a child-pornography-related e-group called "Candyman," the

defendant's motion to withdraw a guilty plea was denied. Although the evidence against the defendant was obtained under the same affidavit found defective in *U.S. v. Perez*, 247 F. Supp. 2d 459 (S.D.N.Y. 2003), *Perez* did not control this case because motions to withdraw guilty pleas and motions to suppress are decided under different standards. See also *U.S. v. Schmidt*, 96 Fed. Appx. 41 (2d Cir. 2004); *U.S. v. Hudak*, 2003 WL 22170606 (S.D.N.Y. Sept. 19, 2003).

*U.S. v. Fiscus*, 2003 WL 1963212 (10th Cir. Apr. 29, 2003). After receiving a tip that the defendant possessed child pornography in violation of his parole, agents conducted a warrantless search of the defendant's home and seized a home computer and co-located diskettes. Neither the original home search nor the agents' subsequent warrantless search of the computer and seized diskettes violated the Fourth Amendment, because warrants are not required for parole searches. See also *U.S. v. Tucker*, 305 F.3d 1193 (10th Cir. 2002).

*U.S. v. Gawrysiak*, 972 F. Supp. 853, *aff'd*, 178 F.3d 1281 (3d Cir. 1999). It was not "unreasonable" for agents to copy all of the defendant's computer files without ascertaining which files fell within the scope of a warrant when evidence indicated that the defendant's business dealings were "pervaded" by fraudulent activity, selection and copying of only crime-related computer files was likely to be time-consuming, and file copying was chosen over outright seizure of the defendant's computer as the "least intrusive" search method available.

*U.S. v. Gleich*, 293 F. Supp. 2d 1082 (D.N.D. 2003). Agents did not exceed the scope of a warrant authorizing the search of the defendant's home and home computer by seizing and searching three computers found in the home, since any of the three could have contained the evidence of child pornography that investigators were seeking.

*U.S. v. Grant*, 218 F.3d 72 (1st Cir.), *cert. denied*, 531 U.S. 1025 (2000). Evidence showing that the Internet screen name registered to the defendant was used to access child pornography while the defendant was physically present in the home gave rise to probable cause to search the defendant's home.

*U.S. v. Gray*, 78 F. Supp. 2d 524 (E.D. Va. 1999). An agent's "routine practice" of opening virtually every single file contained in a computer hard drive was not an unconstitutional general search. The defendant was exceptionally computer savvy, and evidence of computer hacking could have been stored anywhere on the computer. Thus, files related to child pornography discovered while the agent was searching for hacking evidence were in "plain view." See also *U.S. v. Wong*, 334 F.3d 831 (9th Cir. 2003) (child pornography discovered while searching for evidence relating to the murder of the defendant's girlfriend was admissible under "plain view" doctrine); *but see U.S. v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (search for evidence of child pornography exceeded scope of search for evidence of drug-related crimes).

*U.S. v. Greathouse*, 297 F. Supp. 2d 1264 (D. Or. 2003). Agents obtained a search warrant for the defendant's residence, a single-family home. The warrant authorized the sei-

zure of “any and all” computers and computer equipment that contained or depicted child pornography. The agents did not exceed the scope of the warrant by seizing all eight computers found in the residence, most of which did not belong to the defendant, because the agents were unaware that the single-family home was shared by five adults. The court suggested in dicta that a more tailored search would most likely have been required had the agents known others resided in the home. Evidence was suppressed on other grounds, namely that the lapse of thirteen months between receipt of a tip that the defendant possessed child pornography and warrant application rendered the evidence too stale to support probable cause. *But see U.S. v. Lacy*, 119 F.3d 742 (9th Cir. 1997) (evidence was not stale despite lapse of ten months before warrant application); *U.S. v. Hay*, 231 F.3d 630 (9th Cir. 2000) (evidence was not stale despite six-month lapse).

*U.S. v. Grimes*, 244 F.3d 375 (5th Cir. 2001). The Fourth Amendment was not violated when agents viewed images discovered by a computer repairman, because the agents did not exceed the scope of the repairman’s private search. The defendant’s possession of images of nude children constituted illegal possession of child pornography, although the children’s “private areas” had been obscured using computer pixel manipulation.

*U.S. v. Habershaw*, 2001 WL 1867803 (D. Mass. May 13, 2001). Agents arrived at the defendant’s residence to investigate reports of a man yelling obscenities at a group of small children. The defendant gave the agents permission to enter his apartment, where agents spotted a computer monitor displaying the message list of a child-pornography-related newsgroup. The defendant gave the agents permission to search the computer, and the agents discovered child pornography. The court found that the defendant validly consented to the search; that the subsequent search warrant, authorizing the search of “any and all” computer equipment, was not overbroad; and that the agents’ search of the computer after the warrant expired was not a “second execution” of the warrant or a “failure to depart the premises,” as the defendant claimed. The court denied the defendant’s motion to suppress. *See also U.S. v. Hernandez*, 183 F. Supp. 2d 468 (D.P.R. 2002) (evidence obtained by searching a seized computer five weeks after expiration of the search warrant was admissible); *but see U.S. v. Brunette*, 76 F. Supp. 2d 30 (D. Me. 1999) (evidence was suppressed when computer search was conducted after warrant expired).

*U.S. v. Hall*, 142 F.3d 988 (7th Cir. 1998). Seizure of an entire computer was justified when the warrant narrowly described the child pornography files sought, since agents would not, under the terms of the warrant, be free to rummage through the defendant’s property.

*U.S. v. Harding*, 273 F. Supp. 2d 411 (S.D.N.Y. 2003). A warrant authorized agents to seize Zip disks and to open and inspect their contents for evidence of fraud and possession of child pornography. The court held that whether or not that portion of the warrant relating to child pornography lacked probable cause, child pornography evidence was nevertheless admissible under the “inevitable discovery” doctrine, since agents would have discovered it while searching for evidence of fraud.

*U.S. v. Hay*, 231 F.3d 630 (9th Cir. 2000), *cert. denied*, 534 U.S. 858 (2001). A warrant authorizing “generic” seizure of all of the defendant’s hardware and software was sufficiently particular because government officials had no way of knowing where child pornography images might be stored. A lapse of six months between documented transmission of child pornography to the defendant’s computer and the government’s application for a warrant did not render the application stale, since collectors of child pornography typically retain images for long periods of time. *But see U.S. v. Greathouse*, 297 F. Supp. 2d 1264 (D. Or. 2003) (lapse of thirteen months between government receiving tip that defendant possessed child pornography and warrant application rendered evidence too stale to support probable cause).

*U.S. v. Hernandez*, 183 F. Supp. 2d 468 (D.P.R. 2002). Noting that computer seizures are analogous to seizures of large quantities of paper documents, the court held that agents are permitted to remove computer equipment from searched premises and examine it at a later date without obtaining a warrant extension. Thus, in this case, evidence of child pornography uncovered during a computer search conducted five weeks after the original warrant expired was admissible. *See also U.S. v. Habershaw*, 2001 WL 1867803 (D. Mass. May 13, 2001) (agents’ search of a seized computer after expiration of a warrant was not “second execution” of the warrant or “failure to depart the premises,” as defendant claimed; thus, the evidence found was admissible); *but see U.S. v. Brunette*, 76 F. Supp. 2d 30 (D. Me. 1999) (evidence was suppressed when computer search was conducted after warrant expired).

*U.S. v. Hunter*, 13 F. Supp. 2d 574 (D. Vt. 1998). During an investigation of an attorney suspected of money laundering, a search warrant authorizing the seizure of “all” computers, storage devices, and software systems from the defendant violated the particularity requirement of the Fourth Amendment. However, the detailed search protocol attached to the warrant application ensured that agents would retrieve relevant files without undue intrusion; thus, the “good faith” exception to the exclusionary rule applied. When a computer search involves potentially privileged documents, screening should be performed by a special master or magistrate judge (although screening in this case by agents who were separated from the prosecutor by a “Chinese Wall” was deemed acceptable).

*U.S. v. Lacy*, 119 F.3d 742 (9th Cir. 1997), *cert. denied*, 523 U.S. 1101 (1998). A lapse of ten months between transmission of images to the defendant’s computer and warrant application did not render evidence too stale to support probable cause, since collectors of child pornography typically retain images for long periods of time. *But see U.S. v. Greathouse*, 297 F. Supp. 2d 1264 (D. Or. 2003). Generic seizure of computer equipment did not violate the Fourth Amendment, since the warrant specified that only child pornography files would be searched. Under 18 U.S.C. § 2252(a)(4)(B), which requires that the defendant must knowingly possess “3 or more books, magazines, periodicals, films, video tapes, or other matter,” “matter” describes the physical medium that contains the child pornography, not the image itself. Thus, the statute criminalizes possession of three or more computer storage devices containing child pornography, *not* three or more image files stored on those devices. The conviction was affirmed. *But see U.S. v. Vig*, 167 F.3d

443 (8th Cir. 1999) (possession of three or more images stored on a single computer hard drive violates the statute).

*U.S. v. Maxwell*, 45 M.J. 406 (C.A.A.F. 1996). The defendant had a reasonable expectation of privacy in his password-protected e-mails. A warrant authorized a search of *one* user name associated with the defendant's "America Online" (AOL) e-mail account, but searches of *all* user names billed to the defendant were conducted. Evidence gathered by searching the user name account that was *not* listed in the warrant was suppressed. The defendant was originally convicted on four counts relating to using his computer to transport obscenity and child pornography; the appellate court vacated the conviction on two counts, affirmed it on two counts, and remanded the case for a rehearing on the sentence.

*U.S. v. Perez*, 247 F. Supp. 2d 459 (S.D.N.Y. 2003). Evidence that the defendant subscribed to the child-pornography-related e-group called "Candyman" absent affirmative evidence that the defendant had actually downloaded, transmitted, or received child pornography, did not provide probable cause for the search of the defendant's home and seizure of his computer equipment. The defendant's motion to suppress was granted. *See also U.S. v. Strauser*, 247 F. Supp. 2d 1135 (E.D. Mo. 2003) (same); *but see U.S. v. Bailey*, 272 F. Supp. 2d 822 (D. Neb. 2003) (concluding that the "Candyman" investigation's defective affidavit did not necessitate suppression of evidence).

*U.S. v. Rossby*, 2003 WL 22682592 (9th Cir. Nov. 10, 2003). The defendant's written consent to a "complete search" of his office—including permission to seize "any letters, papers, materials, or other property which [officers] may desire"—reasonably included consent to search the contents of the defendant's laptop computers for evidence of mail and wire fraud.

*U.S. v. Simons*, 206 F.3d 392 (4th Cir. 2000), *cert. denied*, 534 U.S. 930 (2001). Where a workplace had a clearly articulated policy of monitoring employee use of the Internet, the defendant, a government employee, did not have a reasonable expectation of privacy in files downloaded onto the hard drive of his office computer. The warrantless search of the defendant's hard drive by remote computer and seizure of his hard drive without notice upon discovery that it contained child pornography did not violate the Fourth Amendment. *See also U.S. v. Bailey*, 272 F. Supp. 2d 822, 824 (D. Neb. 2003) (defendant did not have a reasonable expectation of privacy in files on his workplace computer after agreeing to be "monitored for appropriate use").

*U.S. v. Slanina*, 283 F.3d 670 (5th Cir.), *vacated on other grounds*, 537 U.S. 802 (2002), *conviction aff'd on remand*, 359 F.3d 356 (5th Cir. 2004). The defendant, a government employee, had a reasonable expectation of privacy in files stored on his work computer because his employer did not inform employees that computer and Internet usage would be monitored. Nevertheless, after a computer repairman discovered evidence of child pornography on the defendant's computer, the government employer did not violate the Fourth Amendment by searching the computer as part of an investigation of work-related misconduct.

*U.S. v. Smith*, 27 F. Supp. 2d 1111 (C.D. Ill. 1998). The defendant's girlfriend, who contacted the police to report that child pornography was stored on the defendant's home computer, validly consented to a warrantless search of the computer because the girlfriend lived in the defendant's home and had free physical access to the computer, the defendant had encouraged her and others to use the computer in the past, and the computer was not password protected.

*U.S. v. Syphers*, 296 F. Supp. 2d 50 (D.N.H. 2003). The government did not act unreasonably by retaining the defendant's computer for seven months while searching for evidence of child pornography. Investigators received a one-year extension to the original warrant, they had an "overwhelming backlog" of computer crime investigations, and the defendant's possession of over 64,000 images of child pornography, some of which required de-encryption before they could be presented as evidence made the search time-consuming.

*U.S. v. Tank*, 200 F.3d 627 (9th Cir. 2000). A search of the defendant's car incident to his lawful arrest, which resulted in the seizure of a Zip disk later found to contain child pornography, was not a violation of the Fourth Amendment.

*U.S. v. Triumph Capital Group, Inc.*, 211 F.R.D. 31 (D. Conn. 2002). In this public corruption case, a computer search warrant provided that agents would make "every effort" to review only those files that responded to a "key-word search," since many documents contained on the computer were privileged. The warrant also approved the agents' use of a taint-team procedure to screen out privileged documents. After conducting several key-word searches, agents conducted a thorough, file-by-file search of the hard drive. Denying the defendants' subsequent motion to suppress, the court held that key-word searches are of limited usefulness; thus, agents acted reasonably by resorting to other search techniques. The fact that the warrant indicated a preference for a particular search method did not prevent agents from using other methods.

*U.S. v. Turner*, 169 F.3d 84 (1st Cir. 1999). After obtaining the defendant's consent to search his apartment in connection with an intruder's assault upon his next-door neighbor, an agent observed a photograph of a nude woman on the defendant's computer. The agent searched the computer for more such images and discovered evidence of child pornography. The district court granted the defendant's motion to suppress, since the computer search exceeded the scope of the defendant's original consent to search. The First Circuit affirmed.

*U.S. v. Upham*, 168 F.3d 532 (1st Cir.), *cert. denied*, 527 U.S. 1011 (1999). A warrant authorizing "generic" seizure of "any and all computer software and hardware" was not unconstitutionally overbroad when there was probable cause to believe that the computer had been used to store and transmit images of child pornography. Prior to seizure the defendant had deleted some 1,400 pornographic images, which the government uncovered using a "specialized utility program." This did not exceed the authority of the warrant, which was concerned with *what* could be searched, not with *how* the search was to be carried out.

*U.S. v. Vig*, 167 F.3d 443 (8th Cir. 1999). Possession of three or more images stored on *one* computer hard drive satisfies the requirement that the defendant must knowingly possess “3 or more books, magazines, periodicals, films, video tapes, or other matter” depicting a minor in a sexually explicit manner. 18 U.S.C. § 2252(a)(4)(B). *But see U.S. v. Lacy*, 119 F.3d 742 (9th Cir. 1997).

*U.S. v. Wong*, 334 F.3d 831 (9th Cir. 2003). Child pornography discovered while searching the defendant’s computer for evidence related to his girlfriend’s murder was admissible under “plain view” doctrine. *See also U.S. v. Gray*, 78 F. Supp. 2d 524 (E.D. Va. 1999) (child pornography discovered while searching for evidence of computer-hacking crimes was admissible under “plain view” doctrine); *but see U.S. v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (child pornography discovered while searching for evidence of drug-related crimes was not admissible under “plain view” doctrine).

*U.S. v. Zimmerman*, 277 F.3d 426 (3d Cir. 2002). An affidavit stating that the defendant had been accused of sexually abusing minors and that he may have showed an image of adult pornography to minors six months before did not provide probable cause for a search of the defendant’s home, including his home computer, for child pornography. The “good faith” exception to the exclusionary rule did not apply, since it was “entirely unreasonable” for agents to believe the warrant was valid. The district court’s order denying the defendant’s motion to suppress was reversed, the defendant’s conviction and sentence were vacated, and the case was remanded.

## **Periodical Articles**

Amy Baron-Evans, *When the Government Seizes and Searches Your Client’s Computer*, 27 *Champion Mag.* 18 (June 2003).

Amy Baron-Evans & Martin F. Murphy, *The Fourth Amendment in the Digital Age: Some Basics on Computer Searches*, 47 *Boston Bar J.* 10 (June 2003).

Stephan K. Bayens, *The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?*, 48 *Drake L. Rev.* 239 (2000).

Hon. Robert H. Bohn, Jr. & Lynn S. Muster, *The Dawn of the Computer Age: How the Fourth Amendment Applies to Warrant Searches and Seizures of Electronically Stored Information*, 8 *Suffolk J. Trial & App. Advoc.* 63 (2003).

Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 *Mich. Telecomm. & Tech. L. Rev.* 39 (2002), available at <http://www.mttlr.org/voleight/Brenner.pdf>.

Jim Dowell, Note, *Criminal Procedure: Tenth Circuit Erroneously Allows Officers’ Intentions to Define Reasonable Searches*: *United States v. Carey*, 54 *Okla. L. Rev.* 665 (2001).

Rachel J. Hess, *Search and Seizure of E-Evidence in Illinois: Cybercrime and the Internet Frontier*, 91 Ill. B.J. 344 (2003).

Anton L. Janik, Jr., *Combating the Illicit Internet: Decisions by the Tenth Circuit to Apply Harsher Sentences and Lessened Search Requirements to Child Pornographers Using Computers*, 79 Denv. U. L. Rev. 379 (2002).

Michael K. McChrystal, William C. Gleisner III & Michael J. Kuborn, *Law Enforcement in Cyberspace: Search and Seizure of Computer Data*, 71 Wis. Law. 35 (Dec. 1998).

Robin Cheryl Miller, *Validity of Search or Seizure of Computer, Computer Disk, or Computer Peripheral Equipment*, 84 A.L.R. 5th 1 (2004).

Francisco J. Navarro, Comment, *United States v. Bach and the Fourth Amendment in Cyberspace*, 14 Alb. L.J. Sci. & Tech. 245 (2003).

Donald Resseguie, Note, *Computer Searches and Seizure*, 48 Clev. St. L. Rev. 185 (2000).

Carla Rhoden, *Challenging Searches and Seizures of Computers at Home or in the Office: From a Reasonable Expectation of Privacy to Fruits of the Poisonous Tree and Beyond*, 30 Am. J. Crim. L. 107 (2002).

Laurence H. Tribe, *The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier*, *The Humanist*, Sept.–Oct. 1991, at 15, available at <http://www.sgrm.com/art1.htm>.

Amy E. Wells, Comment, *Criminal Procedure: The Fourth Amendment Collides with the Problem of Child Pornography and the Internet*, 53 Okla. L. Rev. 99 (2000).

Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75 (1994).

### **Other Secondary Sources**

Mitchell Kapor & Mike Godwin, *Civil Liberties Implications of Computer Searches and Seizures: Some Proposed Guidelines for Magistrates Who Issue Search Warrants*, at <http://www.sgrm.com/art-5.htm>.

*Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, United States Dept. of Justice, July 2002, at <http://www.cybercrime.gov/s&smanual2002.htm>.