Special Needs Offenders Close-up

FEDERAL JUDICIAL CENTER

APRIL 2002

Cyber Crime and Cyber Terrorism

by Mark Sherman

Federal Initiatives Take on Cyber Terrorism

what's NEW

The federal government has recently taken several steps against cyber crime and cyber terrorism. Cyber crime includes child sexual exploitation, fraud, hacking, and software and recording piracy. Cyber terrorism, which is conducted by both international and domestic organizations, includes politically motivated crimes designed to generate fear, such as attacks that lead to death or bodily injury, explosions, severe economic loss, or attacks against critical infrastructures.

In July 2001 the Justice Department announced the formation of ten Computer Hacking and Intellectual Property (CHIP) units based in U.S. attorneys' offices across the country and dedicated to prosecuting cyber crime. In the aftermath of September 11, the White House announced the appointment of a special advisor for cyberspace security. In addition, the FBI announced an overhaul of its top management that places more emphasis on counterterrorism and cyber crime. Included in this overhaul is the creation of a new division on cyber crime within the Bureau's criminal investigation section.

Perhaps the most far-reaching federal initiative has been enactment of the post-September 11 USA Patriot Act. While the Act does not directly affect the work of probation and pretrial services officers, it is a major law enforcement initiative that amends various sections of the United States Code. With regard to cyber crime and cyber terrorism, this new law

- amends the Electronic Communications Privacy Act (ECPA) (18 U.S.C. §2703) to allow investigators to use warrants obtained under ECPA to compel records outside of the district in which the issuing court is located, thus enabling courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of agents, prosecutors, and judges in the districts where major Internet service providers (ISPs) are located
- amends the computer hacking statute (18 U.S.C. §1030) by 1) increasing to a maximum of 20 years the prison sentence for hackers who damage protected computers, 2) clarifying the mens rea required for such offenses to make explicit that a hacker need only intend damage, not a particular type of damage, 3) adding a new offense for damaging computers used for national security or criminal justice, 4) expanding the coverage of the statute to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce, 5) counting state convictions as prior offenses for purposes of recidivist sentencing enhancements, 6) allowing losses to be aggregated for purposes of meeting the $5,000 jurisdictional threshold, and 7) instructing the U.S. Sentencing Commission to amend the appropriate guidelines
- amends the wiretap statute (18 U.S.C. §2516) by adding felony violations of the computer hacking statute (18 U.S.C.

About *Special Needs Offenders Close-up*

Close-up brings the field up to date on recent developments and district-based initiatives related to defendant and offender populations covered by the original Special Needs Offenders series. It includes population-specific news, information on the latest investigation and supervision approaches, job aids, information about training, and descriptions of practices and innovations developed by individual offices. *Close-up* will be accompanied by a live FJTN broadcast and topical discussion on the Court Operations Exchange. Consult the *FJTN Bulletin* for broadcast information. Both the FJTN Bulletin and Court Operations Exchange can be accessed through the Center's DCN site at http://jnet.fjc.dcn.

§1030) to the list of predicate offenses for the interception of communications

- ❍ changes the way in which the wiretap statute and ECPA apply to stored voice communications so that law enforcement can obtain such communications using the procedures set out in ECPA (such as a search warrant) rather than those in the wiretap statute (such as a wiretap order)
- ❍ amends 18 U.S.C. §2702 to permit but not require an ISP to disclose to law enforcement either content or non-content customer records in emergencies involving immediate risk of death or serious physical injury to any person. This amendment also allows ISPs to disclose information to protect their rights and property.
- ❍ allows victims of computer attacks to authorize authorities or others acting under color of law to monitor trespassers on their computer systems. Authorities will be able, after obtaining permission from the owner of the protected computer, to intercept the communications of a computer trespasser transmitted to, through, or from a protected computer.
- ❍ requires the Attorney General to establish regional computer forensic labs and to provide support for existing labs to enable them to provide certain forensic and training capabilities

Note: For further guidance on cyber-specific aspects of the USA Patriot Act, see the Justice Department's Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, *http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm.*

AO/OPPS Assists Field with Cyber Crime

The Administrative Office of the U.S. Courts and its Office of Probation and Pretrial Services (OPPS) are also addressing cyber crime. In September 2001, the AO published a special issue of *Federal Probation* about technology and corrections. The issue contains several articles by officers with expertise in sentencing and supervision of cyber offenders and defendants. In January 2002 OPPS distributed cyber crime training materials to all probation and pretrial services chiefs. These materials, produced by the National White Collar Crime Center (NW3C) and the National Cybercrime Training Partnership, included the CD-ROMs *The Internet as an Investigative*

Use of computers, networks, and connected devices alleged in planning and financing of terrorist attacks

The following incidents illustrate that members of terrorist organizations are using computers, networks, and connected devices to carry out their work and that such use varies in sophistication. In light of the heightened federal law enforcement focus on terrorism, it is possible that more individuals with ties, or alleged ties, to terrorist organizations will be subject to federal probation and pretrial services supervision. Thus, it is important that officers understand how these individuals are using computers, networks, and connected devices.

In December 2001 the *Wall Street Journal* reported that two of its reporters purchased a desktop computer from a looter in Kabul that allegedly had been used by al Qaeda members. The hard drive contained a memo referring to a "legal study" regarding the killing of civilians and letters referring to the "great value" of attacks on Americans and Jews and to an interview to be conducted by al Qaeda members posing as journalists with anti-Taliban leader Ahmed Shah Massoud. Massoud was killed by a bomb on September 9 during the interview. Other files included a video of people fleeing the World Trade Center on September 11 and an outline of a project to develop chemical and biological weapons. A number of files were encrypted using Windows 2000's standard 40-bit DES Encrypting File System. It took the *Journal* five days to crack the encryption keys.

A related story said that a joint investigation by the Treasury and Justice departments, the FBI, and other federal agencies found that the September 11 operation was financed through wire transfers and credit card and ATM transactions tied to a bank account in Dubai, United Arab Emirates.

In January, reports surfaced that Richard Reid, accused of trying to blow up an American Airlines flight with bombs hidden in his shoes, sent several e-mails about the bombing from a Paris cyber café to contacts in Pakistan in the days before he boarded the plane. Also in January, the FBI issued an alert to law enforcement agencies and the Nuclear Regulatory Commission warning that al Qaeda may have been probing Web sites, including some dealing with nuclear information.

Tool and *Prosecuting Cases that Involve Computers* and the VHS videotape *Cyber Crime Fighting: The Law Enforcement Officer's Guide to Online Crime*. In addition, the AO is studying the possibility of including information on supervision of cyber crime offenders in the revised Monograph 109.

The Center is grateful to OPPS and Office of General Counsel personnel on the Center's planning committee for this cyber crime and cyber terrorism *Close-up*.

On-line Cyber Crime Information Networks for Federal Probation and Pretrial Services

Two on-line cyber crime resources specifically for federal probation and pretrial services officers are now available. Cyber Crime Information Resources contains cyber crime news, discussion forums, an on-line library, links of interest, and a substantial forensics and utility software archive. The site is for the exclusive use of federal probation and pretrial services. To apply for access, go to http://www.cybercrime.flmp.uscourts.gov.

Supervision of the Cyber-savvy Offender or Defendant is a listserv (e-mail forum) maintained by the Eastern District of New York and facilitated by federal probation and pretrial services officers from several districts. Topics range from basic to advanced. Membership is open to federal court employees. Topics include reviews of monitoring and forensics software, development of cyber-specific special conditions and policies, and training opportunities. To join, register at http://apollo.nyed.circ2.dcn/cgi-bin/wa?SUBED1=cybercrime&A=1.

The Court Operations Exchange is an electronic forum maintained by the Federal Judicial Center for court staff to share information and ideas. The Exchange contains topical discussions related to cyber crime. To gain access, log onto the Center's DCN intranet site at http://jnet.fjc.dcn, click "Court Staff Education," then scroll down the menu and click "Court Operations Exchange."

New Cyber Crime Manuals

In 2001 the Justice Department produced two manuals for law enforcement officers working cases that involved computers. While both are designed for officers carrying out criminal investigations, federal probation and pretrial services officers have found them helpful in planning and conducting searches of defendants' and offenders' computers.

Cyber-specific special conditions: recent case law

In *United States v. Peterson,* 248 F.3d 79 (2d Cir. 2001), the U.S. Court of Appeals for the Second Circuit held that a special condition of probation absolutely barring the defendant's use of computers or the Internet was unreasonable since such use was not reasonably related to the defendant's current or prior offenses, especially since the defendant was consistently employed in computer-related jobs. The defendant had pleaded guilty to bank larceny in connection with his failing computer business. He had a prior state court sex-offense conviction, which had not involved computer use.

In *United States v. White,* 244 F.3d 1199 (10th Cir. 2001) the U.S. Court of Appeals for the Tenth Circuit held that a special condition of supervised release that prohibited the defendant, who had been convicted of receiving child pornography but had not used a computer to do so, from "possessing a computer with Internet access" was ambiguous and remanded the case to the district court for clarification. The court noted that the condition was "at the same time potentially too narrow and overly broad" and did not comport with either statutory requirements or "the realities of the Internet and its rapidly changing technologies."

In *United States v. Walser,* 275 F.3d 981 (10th Cir. 2001) the U.S. Court of Appeals for the Tenth Circuit affirmed the district court's imposition of a special condition barring the defendant's use of or access to the Internet without the prior permission of the U.S. probation officer. The case involved a conviction for possession of child pornography that had been downloaded from the Internet onto the defendant's personal computer. In upholding the condition, the court stated that "the condition of release is not as ill-tailored as the one at issue in *White* [because the defendant] is not completely banned from using the Internet. Rather, he must obtain prior permission from the probation office. Thus, the condition more readily accomplishes the goal of restricting use of the Internet and more delicately balances the protection of the public with the goals of sentencing."

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations provides specific guidance for carrying out computer searches to comply with constitutional and statutory guidelines. (Available at http://www.cybercrime.gov/searchmanual.htm)

Electronic Crime Scene Investigation: A Guide for First Responders provides specific information on different computer systems, components, and connected devices and guidance on securing and documenting the scene; collecting evidence; packaging, transporting, and storing evidence; and conducting forensic examination. (Available at http://www.ncjrs.org. Click on "Law Enforcement" and "computer-related crime.")

The U.S. Secret Service and International Association of Chiefs of Police have developed *Best Practices for Seizing Electronic Evidence*, a pocket-sized, laminated guide that identifies issues and provides advice and tips related to search and seizure of electronic evidence. (Available from the U.S. Secret Service, Financial Crimes Division, Electronic Crimes Branch, (202) 406-5850).

Cutting-Edge Cyber Crime-Control Practices of U.S. Probation and Pretrial Services

In-district resource coordination

Several districts have developed coordinator, specialist, or resource positions in which a skilled officer or team of officers lead case consultation and anti-cyber-crime initiatives.

Ohio Northern probation named two officers as computer crime coordinators who focused on understanding computer crime, collecting information about computer offenders in the district, examining U.S. Sentencing Guidelines implications for criminal computer use, assessing the risk posed by computer offenders, developing investigative and supervision techniques regarding computer offenders, and developing cyber-specific special conditions. With the approval of the chief, one of the coordinators initiated the Northern Ohio Probation Cybercrime Working Group, which consists of the chief and members of the management team, probation officers, and representatives from the office's automation unit. After the working group identified several needed tasks and duties, the district created a specialist posi-

Terrorism and national security amendments to the Sentencing Guidelines

The U.S. Sentencing Commision's 2001 amendments addressed terrorism and national security. While the amendments do not speak to the use of computers or connected devices, they involve offenses in which computers or connected devices may be instruments.

- §2L1.2(b)(1)(A)(v) now provides for a 16-level increase where a defendant previously was deported or unlawfully remained in the United States after a conviction for a felony that is a national security or terrorism offense.
- §2M5.1(a)(1) now provides for a base offense level of 26 for evasion of export controls if national security controls or controls related to the proliferation of nuclear, biological, or chemical weapons or materials were evaded.
- §2M5.2(a)(1) now provides for a base offense level of 26 for export of arms, munitions, or military equipment or services without a required validated export license.
- §2M6.1, which was substantially amended, now provides three alternative base offense levels and various enhancements for unlawful production, development, acquisition, stockpiling, alteration, use, transfer, or possession of nuclear material, weapons, or facilities; biological agents, toxins, or delivery systems; chemical weapons; or other weapons of mass destruction.
- §2S1.1 and §2S1.2 were consolidated. Among other things, the new guideline §2S1.1 provides a six-level enhancement for third-party money launderers who knew or believed that any of the laundered funds were the proceeds of, or were intended to promote, certain types of more serious underlying criminal conduct including but not limited to offenses involving national security and terrorism.

For more on the USSC's reasons for these amendments, see its *Guidelines Manual Supplement to Appendix C* (2001). A "reader-friendly" version of the amendments can be downloaded from the USSC's Internet Web site at *http://www.ussc.gov/guidelin.htm.*

tion. The officer occupying the position had served as the district's primary computer crime coordinator and has received extensive cyber crime-related technical training from SEARCH, the Federal Law Enforcement Training Center (FLETC), and the National Cybercrime Training Partnership/National White Collar Crime Center (NCTP/NW3C).

For more information, contact USPO Art Bowker at Arthur_Bowker@ohnp.uscourts.gov. Also, read "Computer Crime in the 21st Century and Its Effect on the Probation Officer" (*Federal Probation*, Sept. 2001), which Bowker co-authored with Indiana Southern USPO Gregory S. Thompson. The article is available at http://jnet.ao.dcn/courtoperations/fcsd/html/federalprob.htm. For more information on training provided by SEARCH, FLETC, and NW3C, see Training∫, page 10 of this *Close-up*.

New York Eastern probation's computer crime specialist is a member of the district's search enforcement team and the Middle Atlantic–Great Lakes Organized Crime Law Enforcement Network, serves as evidence technician and ChoicePoint liaison, and represents the district on the New York Electronic Crimes Task Force and the High Tech Crime Consortium. The specialist received training from NW3C.

For more information, contact Sr. USPO Brian Kelly at Brian_Kelly@nyep.uscourts.gov. Also, see Kelly's article "Supervising the Cyber Criminal" (*Federal Probation* Sept. 2001), which is available at http://jnet.ao.dcn/courtoperations/fcsd/html/federalprob.htm.

Florida Middle probation created an electronic information specialist position. The specialist, who is responsible for conducting forensic examination of offenders' computers, when authorized, is certified in specific types of programming and has received forensics training from NW3C and FLETC.

Texas Western pretrial services has created the position of field automation and electronic monitoring specialist. With regard to automation, the specialist develops the district's cyber crime resources, policies, and training and consults on cyber crime cases. The specialist has received training in computer forensics from FLETC and is a member of the U.S. attorney's computer crime investigators work group.

For more information, contact Sr. USPSO Lanny Newville at Lanny_L_Newville@txwpt.uscourts.gov. Also, see Newville's article "Cyber Crime and the Courts—Investigating and Supervising the Information Age Offender" (*Federal Probation*, Sept. 2001), which is available at http://jnet.ao.dcn/courtoperations/fcsd/html/federalprob.htm.

New York Western (combined) and **South Carolina** probation have informally designated at least one officer in each district to serve as the computer "go-to" person on cyber crime cases. In New York Western the designated officer has obtained forensics training from NW3C and the International Association of Computer Investigative Specialists (IACIS) and belongs to the local Law Enforcement Crime Consortium, which maintains a regional computer forensics lab. The designated officer in South Carolina has an advanced degree in information technology, heads the district's cyber crime task force, conducts in-district cyber crime training, and has completed a needs assessment on cyber crime for the district.

For more information, contact USPO Kathleen Horvatits at Kathleen_Horvatits@nywp.uscourt.gov and USPO Monica Hampton at Monica_Hampton@scp.uscourts.gov.

Arizona pretrial services has designated two officers as computer crime coordinators (special assignment). These officers participated in the NW3C Basic Data Recovery and Analysis class and will attend computer forensic software training in May 2002. They have drafted a computer crime supervision and search policy, which is currently under review in the district. The district uses monitoring software to monitor defendants' computer use.

For more information, contact USPSO Ruben Morales at Ruben_Morales@azd.uscourts.gov.

District of Columbia probation has designated a line officer and a supervisor as automation coordinators. They discuss cyber crime issues and determine training needs. The line officer supervises the district's cyber crime offenders as part of a regular caseload and serves as liaison between the office's systems staff and end users. Both coordinators serve on the district's automation committee, which consists of at least one member from each unit in the office, (i.e. supervision and presentence officers, SUSPOs, probation assistants, and the systems group). The committee meets monthly to review the office's computer needs related to research and development of programs, reliability of programs and equipment, training of staff, long-range planning, security, and accountability of the systems group.

For more information, contact USPO Andre Wilson at Andre_Wilson@dcp.uscourts.gov.

Kansas (combined) has formed a High-Tech and Computer Crime Team consisting of three officers from different offices and staff from the district's systems department. The

team, which serves as a computer crime resource, takes the lead on development of in-district cyber crime policy, training, and practice. The district has developed a search policy that incorporates information on searching offender computers, a computer restriction and monitoring program for offenders with a cyber-specific special condition, and training for both probation staff and the court.

For more information, contact USPO Shawn Brewer at Shawn_Brewer@ksp.uscourts.gov, USPO Michelle Caples at Michelle_Caples@ksp.uscourts.gov, or USPO Bryce Beckett at Bryce_Beckett@ksp.uscourts.gov.

Information gathering

New York Eastern and **Ohio Northern** probation have developed forms to gather an offender's computer and Internet data. The forms contain questions about the offender's computer hardware, software, and Internet accessibility and use, including passwords and ISPs.

For more information, contact Sr. USPO Brian Kelly at Brian_Kelly@nyep.uscourts.gov or USPO Art Bowker at Arthur_Bowker@ohnp.uscourts.gov.

Computer search policies

Some probation offices have developed search policies that address searches of computers and connected devices. Similarly, because the practice by courts in some districts has been to order search conditions at the pretrial stage, some pretrial services offices have developed cyber search policies.

Development of computer search and seizure policies by federal probation and pretrial services officers should begin with the Criminal Law Committee's Model Search and Seizure Guidelines. The Guidelines are based on the premise that "while searches by probation officers may occasionally be justified, they are disfavored and should be discouraged." Searches or seizures of any kind by pretrial services officers are not authorized by statute and are not included in the Guidelines. They should not be performed unless ordered by the court.

Part of the "Memorandum to U.S. District Judges, U.S. Magistrate Judges, and Chief Probation Officers on Searches and Seizures" (May 3, 1993), the Model Search and Seizure Guidelines are contained in the Federal Judicial Center's *Search and Seizure: Training Reference Guide* (1995). For more information on applying the guidelines to cyber searches and seizures, see the Center's August 2000 *Special Needs Offenders Bulletin: Introduction to Cyber Crime* (hereafter, *Introduction to Cyber Crime*), which is available at http://156.132.47.230:8081/newweb/jnetweb.nsf/pages/66. For opinions of the AO Office of General Counsel on cyber crime search and seizure policies, go to http://jnet.ao.dcn/courtoperations/fcsd/html/search__seizure.htm.

Kansas (combined) has developed a search policy that incorporates searches and seizures of computers and connected devices. The AO Office of General Counsel has issued a positive opinion of the policy.

For more information, contact USPO Shawn Brewer at Shawn_Brewer@ksp.uscourts.gov, USPO Michelle Caples at Michelle_Caples@ksp.uscourts.gov, or USPO Bryce Beckett at Bryce_Beckett@ksp.uscourts.gov.

Arizona pretrial services is developing a computer crime supervision and search policy to help officers conduct searches pursuant to special conditions ordered by the court. The draft policy includes sections on statutory authority, purpose, policies, plain view, consent, conduct of searches, and processing evidence. The draft policy has not been reviewed by the AO Office of General Counsel.

For more information, contact USPSO Ruben Morales at Ruben_Morales@azd.uscourts.gov.

Special conditions

New York Eastern probation has developed a bench guide to assist judges with such issues as classification and wording of special conditions. The guide includes the following cyber-specific special conditions:

- The defendant is not permitted to access a computer or connected device (except a landline telephone) at any time.
- The defendant is not permitted to access the Intranet/Internet or bulletin board systems at any time.
- The defendant is not permitted to engage in the use of encryption.

Writing in *Federal Probation* in September 2001, Sr. USPO Brian Kelly, New York Eastern's cyber crime specialist, noted that

> [h]ow restrictive [computer and Internet usage-related] special conditions should be is based on the severity of the instant offense and the offender's criminal history. For example, a first-time offender who has committed an isolated denial of service attack

against a former employer may not warrant a full prohibition from computers and/or the Internet but rather a condition prohibiting any contact, including computer contact, with the former employer, as well as employer notification if the offender plans to obtain employment within the computer industry.

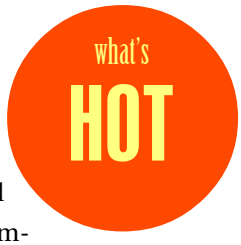
This point is particularly important in light of cases such as *United States v. Peterson,* 248 F.3d 79 (2d Cir. 2001), where the U.S. Court of Appeals for the Second Circuit held that a special condition of probation absolutely barring the defendant's use of computers or the Internet was unreasonable since such use was not reasonably related to the defendant's present or prior offenses. (See box, page 3.)

Ohio Northern probation's Cybercrime Working Group has developed a draft *Cybercrime Manual* for probation staff that contains information similar to that in New York Eastern's bench guide.

As an alternative to listing cyber-specific special conditions on a case-by-base basis, some districts are developing computer restriction and monitoring programs akin to the successful electronic monitoring program. (See Figure 1, page 8.) **Ohio Northern** probation, **Kansas** (combined), and **Texas Western** pretrial services have developed similar approaches for defendants and offenders subject to a single cyber-specific condition with the program incorporated by reference. Texas Western pretrial services has created a companion "Officer's Cybercrime Quick Reference" to assist officers in supervising defendants accused of cyber crime offenses, including those subject to the computer restriction and monitoring program.

For more information on questions to ask cyber offenders during presentence investigation and on cyber-specific special conditions, see *Introduction to Cyber Crime*, pages 11–12.

Monitoring and Forensic Technologies



Several districts have begun using different types of technology to assist in monitoring defendants' and offenders' computer use and to examine their hard drives. Understanding variations in complexity and invasiveness among monitoring and forensic applications is critical for the officer and the court. For example, monitoring a defendant's or offender's computer use through software installed by an officer on the defendant's or offender's computer hard drive may constitute a search. However, using a Web-based application to monitor a defendant's or offender's operation of a Web site merely constitutes surveillance.

Improper or inappropriate use of monitoring and forensic applications can result in serious adverse ramifications for officers and agencies (e.g., civil liability) and the public (e.g., harming or causing the loss of electronic evidence that could be used in a future prosecution). Experienced officers advise that under no circumstances should such applications be used by an individual who has not been trained in their use and advised about their appropriateness.

SEARCH reviews five computer-monitoring programs

SEARCH, the National Consortium for Justice Information and Statistics, has evaluated five commercial computer monitoring programs available for use by probation and pretrial services officers. The five products tested were Boss Everywhere 2.3, Desktop Surveillance 3.6b, Eblaster 2.0, PC Activity Monitor Pro 4.0, and STAR-Rtm PC and Internet Monitor 3.02 Pro. The evaluation report is available at http://www.search.org/publications/bibliography.asp.

Officers must remember that a cyber-savvy defendant or offender can circumvent even the most sophisticated monitoring application—especially if it has been installed on the defendant's or offender's hard drive. Thus, officers with expertise in supervising such defendants and offenders note that simply because a technology is available does not mean that it should be used and that an application should never take the place of traditional supervision approaches. Monitoring technology merely supplements traditional, tried-and-true approaches.

Finally, commercial products do not necessarily come cheap. Prices of monitoring software packages range from $50 to $175, while forensic software packages typically cost from $500 to $1,700.

The following reviews of monitoring and forensic applications were contributed by officers who have used them. Of course, inclusion of these reviews here does not constitute endorsement by the Federal Judicial Center.

Monitoring applications

Spector and E-blaster. Spector is a screen-recording program that can be installed on a hard drive and configured to capture screen images at specified intervals and store them in an encrypted file. It can store up to five or six days' worth of activity. E-blaster, which can accompany Spector, automatically e-mails to the supervision officer the defendant's or offender's chat activity, URLs visited, processes run on the computer, and any images accessed. The tool is limited in that information must be retrieved frequently because the file may become too large and delete old information. Also, applications and files are stored on the offender's hard drive and therefore are susceptible to alteration or deletion. Spector works on Windows and Macintosh operating systems; E-blaster is available for Windows only. For more information on Spector and E-blaster, go to http://www.spectorsoft.com. *Reviewed by Sr. USPO Brian Kelly (Brian_Kelly@nyep.uscourts.gov), and USPO Monica Hampton (Monica_Hampton@scp.uscourts.gov).*

Echo. This tool is a remote Internet monitoring application. After installation and configuration on the offender's hard drive, the offender's system sends real-time information of all Internet activity (e-mail, chat, and Web site access) to a designated server. The application requires limited hard drive space, operates "hidden," and can be monitored from the of-

Figure 1. *Example of a Computer Restriction and Monitoring Agreement*

Ohio Northern probation's Computer Restriction and Monitoring Program is invoked with the following special condition: *"You shall provide the U.S. Probation Office with accurate information about your entire computer system (hardware/software); all passwords used by you; and your Internet Service Provider(s); and will abide by all rules of the Computer Restriction and Monitoring Program."*

General Provisions

1. I, _____, have been placed in the Computer Restriction and Monitoring Program. I agree to comply with all program rules set forth in this agreement, and the instructions of my probation officer. I understand that this agreement is, by reference, part of the order setting conditions and that failure to comply with its provisions or the instructions of my officer will be considered a violation of my supervision and may result in an adverse action. I agree to call my officer immediately if I have any questions about these rules or if I experience any problems that may hinder my compliance with this program.
2. I understand I must complete the Computer/Internet Data Form and return within seven days.
3. I shall possess and/or access only computer hardware or software approved by the U.S. Probation Office. I shall obtain written permission from the U.S. Probation Office prior to obtaining or accessing any additional computer hardware/software or making any alterations to my system.
4. I shall only use Internet Service Providers(s) approved by the U.S. Probation Office. I shall obtain written permission from the U.S. Probation Office prior to changing ISP or entering into agreements with any additional ISP.
5. I agree to allow the U.S. Probation Officer to install software/hardware designed to monitor computer activities on any computer I am authorized to use. I understand that the software may record any and all activity on my computer, including the capture of keystrokes, application information, Internet use history, email correspondence, and chat conversations. I further understand that a notice will be placed on the computer at the time of installation to warn others of the existence of the monitoring software on my computer. I agree not to attempt to remove, tamper with, reverse engineer, or in any way circumvent the software/hardware.
6. I understand that my supervising officer may use measures to assist in monitoring compliance with these conditions such as placing tamper resistant tape over unused ports and to seal my computer case.
7. I will notify all individuals that have access to my computer system that it subject to monitoring and/or search/seizure.
8. I shall not create or assist directly or indirectly in the creation of any electronic bulletin board, ISP, or any other public or private network without the prior written consent of the U.S. Probation Office. Any approval shall be subject to any condition set by the U.S. Probation Office or the Court with regard to that approval.
9. I understand the U.S. Probation Office may determine a Web site and/or material is a detriment to my success in this program and therefore prohibit future access to said Web site/materials. I will abide by this decision pending any ruling by the Court to the contrary.
10. I understand that my officer will use telephone calls and unannounced personal visits to monitor my compliance. When I am at home, I agree to promptly answer my telephone or door.
11. I will provide copies of credit card billing records or other financial records monthly and will not open any new lines of credit without authorization of my supervising officer. I understand that my supervising officer has the authority to request my credit history information to confirm my compliance with the conditions of release and these program rules. My signature on this document signifies my consent for the release of the credit history information.

Defendant _____ Date _____

Supervising Officer _____ Date _____

fice. However, it monitors only on-line activity, requires a dedicated server, and is susceptible to alteration or deletion by the offender. Echo works on Windows operating systems only. For more information, go to http://pearlsw.com. *Reviewed by Sr. USPO Brian Kelly (Brian_Kelly@nyep.uscourts.gov).*

Other monitoring technology

WHOIS. This free web-based tool enables officers to look up a registered domain name and obtain information about the owner of a particular Web site. There are several WHOIS sites. The most popular, Better-Whois and VeriSign Global Registry Services, combine searches of the various registries. For more information, go to http://www.Better-Whois.com or http://www.VeriSign-grs.com. *Reviewed by Sr. USPO Dan Wieser (Florida Middle) (retired).*

SamSpade.org. This Web site helps officers monitor the activities of offenders who have their own Web sites. It provides ping, WHOIS, and trace route information and shows how to use these and other features to find the owner of a Web site and the site's location. SamSpade works best when combined with ChoicePoint or Lexis databases. For more information, go to http://www.samspade.org. *Reviewed by Sr. USPO Dan Wieser (Florida Middle) (retired).*

Anonymizer. This application allows the officer to visit defendant or offender Web sites anonymously without having any unwanted files or code placed on the officer's computer and without revealing the officer's computer Internet protocol (IP) address. The tool can serve as a deterrent if the defendant or offender knows the officer could be watching at any time. The basic application is free. For more information, go to http://www.anonymizer.com. *Reviewed by USPO Monica Hampton (Monica_Hampton@scp.uscourts.gov).*

Forensic Tools

EnCase. This forensic software tool allows the officer to conduct non-invasive investigation, including drive imaging, previewing, word searching, and scripting. It features a graphical user interface that enables examiners to easily manage large volumes of computer evidence and view all relevant files, including "deleted" files, file slack, and unallocated data. The officer can perform initial "previewing" of a target drive, acquire evidentiary images, search and recover data, and obtain reports within the same application. Use of the tool does not alter data. EnCase has a report feature which generates reports and extracts documenting the investigation results and integrity of the original data with a chain of custody. For more information, go to http://www.encase.com. *Reviewed by Sr. USPSO Lanny Newville (Lanny_L_Newville@txwpt.uscourts.gov).*

ComputerCop Professional P3. The P3 CD loads in the offender's computer in Windows and searches for images or keywords. It will also search RAM and file slack and zip files, but at increased search time. P3 locates "hidden" graphic files where file extensions were changed. The useful "crime category" option allows approximately 7,500 words and phrases in 25 crime categories to be selected for searching. The software also allows the officer to search his or her own buzzwords. If images or keywords are found, the files can be downloaded to diskette or an external drive for further review in "Case Manager," which compiles a report complete with audit trail. For cases involving a large number of images, Case Manager can also deliver a timed slideshow presentation. The software is fast and easy to use. For more information, go to http://www.computercop.com. *Reviewed by USPO Scott MacNichol (Scott_MacNichol@flmp.uscourts.gov).*

An on-line briefing for judges

Texas Western pretrial services has developed a self-running, narrated on-line briefing for the district's judges: Computer Searches and Access Monitoring Tools. The briefing serves as an example for officers in other districts who want to provide judges with such information. A PowerPoint presentation, the briefing includes

- an overview of legal issues
- discussion of special conditions
- discussion of computer restriction and monitoring programs
- an overview of monitoring software tools
- playback simulation of *Spector* monitoring software
- a "search continuum" flowchart

To view Computer Searches and Access Monitoring Tools, go to http://www.cybercrime.flmp.uscourts.gov/Presentation/CAMT.ppt.

ComputerCop Forensic. This tool allows the officer to access information from an offender's computer via a parallel port cable without risk of alteration. The offender's system is booted from a DOS diskette. The software allows viewing of all image files, text files pursuant to a keyword search, deleted files, and file slack. The officer can pick which files to save into the "Case Manager" feature and allows various reports to be submitted. It can be installed onto a laptop for examinations in the field. Easy to use, the tool is not a true forensic application: The user cannot pick and choose which files to view and must perform a scan first. For more information, go to http://www.computercop.com. *Reviewed by Sr. USPO Brian Kelly (Brian_Kelly@nyep.uscourts.gov).*

Ilook Investigator. This program can be used to examine images obtained from any forensic imaging system that creates a straight sector dump of the imaged media. It may also be used to examine Safeback image files, EnCase image files, ISO and CIF CD images, VMWare virtual disks, and ILook image files. Ilook, which consists of a main executable file, runtime files, and on-line help, will run on Windows NT and 2000. The application has a steep learning curve but is available free to law enforcement. For more information, go to http://www.ilook-forensics.org. *Reviewed by Sr. USPO Dan Wieser (Florida Middle) (retired).*

Training

Internal Training

Kansas (combined) conducts a one-day program for officers about types of cyber crime, computer hardware, the district's search policy and special conditions, and monitoring software and how to use it. The district's chief also conducts a presentation for judicial officers.

For more information, contact USPO Shawn Brewer at Shawn_Brewer@ksp.uscourts.gov, USPO Michelle Caples at Michelle_Caples@ksp.uscourts.gov, or USPO Bryce Beckett at Bryce_Beckett@ksp.uscourts.gov.

Montana (combined) conducts an introductory cyber crime program for officers that covers origins and types of crime involving automated devices, issues related to officer duties in report writing and supervision (including development and enforcement of special conditions), and an overview of monitoring software and computer forensics. The training includes several handouts and a guest lecture by an agent from the Montana Criminal Investigation Bureau.

For more information, contact USPO Wes Estep at Wes_Estep@mtp.uscourts.gov.

External Training

The training programs described below are advanced. Information on introductory and basic technical training can be found on page 14 of *Introduction to Cyber Crime.*

National White Collar Crime Center/National Cybercrime Training Partnership. NW3C/NCTP, a Department of Justice-funded organization, offers Advanced Data Recovery and Analysis (ADRA). This in-depth, 40-hour course, which is taught only at NW3C headquarters in Fairmont, West Virginia, covers large hard drives, new partition types, Windows NT/2000/XP NTFS, advanced imaging, alternate media, transient data, and Internet issues. It is free and is limited to 20 students. Prior computer forensic training is required. Several federal probation and pretrial services officers have participated in NW3C courses. For more details, see http://www.cybercrime.org for more details.

FLETC-SCERS. This two-week advanced course exposes participants to a variety of imaging and forsenic tools. Not only do individuals learn important skills, they are also provided software and hardware to complete forensic investigations. Software is available exclusively to those who complete the course. Until recently, the course was offered only at the Federal Law Enforcement Training Center in Glynco, Georgia, but it is now available regionally. Participants must have computer investigation expertise. Fees range from $1,500 to $6,000, depending on where the course is held and what software and hardware will be provided to attendees. Seating is limited to 30 students. To date, only three federal probation and pretrial services officers (from Ohio Northern probation, Florida Middle probation, and Texas Western pretrial services) have attended this course. For details, go to http://www.fletc.gov.

SEARCH, the National Consortium for Justice Information and Statistics, offers a variety of courses on computer forsenics and Internet investigations. According to several probation officers, it is one of the most respected training organizations in the field. Courses range from approximately five days to two weeks. Most courses are held only at SEARCH's facility in Sacramento, California. Fees for courses vary. See http://www.search.org for more details.

Cyber Crime Investigation and Supervision Tips

When investigating and supervising cyber-savvy defendants and offenders, officers should do the following:

- ❍ Continue to use traditional information-gathering techniques, identifying cues, and supervision techniques. Even the most complex monitoring technology can be circumvented by a cyber-savvy individual.
- ❍ Obtain appropriate training and expert probation- or pretrial services-related advice before using any monitoring or forensic technology.
- ❍ In the case of a hacker/cracker, ask questions designed to determine the defendant's or offender's level of expertise. For example, is he or she a script kiddie? Was the person using social engineering? What is the person's technical education and employment background? Does he or she have a history of hacking/cracking? Does he or she belong to hacker groups?
- ❍ Be aware that "cyber" individuals accused or convicted of nontechnical offenses may not be categorized as "cyber" defendants or offenders. In such situations it is important for pretrial services officers, presentence officers, and judicial officers to review the (alleged) conduct that led to the offender's indictment to determine whether cyber-specific special conditions should be recommended and imposed.
- ❍ Fashion cyber-specific conditions that are related to the defendant's or offender's (alleged) offense conduct and convey an understanding of the uses of computers and computer networks.

According to the Administrative Office of the U.S. Courts' Office of General Counsel, with regard to search and seizure, probation and pretrial services officers and judges should be aware of these issues:

- ❍ Installation and use of monitoring software on a defendant's or offender's computer most likely constitutes a search.
- ❍ A computer search is analytically similar to a regular search in terms of third-party liability. If performed pursuant to a valid search condition, some invasion of privacy of a third party and some possibility of damage to a third party's property is inevitable but should not result in liability unless negligent or excessive.
- ❍ Searches or seizures of any kind by pretrial services officers are not specifically authorized by statute and are not included in the Model Search and Seizure Guidelines promulgated by the Criminal Law Committee; they should not be performed unless ordered by the court.
- ❍ Searches by probation officers are disfavored, and alternatives should be used whenever possible.
- ❍ Searches of a defendant's or offender's computer, where authorized, should be conducted only by highly trained personnel.
- ❍ Automation personnel should not be taken into the field to conduct a computer search.
- ❍ If the court orders the use of monitoring software and expects officers to check it randomly or regularly, it should specifically so order as part of the condition.
- ❍ The damage in a computer search, such as the loss of important data, could be far more serious and costly than the physical damage that might occur as a result of a traditional search. If technical incompetence or negligence on the part of the searcher causes such loss, the potential for liability is much more significant. Another potential for liability is a computer search that is broader than necessary to accomplish its purpose. Caution and technical expertise are necessary to avoid these problems.
- ❍ The Privacy Protection Act (PPA) and the Electronic Communications Privacy Act (ECPA) both create liability for computer searches that violate their provisions. However, neither of the acts will apply in the vast majority of situations in which a probation or supervised release search might occur.
- ❍ The PPA (42 U.S.C. §2000aa et seq.) specifies that government officers, "in connection with the investigation or prosecution of criminal cases," may not search for or seize work product and other documents intended for public dissemination unless there is probable cause that the person possessing the materials committed the criminal offense to which the materials relate. It is, of course, unlikely that the information in an offender's computer in which an officer has an interest will be intended for public dissemination. Furthermore, court-ordered or consensual searches conducted by probation officers are for the specific purpose of ensuring the offender's compliance with court-ordered conditions of supervision, not the investigation or prosecution of a criminal offense; therefore, it is likely

that section 2000aa-6 would be inapplicable to any search by a probation officer. This view comports with the purpose of the Act, which is to protect individuals' First Amendment privacy rights. Of course, for individuals under probation and supervised release supervision, the expectation of privacy is diminished. When conditions imposed under the authority of 18 U.S.C. §§ 3563(b) and 3583(d) impinge on the right to privacy, they are valid so long as they are reasonably related to the twin goals of supervision: rehabilitation of the offender and protection of the public.

- The ECPA has two parts. Title I is an amendment to the wiretap provisions at 18 U.S.C. § 2510 et seq. and deals with the "interception" of transmission. The term *interception* has been very narrowly defined, and nothing an officer is likely to do would constitute an "interception." Use of software that records communications or sources of communications is probably not

More Cyber Crime FAQs

Q: What are the pitfalls of using monitoring software?

A: It can be very easy for a defendant or offender to circumvent monitoring software. The defendant or offender can boot from diskettes, CDs, external drives or other storage devices, or he or she can simply use another computer that's not being monitored. Monitoring applications are similar to an EM program where the defendant or offender can remove the bracelet and the officer is not able to tell when it is off or on. Monitoring software can create a false sense of security for the officer. It also generates a large volume of information to sort through and, therefore, creates a lot of extra work that can require the officer to spend a disproportionate amount of time on the case.

Q: What are some red flags I should be aware of when supervising a cyber-savvy defendant or offender and using monitoring software?

A: One way of circumventing monitoring software designed for use on Windows systems is, simply, not to start Windows. Therefore, you should keep an eye out for DOS-based Web browsers on Windows 3.x, 95, and 98 machines. A defendant or offender can press F8 when the computer boots, bypass Windows, go straight into DOS, and use Web browsers available for DOS without detection.

Q: What resources exist for learning more about Linux in the context of cyber crime?

A: Linux is a popular operating system for drive imaging and searches with utilities such as "dd" and "grep." A good resource to learn more about Linux is *The Law Enforcement Introduction to Linux—A Beginner's Guide.* It is available at http://www.ohiohtcia.org/resource.html.

Q: I recently completed NW3C's Basic Data Recovery and Analysis course, and I'm putting together a formal proposal for my chief and management team. I have a general idea about how I want a cyber crime program to work in my district but would like some guidance from the field. Has anyone in the system put together a district policy for cyber crime or cyber offenders?

A: The following probation and pretrial services offices have developed or are developing cyber crime programs of varying complexity in their districts: Texas Western pretrial services, Arizona pretrial services, Kansas (combined), Florida Middle probation, South Carolina probation, New York Western (combined), District of Columbia probation, Ohio Northern probation, and Montana (combined). Contact information for lead officers in each of these districts, as well as for other officers who have developed individual cyber crime expertise, can be found throughout this *Close-up*.

Q: Our management team foresees problems if cyber crime cases are not assigned to an officer who is technically savvy because of the issues that might arise when a violation hearing is held and defense counsel asks questions about the nature of the violation. We are trying to solve this potential problem but aren't sure how to go about it. What districts have created automation specialist positions or taken other less formal steps?

A: Some offices, such as Ohio Northern, Florida Middle, and New York Eastern probation and Texas Western pretrial services, have created automation specialist positions. Others, such as Texas Western pretrial services have a combined automation–EM specialist position. Still other offices (e.g., District of Columbia probation, New York Western (combined), Arizona pretrial services) have designated officers who are technically competent to serve as computer or automation resources. These officers may be assigned cases involving cyber crime or asked to consult with line officers supervising and conducting presentence investigations on such cases. They may also be expected to perform computer searches (where such searches are authorized) and to serve as liaison for systems personnel, the U.S. attorney, and professional development organizations.

an "interception" and would not be covered by title I.

- Title II (18 U.S.C. § 2701 et seq.) applies only to the access of communications electronically stored in an electronic communication service such as provides computer storage or processing services to the public. It requires a warrant and advance notice for most searches covered by ECPA. The Act is designed to protect the privacy interests of the innocent users of such services. The act would cover, for example, intra-company networks, electronic bulletin board systems, and other on-line systems. It would not ordinarily include personally owned, or stand-alone, computers, even though they may be used to send and receive communications by means of an electronic communications service. Accordingly, for purposes of these statutes, the search of personal computer records may be accomplished as any other probation officer-conducted searches in most situations that officers are likely to encounter. Of course, it is possible that an offender might be in the business of providing an electronic communications service to the public. If this is the case, then Title II of the ECPA may apply, and the officer should refrain from searching without advising the court and, perhaps, consulting the U.S. attorney's office. If the operation of the service presents a danger to the public, the officer might consider recommending to the court a special condition that restricts such activity.
- The lack of officer expertise in handling contraband, and the lack of appropriate facilities for storing it, provide further reasons for the caution embodied in the Criminal Law Committee's Model Search and Seizure Guidelines. The Guidelines provide that officers handling seized contraband observe chain-of-custody procedures and turn the contraband over to appropriate law enforcement officers as quickly as possible. If this is impossible, contraband such as child pornography should be handled pursuant to chain-of-custody procedures and securely maintained. The court should be advised of the existence of the contraband as well as how it is secured. The maintenance of lawfully obtained evidentiary material by a law enforcement agency should not result in criminal liability to officers of that agency.
- Finally, districts are eligible to become partners with the National Cybercrime Training Partnership of the National White Collar Crime Center to receive assistance in developing training programs for officers.

Additional Information on Cyber Crime

Blyth, Andrew, and Kovacich, Gerald L. *Information Assurance: Surviving the Information Environment.* New York: Springer Verlag, 2001. http://www.springer-ny.com.

Caloyannides, Michael. *Computer Forensics and Privacy.* Norwood, Mass.: Artech House, 2001. http://www.artech-house.com.

Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* Burlington, Mass.: Academic Press, 2000. http://www.academicpress.com.

Casey, Eoghan (ed.). *Handbook of Computer Crime Investigation: Forensic Tools & Technology.* Burlington, Mass.: Academic Press, 2001.

Federal Probation: Special Issue on Technology and Corrections (September 2001). Washington, D.C.: Administrative Office of the U.S. Courts.

Kruse, Warren G., and Heiser, Jay G. *Computer Forensics: Incident Response Essentials.* Boston: Addison-Wesley, 2002. http://www.aw.com/cseng.

Painter, Christopher M. "Supervised Release and Probation Restrictions in Hacker Cases." *U.S. Attorneys' Bulletin* (March 2001). http://www.cybercrime.gov/usamarch2001_7.htm.

National White Collar Crime Center. *The Internet as an Investigative Tool* (version 2.0) (CD). Morgantown, W.Va.: National White Collar Crime Center (undated). http://www.nw3c.org.

Prosise, Chris, and Mandia, Kevin. *Incident Response: Investigating Computer Crime.* New York: McGraw-Hill Professional Publishing, 2001.

Sammes, Tony; Jenkinson, Brian; and Sammes, A.J. *Forensic Computing : A Practitioner's Guide.* New York: Springer Verlag, 2000.

The Honeynet Project. *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community.* New York: Addison-Wesley, 2001.

Vacca, John R. *Computer Forensics: Computer Crime Scene Investigation.* Hingham, Mass.: Charles River Media, 2001. http://www.charlesriver.com.

U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, National Law Enforcement and Corrections Technology Center. *TechBeat.* www.nlectc.org; (800) 248-2742; asknlectc@nlectc.org (newsletter available on-line or in hard copy).

U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. *Electronic Crime Scene Investigation: A Guide for First Responders.* Washington, D.C., 2001. http://www.ncjrs.org.

U.S. Department of Justice, Computer Crime and Intellectual Property Section. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Washington, D.C., 2001. http://www.cybercrime.gov/searchmanual.htm.