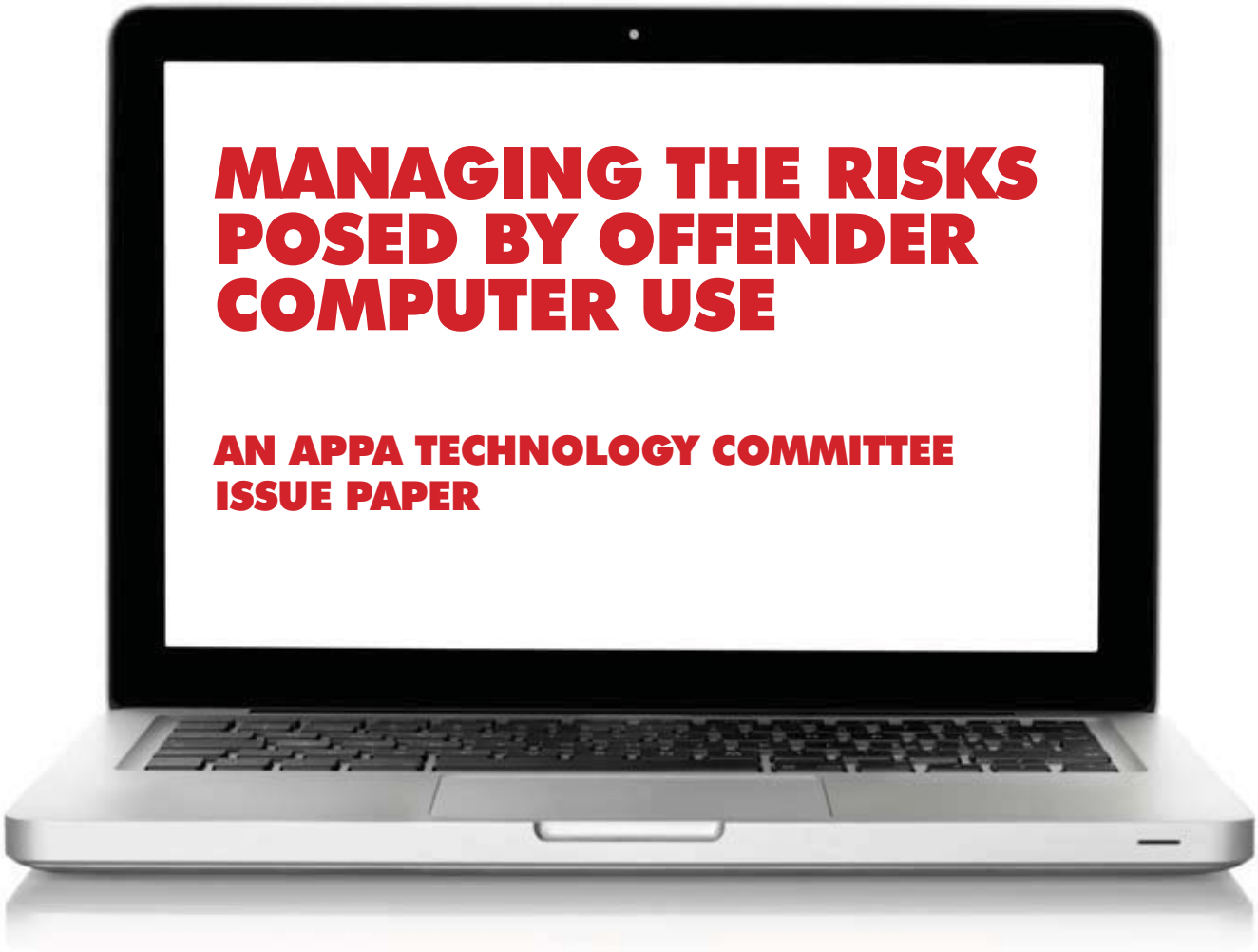

ABOUT THE ISSUE

Since the dawn of the Information Age, individuals have used technology to commit crimes. Initially such acts were committed by those with specific skills or knowledge to break or hack into computer[1] systems and/or manipulate them to steal services, data and/or funds. Some also used their skills to simply destroy systems and/or data. Increased computer availability, use and connectivity particularly with the advent of the Internet, has made the general population, including criminals, accustomed to computers and their uses.

Technology can dramatically increase the effects of criminal behavior and therefore poses a unique risk to the community. For example, near perfect counterfeit checks and currency can be easily created with today's technology. As a result, juveniles committ delinquent acts

that in the past only sophisticated adult criminals could accomplish (Bowker, 1999 and 2000). Furthermore, technology is being used by other types of criminal offenders. The *2009 National Gang Threat Assessment* reflects:

> "Gang members often use cell phones and the Internet to communicate and promote their illicit activities. Street gangs typically use the voice and text messaging capabilities of cell phones to conduct drug transactions and prearrange meetings with customers. Members of street gangs use multiple cell phones that they frequently discard while conducting their drug trafficking operations. For example, the leader of an African American street gang operating on the north side of Milwaukee used more than 20 cell phones to coordinate drug-related activities of the gang; most were prepaid phones that the leader routinely discarded and replaced. Internet-based methods such as social networking sites, encrypted e-mail, Internet telephony and instant messaging are commonly used by gang members to communicate with one another and with drug customers. Gang members use social networking Internet sites such as MySpace®, YouTube®, and Facebook® as well as personal web pages to communicate and boast about their gang membership and related activities" (pg. 10).

With the click of a mouse, sex offenders can use a computer to anonymously "groom" numerous children simultaneously for later molestation or distribute their "collections" of pornography to hundreds of other offenders or to children (Bowker and Gray, 2004). The media has focused on sex offenders on social networking sites. In February of 2009, MySpace® had reportedly removed 90,000 sex offenders from its site since 2007 (Wortham, 2009). At the end of 2009, New York's Electronic Securing and Targeting of Online Predators Act (e-STOP) resulted in the removal from major social networking sites 11,721 profiles associated with 4,336 dangerous sexual offenders registered in New York (WIVB.com, 2010).

The Supreme Court of New Hampshire recently ruled that a special computer condition imposed by a probation officer in a child pornography case was "essential to ensure the effective rehabilitation and supervision of the defendant"
(State of New Hampshire vs. Steve Merrill, 2010).

Increasingly there are efforts to prohibit or restrict computer and/or Internet use, particularly when dealing with sex offenders. The Council of State Governments reported that from 2007 to 2008, 23 states had introduced legislation to restrict or prohibit Internet access by sex offenders (Council of State Governments, 2010). As of July 2009, approximately twenty-five states had laws mandating Internet identifiers be included in sex offender registration.[2]

There are at least 16 states[3] with statutes authorizing computer and Internet prohibitions and/or restrictions (Council of State Governments, 2010, LaMagna and Berejka, 2009, Maryland Division of Probation and Parole, 2010, and National Conference of State Legislatures, 2009). Most statutes are specific to sex offenses, but some states also authorize restrictions for other offenses. For example, Nevada also includes cyberstalking as an offense for which such restrictions can be applied.[4] Minnesota gives its corrections commissioner authority to fashion such conditions if a "significant risk exists that a parolee, state-supervised probationer or individual on supervised release may use an Internet service or online service to engage in criminal activity or to associate with individuals who are likely to encourage the individual to engage in criminal activity" (Minnesota Office of the Revisor of Statutes, 2010). Some states have also given authority to courts to fashion conditions which can restrict or prohibit Internet or computer use during supervision. In New Hampshire, probation officers have the statutory authority to impose special conditions, including computer restrictions, without prior sentencing court approval. The Supreme Court of New Hampshire recently ruled that a special computer condition imposed by a probation officer in a child pornography case was "essential to ensure the effective rehabilitation and supervision of the defendant" (State of New Hampshire vs.

Steve Merrill, 2010). In the federal system,[5] the United States Code provides broad statutory authority for federal courts to impose such conditions on all cases involving a cyber-risk. The *2009 Federal Sentencing Guidelines Manual*[6] also clearly delineates such conditions should be considered in sex offender cases (United States Sentencing Commission, 2009). Inherent in many of these laws is the ability for probation and parole officers to search computers and monitor their use.

Other countries also appear to be posed to start utilizing computer monitoring to manage the risk posed by sex offenders on the Internet. In the United Kingdom the *Sexual Offences Act 2003* introduced measures designed to monitor sex offender actions through the use of prohibition orders, which can include computer restrictions and/or installation of monitoring software. These court ordered restrictions are enforced via Multi-Agency Public Protection Arrangements with police, as opposed to corrections officials, charged with monitoring computer use (Elliott, Findlater and Hughes 2010).

As criminal offender computer and Internet restrictions are increasing, society is becoming more and more dependent upon computer access. Jennifer Granick, Director of the Stanford Center for Internet and Society observed "Without a computer in this day and age, you can't work, you can't communicate, you can't function as people normally do in modern society" (Richtel, 2003). It is therefore no wonder that many courts have struck down total bans on computer and/or Internet use as overly restrictive (Blaisdell, 2009; Bowker and Thompson, 2001; Curphey, 2005; and Miller, et al, 2006). As total prohibitions on all computer and/or Internet use becomes harder to legally justify, officers must look to what Jim Tanner describes as computer management. Specifically:

> "Computer management is like everything else we do in community supervision. We set reasonable conditions and monitor them routinely and randomly. Can an offender get away with taking one drink and us not catching them? Of course. Can an offender get away with being late on curfew and we not notice? Of course. Can an offender visit one or two pornographic web sites and we not catch it? Of course. But if they engage in any illicit activity long enough or often enough, we will find evidence of this and take action. Our goal with computer management is to set responsible conditions of probation/parole and to routinely monitor compliance with these conditions" (Tanner, pg. 6).

It is important to note that strong policies and procedures are an essential prerequisite to implementing a computer management capability. Agencies, in consultation with their judiciary and local prosecuting attorney, should establish guidelines that may include the need for specific conditions of supervision related to computer use, approved tools for use by the agency and protocols for proper seizure and preservation of digital evidence.

THE MAJOR COMPONENTS OF COMPUTER MANAGEMENT

There are five components to good computer management in the supervision of people on probation, parole or supervised release. The components are:

1. Central to computer management is accurate and up-to-date knowledge about what computers a supervisee has or may use. Once this knowledge is obtained, officers must restrict the probationer's or parolee's access to only those computers which can either be monitored or searched. This can be accomplished by requiring detailed written disclosure of supervisees' computer equipment and requiring them to use only authorized devices. Use beyond what is authorized is considered a violation. This provides the probationer or parolee the ability to have computer/Internet access but under the officer's purview (Bowker and Thompson, 2001 and Newville, 2001). Agencies may consider conducting a search of the supervisees' home, where permissible and practical, in order to validate the offender's disclosure statement.

2. The next component is deciding how to monitor the computer or Internet use. Some agencies advocate periodic random searches of computers. Others advocate the installation of monitoring software. Each approach has its pros and cons (see table 1). In practice, the ideal approach is to integrate both approaches to provide effective cyber-risk management (Bowker, 2010).

3. The third component requires officers to venture beyond the traditional brick and mortar world to cyberspace itself. Going on-line allows officers to find probationers or parolees who may have used unauthorized computers to get on social networking sites or visit other risky websites. Despite some agencies' concerns, going into cyberspace is a legitimate investigative tool for community corrections officers (Bowker, 2009). Some officers have realized that checking social networking sites can provide a substantial amount of intelligence on all people on their caseload, not just those convicted of sex offenses. Blalock (n.d.) refers to this practice as conducting a "virtual home visit", which is simply an examination of a supervisee's social network profile (virtual home), which can be effective to investigate violations and to locate absconders.

4. The fourth component is incorporating complementary technologies which augment computer management. Agencies may require high risk individuals to be tracked via location-based monitoring devices. Exclusion zones can be established that cover traditional high-risk locations such as schools and playgrounds but may also include locations where unmonitored computer access is readily available. Historical location data can be useful in determining patterns of behavior which can prompt the officer to find out more about that particular location and confront the probationer or parolee, if necessary. Some monitoring software for cell phones have already integrated global positioning technology into their features. One

COMPUTER SEARCHES	COMPUTER MONITORING
Can detect evidence months, even years old.	Only monitors from time software is installed. Will not open and search files/directories. Will record whatever the user does on the monitored system after installed.
Can be used to examine all operating systems and any device with memory, including all computers, cell phones, I-Pods, MP3 Players, gaming devices, GPS devices, cameras, printers, USB drives, memory sticks, etc.	Monitoring software is primarily limited to Windows and Apple operating systems and computers. Hardware devices can be used for other operating systems. Some cell phones can be monitored. However, there is no monitoring software or hardware for gaming devices, I-Pods, cameras, and other devices.
Wiping utilities can destroy evidence. Encryption programs can prevent evidence from being reviewed. Steganography can conceal evidence all together. These programs can therefore reduce a search's effectiveness. A search might detect the presence or use of these programs and can be used to determine if monitoring software has been defeated. Additionally, searches can be used to examine computers which were used in lieu of a monitored computer.	Monitoring software records everything that occurs, including using wiping, encryption and/or steganography programs. Results can also be forwarded to a remote location, out of offender's control. The results can be reviewed showing the evidence as well as attempts to conceal or destroy it. Disabling monitoring software itself can occur. However, getting it back up and running, without detection is usually problematic. Best way to overcome monitoring is simply to use a non-monitored computer.
Depending upon extent of search may take up to an hour, days or even weeks.	Software installation is fast, usually done in less than half hour. Time spent reviewing monitoring results is dependent upon number of alerts received and user activity. Average estimated review time varies from few minutes to several hours. The reviews, dependent upon software, might need to occur on site vs. in the office.
Traditionally searches required direct access to computer. However, there is some forensic software that allows a remote search of a system. As such an officer installs software on the system that allows an officer to view via the Internet what is on an offender's system at anytime.	Software can either maintain results on the target computer, which requires direct access or can forward results to an officer or to a server for review over the Internet.
Dependent upon when search is done. If search not done for days noncompliance will not be detected for days.	Software that reports via the Internet can generate alerts and/or monitoring reports which can be reviewed almost real time. Software that does not communicate via the Internet, like a search, will only reveal noncompliance when it is reviewed.
Dependent upon whether a simple preview search is done or full forensic examination. The more in depth the greater the need for equipment/software/training.	Software and/or service must be purchased. Little training is required to install and monitor.

such product forwards content from text/email messages sent and received, pictures taken with the cell phone and the cell phone's physical location via global positioning. This feature may find its way in other monitoring software, particularly for lap top and net book computers, allowing officers to locate an individual and the mobile device used when a serious violation occurs. Another monitoring company also incorporates fingerprint readers into their product to further establish who is using a computer that is being monitored. Polygraph examinations also provide a method for ascertaining if probationers or parolees have accessed unmonitored computers.

5. The final component requires that officers continue to incorporate field visits, to residences, employment sites, schools and other relevant locations as part of computer management. Interviews with family, employers and friends can reveal access to unmonitored computers and the Internet. Unannounced home visits have often revealed undisclosed computers or unattended power supply strips for unauthorized lap tops or other devices.

The complexity and diversity of criminal and delinquent activities enabled and accelerated by technology can be daunting but that cannot be used as an excuse for a "wait and see" strategy. Expertise is developed over time and agencies are encouraged to start with the major components and to develop their expertise by focusing on specific strategies and offense types. Starting the process now will help prepare agencies for future challenges that will continue to occur as probationers or parolees find new and innovative ways to exploit developing technologies.

TRAINING

There is generally held assumption that banning computer and Internet access is the best practice because officers either do not have or cannot obtain the technical ability to otherwise monitor computer use. Monitoring and searching computers does require training while little or no expertise is needed to recognize a computer's presence. Are probation or parole officers somehow not capable of developing the same technological prowess that the general public, including those on their caseload may possess? The answer is no, as officers are likely already using technology in the workplace and in their private lives. Clearly they are capable of developing the expertise needed to manage the cyber-risk. One such officer recently graduated from the National Computer Forensics Institute (NCFI) and other officers from around the country have graduated from similar programs (Times of Wayne County, 2010). Officers should avail themselves to training that assists them in addressing the major computer risk management components addressed in this paper. There are numerous organizations that can help officers prepare for computer searches/monitoring and cyberspace investigations. A list of training opportunities is provided in the Appendix.

CONCLUSION

Almost a third of the states have laws authorizing computer and Internet prohibitions and/or restrictions. Fifty percent of the states now require that sex offenders disclose Internet identifiers as part of their registration. Legislatures are increasingly requiring probation and parole officers to focus on sex offenders' computer and/or Internet access. At the same time courts are also becoming more reluctant to impose a total ban on all computer and Internet use for each and every person on probation or parole, including sex offenders. Computer searches and/or monitoring software deployment are now being implemented by many probation and parole agencies to address risk of computer crimes. The benefits of computer use scrutiny are not limited to sex offenders. Evidence of drug, property, bullying or domestic violence and stalking offender noncompliance can often be found on social networking sites. Probation and parole officers must expand their role as monitoring agents to include cyberspace. It is ill-advised to simply ignore probationers' or parolees' on-line activities in our technology-dependent society. Too frequently what occurs in cyberspace has real world consequences. Only by adopting good computer management skills can we hope to address the cyber-risk posed by the increasing offender population using computers for criminal and delinquent activities and/or other violation behavior.

REFERENCES

Blalock, Shannon F. (n.d.) *Virtual Home Visits: A Guide to Using Social Networking Sites to Assist with Offender Supervision and Fugitive Apprehension*. Mimeo.

Blaisdell, Krista L. (2009) "Protecting the Playgrounds of the Twenty-First Century: Analyzing Computer and Internet Restrictions for Internet Sex Offenders" *Valparaiso University Law Review, 43(3)* 1155-1210.

Bowker, Art. (2010) "A High Tech Synergy to Managing the Cyber-sex Offender", Corrections.com Retrieved Aug. 1, 2010 from http://www.corrections.com/news/article/23722-a-high-tech-synergy-to-managing-the-cyber-sex-offender

Bowker, Arthur L. (1999) "Juveniles and Computers: Should We Be Concerned?" *Federal Probation. 63(2)* 40-43.

Bowker, Arthur L. (2000) "Advent of the Computer Delinquent", FBI *Law Enforcement Bulletin*, December, 7-11.

Bowker, Art (2009) "Supervision in Cyberspace". Corrections.com Retrieved Aug. 1, 2010 from http://www.corrections.com/news/article/22580

Bowker, Art and Michael Gray. (2004) "An Introduction to the Supervision of the Cybersex Offender." *Federal Probation. 68(3)* http://www.uscourts.gov/uscourts/FederalCourts/PPS/Fedprob/2004-12/cybersex.html

Bowker, Arthur L. and Gregory Thompson. (2001) "Computer Crime in the 21st Century- Its Effect on the Probation Officer", *Federal Probation. 65(2)* 18-24.

Council of State Governments. (2010) *Legislating Sex Offender Management: Trends in State Legislation 2007 and 2008*. Lexington, KY: author.

Curphey, Shauna (2005) "*United States v. Liftshitz*: Warrantless Computer Monitoring and the Fourth Amendment." *Loyola of Los Angeles Law Review. 38(5)* 2249-2274. Retrieved Aug. 1, 2010 from http://llr.lls.edu/documents/documents/curphey.pdf

Elliot, I. A., D. Findlater and T. Hughes. 2010. "A Practice Report: A Review of e-Safety Remote Computer Monitoring for UK Sex Offenders." *Journal of Sexual Aggression*. 16(2), 237-248.

LaMagna, R. and M. Berejka. 2009. "Remote Computer Monitoring: Managing Sex Offenders' Access to the Internet", *Journal of Offender Monitoring, 21(1)*, 11-24.

Maryland Division of Probation and Parole. (n.d.) *The Management of Sexual Offenders by the Maryland Division of Parole and Probation*. Retrieved November 22, 2010, http://www.dpscs.state.md.us/publicinfo/features/DPP_Workshop_Mng_Sex_Offenders.shtml

Miller, Dane C., Samantha Maulupe, Akashata Nikikund, and Sarosh Shetty. (2006). "Conditions of Supervision that Limit an Offender's Access to Computers and Internet Services: Recent Cases and Emerging Technology." *Criminal Law Bulletin. 42(4)*.

Minnesota Office of the Revisor of Statutes. (2010). 243.055 Computer Restrictions, Retrieved November 22, 2010 from https://www.revisor.mn.gov/statutes/?id=243.055

National Gang Intelligence Center. (2009) *National Gang Threat Assessment*. Washington, DC: author.

National Conference of State Legislatures. (2009) *Sex Offender Computer Restriction & Registration Related Statutes, Updated February 2009*. Denver, CO: author.

National Conference of State Legislatures. (2009) *State Legislation Relating to Internet Social Networking Sites Updated April 2009*. Denver, CO: author.

Nevada Revised Statutes. (2009) Section 213.1258, Retrieved October 15, 2010 from http://www.leg.state.nv.us/NRS/NRS-213.html#NRS213Sec1258

Newville, Lanny L. (2001) "Cyber Crime and the Courts-Investigating and Supervising the Information Age Offender." *Federal Probation. 65(2)* 11-17.

Richtel, Matt. (2003) "Monitoring Criminals' Internet Use is a Matter of Law." *New York Times*. January 21, 2003, Retrieved Aug. 1, 2010 from http://www.nytimes.com/2003/01/21/technology/21MONI.html?pagewanted=all

State of New Hampshire vs. Steve Merrill, June 30, 2010, Retrieved Aug. 1, 2010, from http://www.courts.state.nh.us/supreme/opinions/2010/2010069merri.pdf

Tanner, Jim. (2007) *Beyond Prosecution: Improving Computer Management of Convicted Sex Offenders*. Boulder, CO: KBSolutions, Retrieved Aug. 1, 2010 from http://www.kbsolutions.com/beyond.pdf

Times of Wayne County. (2010) "Probation Officer Certified in Computer Forensics", Retrieved Aug. 1, 2010 http://www.thetimesofwaynecounty.com/index.php?option=com_content&view=article&id=1319:main-story&catid=108:featured-news

WIVB.Com. (2010) "Sex Offenders Removed from Social Sites: E-STOP Law Results in Removal from Websites" LIN Television Corporation. February 2, 2010, Retrieved Aug. 1, 2010 from http://www.wivb.com/dpp/news/new_york/Sex-offenders-removed-from-social-sites

Wortham, Jenna. (2009) "MySpace Turns Over 90,000 Names of Registered Sex Offenders" *New York Times*. February 3, 2009, Retrieved Aug.1, 2010 from http://www.nytimes.com/2009/02/04/technology/internet/04myspace.html

United States Sentencing Commission. (2009) *Guidelines Manual* §3E1.1 (Nov. 2009). Washington, DC: author.

18 U.S.C. §1030 (e) (1), Retrieved Aug. 1, 2010 from http://www.usdoj.gov/criminal/cybercrime/1030NEW.htm

18 U.S.C. §3563 - Conditions of Probation, Retrieved Aug.1, 2010 from http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t17t20+1453+31++%28sentencing%29%20%20AND%20%28%2818%29%20ADJ%20USC%29%3ACITE%20%20%20%20%20%20%20%20%20%20

18 U.S.C. §3583 - Conditions of Supervised Release, Retrieved Aug.1, 2010 from http://uscode.house.gov/uscode-cgi/fastweb.exe?getdoc+uscview+t17t20+1465+7++%28supervised%20release%29%20%20AND%20%28%2818%29%20ADJ%20USC%29%3ACITE%20%20%20%20%20%20%20%20%20%20%20

ENDNOTES

[1] For this discussion "the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device," which is reflected in the federal statute, 18 U.S.C. § 1030 (e)(1). This definition is very similar to many state statues, and encompasses not only desktop and lap top computers, but gaming devices, cell phones, I-Phones, and similar devices yet to be invented.

[2] The disclosure of Internet identifiers is consistent with 2008 of registration regulations implemented by the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking required by the *Adam Walsh Child Protection Act of 2006* and the *Keeping the Internet Devoid of Sexual Predators Act of 2008 (KIDS Act of 2008)*.

[3] The states are: CA, FL, GA, IL, IN, KY, LA, MD, MN, NC, NY, NJ, ND, NV, OK, and TX.

[4] Nevada Revised Statutes Section 213.1258

[5] 18 U.S.C. §§ 3563 and 3583

[6] §§5B1.3(d)(7)(B) and 5D1.3.(d)(7)(B)

Art Bowker, M.A. is a Blog Writer at The Three C's (Computers, Crime, and Corrections), and a Cybercrime Specialist at Corrections.com.

APPENDIX

TRAINING OPPORTUNITIES AS OF JANUARY 1, 2011

- National Computer Forensics Institute (NCFI) (http://www.ncfi.usss.gov/overview.html) Established in 2007, the NCFI offers extensive computer forensic training. All travel, lodging, and per diem expenses are paid by the U.S. Department of Homeland Security and courses are provided at no cost to attendees. Upon completion of training, attendees are issued all computer equipment, hardware, software, manuals, and tools necessary to conduct electronic crimes investigations and forensic examinations.
- The National Law Enforcement and Corrections Technology Center (http://www.prod.justnet.org/Pages/fieldsearch.aspx) maintains a list of Certified Field Search Instructors who are available to provide basic training on the Field Search software. In addition, a training video is available online. Field Search is a free software program, specifically developed by NLECTC to assist officers supervising the cybersex offender.
- The National White Collar Crime Center (http://www.nw3c.org/) has computer investigations courses for all skill levels. One such course, STOP: Secure Techniques for Onsite Previews, provides officers with software that can be used to quickly preview an offender's computer onsite. The training itself is free. Software used in STOP course is also free.
- The Federal Bureau of Investigation's Regional Computer Forensic Labs (RCFL) (http://www.rcfl.gov/index.cfm?fuseAction=Public.P_trainingCourses), offers some courses that are available to officers. One such free course is Image Scan Training. This training provides free software for accurately viewing a variety of graphics formats on an offender's computer, without making changes to any files. It can be run onsite and is ideal for child pornography investigations.
- The American Probation and Parole Association (http://www.appa-net.org/eweb/) offers the course "Managing Sex Offenders' Computer Use." This is one of the few courses specific to the needs of probation and parole officers in supervising cybersex offenders.
- SEARCH: The National Consortium for Justice Information and Statistics (http://www.search.org/) has excellent training and free materials for officers starting out in cyberspace, including courses on social networking investigations and cell phone examinations.
- The High Technology Crime Investigation Association (www.htcia.org) also provides valuable training and networking opportunity for individuals at all skill levels.
- Finally, many police academies offer courses that probation and parole officers can take in computer and Internet investigations. Checking a particular state or jurisdiction's training academy website can locate these courses.