Remote Computer Monitoring: Managing Sex Offenders' Access to the Internet

by Richard C. LaMagna and Marc Berejka*

Overview

Sexual victimization of children is heinous. Unfortunately, for all its wonders, the Internet has facilitated a dramatic increase in this type of crime. This is manifested in both the exponential growth of the development, distribution, and viewing of child pornography, as well as in the luring of children into harmful real-world situations. Often these two crimes are interconnected. Compounding the problem are two other sad realities. First, many supervising officers tasked with managing sex offenders have overwhelming caseloads that limit their ability to provide effective supervision. Second, even where staffing might be adequate, officers typically do not receive the tools or the necessary training to manage offenders' computer and Internet use.

Capabilities of Remote Computer Management Tools. Monitoring and regular inspection of computers used by probationers and parolees is a relatively new practice and the first software tools used for this purpose were introduced less than 10 years ago. These software tools, often referred to as computer/Internet management products, evolved from software developed to automate practices used by forensic specialists in laboratories to examine computers for evidence in criminal investigations. Today's most advanced computer management products include remote access via the Internet and are fundamentally different from computer forensics tools.[1] Remote computer management tools can accomplish the following:

- Monitor offenders' computer and Internet use and alert officers of violations on a close to real time basis;
- Restrict the nature and extent of offenders' Internet activities;
- Deter high-risk computer and Internet use behavior because the offender knows that their activities will be detected;
- Do not require officers to have specialized computer skills;
- Can be configured to protect the rights of the offender (such as client/attorney privilege); and
- Cost up to one-tenth the cost of GPS tracking systems.

So notwithstanding the capabilities of advanced offender computer and Internet management systems, they are underutilized and large numbers of sex offenders engaging in high risk and criminal activities evade detection.

Legislation and Funding. Lawmakers can and should step into this breach. In a number of states, legislators are passing new laws that empower courts and probation systems to manage the computer and Internet use of convicted sex offenders —within constitutional and other legitimate legal limits. This is a good first step. The second, essential step is to provide sufficient financial and human resources so that remote computer management technologies can deliver the benefits for which they are designed. In particular, the caseloads of those who monitor the most dangerous sex offenders need to be capped, which may require the hiring or redeployment of more supervising officers or implementing specialized sex offender supervision units. In interviews, probation experts indicate that the maximum caseload for officers supervising sex offenders should be 25 to 30. Moreover, the officers tasked with supervising these offenders must have adequate expertise in sex offender management and ready access to ongoing training, so they can keep up with offenders' use of technology and their ever-changing strategies to avoid the law.

Judicial Education. As a complement, we need greater judicial education on how these monitoring technologies can be implemented to protect the community, without infringing upon the privacy and Fourth Amendment rights of offenders and defendants. With such education, the judiciary can better support and empower probation and parole departments in their efforts to address these supervisory challenges of sex offender caseloads.

Lawmakers willing to step into this breach will find ample support for their efforts – from law enforcement, probation and parole officers, victim advocates, the sex offender treatment community and, of course, parents. Failure to address these needs denies supervision agencies the opportunity to achieve higher levels of sex offender containment with a powerful and cost-effective supervision tool and would add another layer of sad realities atop this already difficult social problem.

About This Article

This article is laid out in five sections. It:

- Provides an update on the extent of the child exploitation problem;

* *Mr. LaMagna is the President of LaMagna and Associates, LLC, International Business Consultants, and is the former Director of Law Enforcement Training and Outreach, Legal and Corporate Affairs, at Microsoft. He has 28 years of federal law enforcement experience at DEA and FBI. He greatly appreciates the time and candor provided by probation officers and other experts who contributed to this paper, as well as the funding and other support provided by Microsoft Corporation—without which this paper would not have been possible. He can be reached at rlamagna@hotmail.com.*

Mr. Berejka is a Senior Director of Technology Policy & Strategy at Microsoft. He has worked on an array of Internet issues over his past 11 years with the company. His current focus is on developing strategies that leverage the capabilities of information technology to advance public policy goals. He can be reached at mberejka@microsoft.com.

The authors wish to recognize Judy Hogaboom, President of IPPC for her assistance in identifying interview candidates. Notwithstanding the support from K&L Gates and the authors' affiliations with Microsoft, the material and views expressed herein are solely attributable to the authors.

- Describes in detail remote monitoring technologies and techniques used to lawfully detect recidivist behavior;
- Examines policy and surveys recent legal activity aimed at enabling remote monitoring as well as protecting children in other manners;
- Discusses gaps in the system that limit the effectiveness of remote monitoring; and
- Suggests policy solutions to fill those gaps.

At a high level, the article finds and suggests:

- Supervision agencies are not sufficiently staffed or funded to take advantage of the capabilities that remote computer and Internet management systems offer. Therefore, convicted sex offenders have greater leeway when they are released than their conditions of release would suggest.
- Supervising officers are not, generally speaking, adequately trained to make maximum use of the capabilities remote computer and Internet management systems offer, nor are they adequately trained to keep up with the evasive actions of offenders.
- The judiciary continues to work through the metes and bounds of what types of monitoring conditions are permissible under the law, though at times it struggles with understanding the technology's flexibility and its sensitivity to privacy concerns.
- There is no escaping the conclusion that addressing each of these gaps requires additional investment from government — investments, however, that if spent wisely will assure laws being passed today would have a real-world impact (i.e., constraining the risk that recidivist sex offenders pose to society and our children).

This article is based on a review of current literature, websites, and materials from technology companies; nine telephone interviews with probation, parole, and pretrial services officers from federal, state, and local agencies; and a thorough review of relevant state statutes and case law.

The goal of this paper is not to upend the generalized probationary rules that have been applied across different classes of offenders. Rather, it is to point out the significant ways the Internet can be used as a tool in sex offender supervision and to discuss the context in which probation and parole agencies operate so that readers have a fuller understanding of the additional challenges imposed on officers by the digital age as well as the opportunities available to empower them with the knowledge and tools necessary to meet these challenges.

Current State of Affairs

Child Exploitation and the Internet. Recent estimates developed at University of California, Berkeley suggest that there are at least 264 million sexually explicit Web pages on the Internet[2]—compared to 25 million reported in 2002.[3] Child pornography is widely available on a subscription basis and by means of peer-to-peer file sharing programs.

Not only does the Internet present an entire corpus of sexually related material for sex offenders, it also presents an enormous pool of potential victims. And that pool is growing. More than 90% of children between the ages of 5 and 17 use computers. More than 65% of youths aged 10 to 17 use the Internet at home. And with increased Internet access at schools and libraries, it is very possible that every teen and "tween" has some ability to engage in Internet-based communications.

The prevalence of Internet-enabled exploitation is disturbing. In a study of youths who use the Internet regularly, 4% indicated that they had received "aggressive," sexually oriented solicitations, including efforts to meet face to face (a quarter of these solicitations, or 1% of the total reporting group, indicated they had been approached by people they knew —mostly other youth).

Research from the University of New Hampshire's Crimes Against Children Research Center (CACRC) concludes that Internet-initiated sex crimes involving adults and juveniles often fit a model of statutory rape. Adult offenders meet children online, develop relationships with, and openly seduce these young victims (in contrast to a model of forcible sexual assault or pedophilic child molestation).[4] The disturbing case in 2002 of Christina Long—a 13-year-old girl from Danbury, Connecticut, who decided to meet someone she had been corresponding with on the Internet, a 25-year-old man, was strangled and raped—is just one tragic example.

Sadly, there also is mounting concern that ongoing, unlimited computer and Internet access undermines the proper treatment and containment of sex offenders. The mere availability of sexually explicit material online seems sufficient to entice offenders to offend again. Andres Hernanadez, Director of the Sex Offender Treatment Program at the Federal Correctional Institution in Butler, North Carolina observes:

> *"The state of knowledge with respect to Internet Child Pornography offenders is in its infancy. My observations of the 217 offenders who participated in the SOTP (Sex Offender Treatment Program) indicate that these Internet child pornographers are far more dangerous to society than we previously thought."*[5]

Studies have shown that many sex offenders do indeed act on their impulses. Most experts agree that adults who have a sexual interest in children cannot be "cured," but instead they must be managed and denied opportunities to act upon their proclivities.[6] While some of these probationers' computer and Internet activity is legal, sex offenders' computer usage poses serious, continuing threats to the community. These threats include, among other things:

- The creation, development, and sharing of child pornography images (which research has shown fuels the desire to have actual sexual encounters with underage victims);
- The live victimization of children through video or webcam recording; and
- The grooming and luring of underage victims for sexual encounters.[7]

Not surprisingly, sexual predators often prey on the most vulnerable of young victims. According to New Hampshire's CACRC, "Most Internet-initiated sex crimes involve adult men who use the Internet to meet and seduce underage adolescents (from 13–15 years old) into sexual encounters."[8]

An Overtaxed System. Further complicating the situation, the system for managing the nation's population of known sex offenders is reaching the breaking point and, arguably, many systems in many jurisdictions are past that point. In 2006, 272,350 rapes and sexual assaults were reported in the United States[9] compared to 209,800 in 2004.[10] About 60% of those convicted of these crimes are placed on probation in the community.[11] As the public increasingly relies on the criminal justice system to contain the behaviors of the ever-growing number of registered and supervised sex offenders, managing sex offenders' use of computers and the Internet is emerging as an essential component of sex offender supervision. But wide scale effective management is still elusive, because of the rapidly changing technology environment and overworked staff burdened with responsibilities that include finding suitable housing for homeless sex offenders amidst changing residency restrictions.

As much as some might hope otherwise, Internet use has become so much a part of our lives and work that many courts have found it unreasonable to completely deny sex offenders access to the Internet.[12] While situations vary by jurisdiction, the courts generally have overturned total bans on computer access, finding such bans to be overly restrictive given the increasingly computer-dependent and Internet-oriented nature of our society. As important, experienced probation officers argue that setting conditions that too heavily restrict a sex offender's computer access only leads the offender to seek ways to access the Internet undetected. As one officer interviewed for this paper states, "We are part cop and part social worker—our interest is not so much in punishing as in getting these people to lead productive and law-abiding lives."

At the other end of the spectrum, the prevalence of, and easy access to, material on the Internet that stimulates many offenders' inappropriate desires for youthful victims make it risky for convicted offenders to have completely unmanaged access to computers and other devices.

Computer and Internet Management Technology

The courts have upheld selective monitoring of probationers' computer and Internet access on the basis of "reasonableness" and the government's "special need" to promote public safety, and during the last decade software tools were introduced that are designed specifically for probation and parole agencies to monitor offenders' computer and Internet use. Agencies are integrating these tools into their sex offender containment supervision strategies and using them to enforce compliance with supervision orders. These new tools are often referred to as computer management systems and their use differs from computer forensics well established in law enforcement.[13]

In the last decade software tools were introduced that are designed specifically for probation and parole agencies to monitor offenders' computer use.

Computer Management vs. Forensics. Computer forensics involves the thorough examination of a computer to determine its current state and recent use. In contrast, computer management technology examines computer use as it occurs. Computer forensics is used to gather evidence about suspected criminal activities whereas computer management technology is used by probation, parole, and court services agencies to ensure compliance with conditions of community supervision, enhance public safety, and mitigate risk to potential victims.

With computer forensics, law enforcement agencies typically confiscate the computer to examine its contents and determine how it has been used. With computer management systems, probation and parole agencies use one of several types of software tools to conduct ongoing inspections of how an offender's computer is being used and in some cases restrict how it can be used. The time required for law enforcement to complete forensics examinations is measured in days or weeks whereas the time required for probation and parole agencies to review information with a computer management system is measured in minutes.[14]

Computer Management Options. A variety of software tools and services have been introduced over the last ten years that offers a range of computer management capabilities to probation and parole officers with sex offender caseloads.

Field Forensic Tools. Field forensic tools are the most fundamental. They automate many of the forensics techniques used by law enforcement and enable computers to be inspected on a regular basis by officers during home and field visits.

Computer Management Tools. Computer management software is more advanced. It is installed on the offender's computer and runs in the background to gather pertinent information about the offender's computer and Internet activities while the computer is being used. These systems require the officer to physically access the monitored computer to retrieve the data that has accumulated since the officer's last visit. These advanced systems typically include control as well as monitoring capabilities. State-of-the-art computer management systems can be precisely configured to set monitoring and alert parameters, detect violations, and avoid infringing on the offender's privacy in his legitimate computer use.

Remote Computer Management Systems. Remote computer management systems incorporate advanced computer management software features and empower officers to monitor and control computer use remotely, on a near real time basis via the Internet. These systems use forced gateway techniques to send pertinent usage information to an Internet server for immediate analysis, review, and archival. The Internet server processes usage information against

rules and parameters set up by the agency and sends alerts by pager or email to officers when prohibited or suspect activity is detected. Remote computer management allows supervising officers to sign onto any Internet-enabled computer to generate reports, spot check offenders' activities on demand or in response to alerts, and conduct near real time review of ongoing computer and Internet use.

Remote computer management programs provide more comprehensive information on a more frequent and timely basis.

Several years ago, Officer Brian Kelly, a Senior U.S. Probation Officer with the U.S. District Court, Eastern District of New York, and a pioneer in computer management, took advantage of having remote access to monitor the computer activities of a convicted sex offender in his mid-20s. It was 11:00 p.m. on a Friday evening and he found that the offender had been instant messaging and was planning to rendezvous with a 13 year-old girl the following day. The offender had been ordered by the court not to have any contact with any person under the age of 18 without permission of the probation officer. The next morning, Officer Kelly conducted an analysis of the most recent data being captured from the offender's computer. He also logged on to a message board frequented by the offender to check for activity. He found the offender had recently posted messages on the board and that the messages weren't coming from the offender's home computer (another violation). The Internet Protocol address attached to the messages revealed the offender's location. Officer Kelly and his colleagues responded to that location, but when they arrived the offender had already left. They found the offender at his home and intervened before the 13 year-old child's safety was jeopardized. Officer Kelly asserts, "Without computer monitoring, we wouldn't have even known about that meeting!"

Offenders are unable to tamper with data and evidence collected by remote computer management systems because this information resides on the secure Internet server. Furthermore, officers do not have access to the offender's privileged information because this information is not stored on the server. Relieved of the burden of traveling to the offender's home just to offload computer and Internet activities, officers can prioritize how intensely they monitor computer usage without being constrained by the impact that travel time has on their workload. As residency restrictions force more and more sex offenders out of the cities and suburbs to reside in rural communities, *remote* access to manage offenders' computer use is emerging as an essential component for resource-constrained agencies.

Computer management improves the efficacy of the overall supervisory system including immediate notification of violations.

The courts also have acknowledged the value of remote monitoring. In *United States v. Balon*,[15] the U.S. Court of Appeals for the Second Circuit commented:

> The difference between real-time monitoring and a probation officer checking the log list at some later date at the user's house might have a potential impact on effective supervision because the latter option affords the user time and opportunity to circumvent the software.

Clearly, remote monitoring programs, when used as a component of an integrated offender management plan, offer the most effective and efficient way to address the challenges posed by the growing problem of sex offender supervision.

Although this article reviews issues and needs that are relevant to maximizing the benefits of remote computer management systems such as Impulse Control and WebCT on victim and public safety, much of the discussion that follows also applies to less sophisticated computer management techniques used by probation and parole agencies.

Getting Started. Remote computer management systems are fairly "user–friendly" and do not require the supervising officer to have above-average computer knowledge. Computer management monitoring and control software is installed on the offender's computer by the officer, vendor, or the offender/defendant.[16] Prior to installing the software the officer learns as much as possible about the offender from his computer, and then he or she "wipes the offender's hard drive clean"(or removes illicit material) and installs the management software. Agencies may use field forensics tools such as Field Search[17] to conduct the initial examination (a process that requires above-average computer skills and takes less than an hour). These examinations often reveal offender-specific key words and phrases that can be used by the computer management software to trigger alerts and establish control parameters to mitigate risk of reoffense.

Once the management software is installed, it activates and operates in the background each time the computer is started. Most computer management software can be installed without requiring any changes to the offender's computer. In some instances, security software residing on the offender's computer may need to be modified, but this is easily accomplished even by inexperienced officers with telephone support from the vendor.

To manage computer use remotely, supervising officers must have access to Internet-enabled computers. They access offender data that resides on the vendor's Internet server by entering their user ID and password. Agencies rarely require additional equipment or software to implement remote computer management software. However, officers that are able to access the Internet only from their office are at a distinct disadvantage when compared to those equipped with wireless Internet-enabled laptops.

Supervision and Remote Computer Management

Monitoring, Control, and Containment. Computer management is one of several tactics used by agencies to achieve higher levels of surveillance and containment and control of sex offenders. Software tools are readily available that automate surveillance, control, and management of offenders' computer use in compliance with judicial orders as well as case law (such as a victim's name or place of work) that trigger immediate notification of the supervising officer. They also allow officers to create controls that prohibit access to certain types of websites, activities, or even messages. Controls, monitoring parameters, and officer notification can be applied on a case-by-case basis or across an entire caseload.

These systems can be precisely configured to the offender's victimization patterns by identifying keywords and phrases.

Data Capture and Analysis. There are three basic ways to capture information about an offender's computer use: keystrokes, data packets, or screen images.[18] Advanced computer management systems often blend multiple methods of data capture. Information provided to the officer reveals how a particular computer is being used—i.e., what programs are running, what interactions are taking place, what files are being accessed, and what these files store.

Monitoring. Monitored activities are time-stamped and organized to facilitate review by the officer. Parameters that include key words and phrases are used to identify relevant information and are based on the notification and reporting requirements. Results are presented to officers in a variety of ways, including immediate alert notification by pager or email, standard- and custom-printed reports, and review of data online. Following are examples of the types of information that may be included in monitoring reports:

- A record that includes a screenshot when fantasy role-playing software such as Everquest is running;
- Images accessed via the Internet or other external devices;
- Web search activities triggered by key words such as "pic" (often used for trading pictures), "let's meet", or a victim's or judge's name;
- Dialogues conducted over chat rooms that may include all outgoing (and when permitted incoming) dialogues or only dialogues triggered by agency-set parameters;
- Internet usage by type of activity and web sites visited; and
- Use of peripherals (removable storage devices) such as an external hard drive, CD, or USB.

Alerts can be sent directly to an officer's pager or by e-mail. The following, real-world case illustrates the value of remote computer management and alert notification:

One morning, an officer came into his office and opened his email to find an alert from his remote monitoring system. The alert notified the officer that an offender had conducted a search on his name. The officer had configured the system in this instance to flag searches on his name and other words, and he wanted screen shots if his last name was detected. Upon receiving the alert the officer logged into system's web interface. The data revealed that at 4:00 a.m. the offender had been searching on the officer's name and was successful in obtaining the officer's address. With that information, the offender mapped the officer's house as revealed by other screenshots. All of this activity was documented and integrated into an audit report for presentation to the court before noon that same day.

Figure 1 Report generated from IPPC's Impulse Control remote computer management software.

Case # 0123-78 – Web Search Terms Report

Print Date: 05/27/2008 Date Range: 05/20/2008-05/27/2008

Report Description: Displays terms used in Internet search engines and sites popularly known for conducting searches. This report is not representative of all searches, but displays data from the more commonly known Internet search engines and search sites. For a list of known search engines and search sites and/or to submit information regarding a new search engine and search site, please go to www.ImpulseControl.net/searchengines.htm.

Log Date	Search Term	Site/Search Engine	Search Type
5/20/2008 01:39:42 PM	behr	google.com	Google Search
5/20/2008 01:44:49 PM	home depot	google.com	Google Search
5/20/2008 01:45:51 PM	sherman Williams	google.com	Google Search
5/20/2008 01:46:23 PM	how to make money doing nothing	ask.com	Search
5/21/2008 09:38:39 AM	Tuesdays	google.com	Google Search
5/21/2008 09:42:27 AM	Ruby Tuesdays	google.com	Google Search
5/22/2008 5:35:23 PM	Find people	google.com	Google Search
5/22/2008 5:37:06 AM	yellow pages	google.com	Google Search
5/22/2008 5:38:21 PM	Jane L. Smith	yellopages.com	Search
5/22/2008 5:44:01 PM	Jane Lee Smith	yellopages.com	Search
5/22/2008 5:38:21 PM	Officer J. Smith and probation	yellopages.com	Search
5/22/2008 5:44:01 PM	Smith	yellopages.com	Search
5/22/2008 5:48:33 PM	map quest	google.com	Google Search

One can only speculate as to what the offender had in mind. But without this information, the officer might have remained in jeopardy.

Reports available with IPPC's Impulse Control illustrate the types of monitoring reports produced by computer management software:

- Detail of High-Risk Activity—including use of a victim's, officer's, or judge's name;
- Top 100 Internet Activities—broken down by web, chat, news, email, and file transfers; officers may then log into the interface to read the chat sessions, email, or information accessed;
- Web Search Terms Report– lists key words and phrases used by offenders to search the Internet;
- Summary of Web Activities by Category Report—shows how offenders are using the Internet;
- Time at Category Report – shows how much time offenders spend on the Internet by type of activity;
- Use of External Removable Media;
- Internet Use Broken Down by Day and/or Hour – helpful for determining patterns of use and for noticing changes in behavior;

Detail, summary, and statistical reports are available by offender, officer, office, or program. When compared over time these reports often reveal changes in behavior. In addition to standard reports officers can review monitoring data online and tag specific items for inclusion in custom reports to present to the courts or for case files. Custom reports may include web sites visited, files accessed, screen images, chat session or list server dialogues, or email correspondence.

Officers can review reports online. Online reports often include hyperlinks. Officers can click on these links to display more detail such as screen shots, images downloaded, or chat session dialogues.

Control Capabilities. Control features allow officers to restrict computer use and Internet access. Parameters can be established to:

- Block access to predefined social networking sites and chat rooms;
- Block access to high-risk sites, such as those promoting weapons, XXX, gambling, drugs, and alcohol;
- Block content that has a victim's name in it;
- Block Anime software programs;
- Allow access to only a list of predefined websites;
- Restrict Internet access by time of day (e.g., allow access only from 9 a.m. to 3 p.m., Monday through Friday).

Impact on Supervision. The experiences of early adopters of computer management systems for community supervision of sex offenders indicate that computer monitoring and control technology is among the more promising "what works" strategies. The application of evidence-based practice is grounded in demonstrating that strategies or systems will produce improved outcomes. It is important to recognize the contribution that information from computer management systems has on the integrity of data (evidence) when evaluating certain supervision strategies such as prohibiting access to high-risk web sites or prohibiting high-risk activities (chatrooms, news groups).

Officers that use computer management software tools tend to have more interaction with the offender as well as treatment providers and members of containment teams because monitoring reports

Computer and Internet monitoring provides highly accurate data about offenders' and defendants' computer use.

Figure 2 Report generated from IPPC's Impulse Control remote computer management software.

Case # 0432-10 – Top-100 Internet Activities Report

Print Date: 04/25/2008 Date Range: 02/22/2008-02/28/2008

Report Description: Displays the top-100 Internet activities of a case for a certain period of time.

Internet Address	Viewing Time	Percentage
www.kiddieacres.com	10 hours	15.90 %
www.incestcartoons.com	4 hours	7.00 %
www.myspace.com	3 hours	4.70 %
www.google.com	2 hours	3.80 %
www.youtube.com	2 hours	3.40 %
search.yahoo.com	2 hours	3.40 %
images.search.yahoo.com	2 hours	3.10 %
www.bored.com	2 hours	3.00 %
comics.incest-art.com	2 hours	2.90 %
www.allcomicsex.com	1 hours	2.20 %
www.toysrus.com	1 hours	2.10 %
gallery.magicincest.com	1 hours	2.10 %
www.porsche.com	1 hours	1.70 %
www.usps.com	1 hours	1.70 %
www.facebook.com	1 hours	1.70 %
gallery.magicincest.com	57 minutes	1.50 %
shopping.yahoo.com	55 minutes	1.50 %
www.walmart.com	49 minutes	1.30 %

reveal more information about offenders' activities and changing risk levels. This technology is being incorporated by innovative agencies committed to evidence-based practices that have implemented supervision strategies based on sex offender containment.

> *"Our Department originally supervised sex offenders with little regard to computer usage. We were tentative about implementing a new supervision responsibility because we didn't know how it would impact our already shrinking budgets, particularly as it related to officer time. Almost immediately we realized what we had been missing. Now it is an integral component of our supervision strategy. What we've learned from monitoring computer and Internet use is that very often the data reveal triggers that, without intervention, would lead to offending behavior.*
>
> *"Because our agency uses the containment model of supervision we have containment teams. Included in the teams are polygraphers, treatment providers, as well as the probation supervision officers. The team meets on a regular basis to review the offender's treatment program and to make necessary changes to the treatment plan. Routinely the intelligence that is generated from [computer and Internet monitoring software] is shared with the containment team to reassess an offender's risk, which often times results in the modification of the offender's treatment plan. We consider [remote computer management] a core aspect of supervision. Over the years we have expanded and improved upon the computer and Internet monitoring supervision to include training officers and expanding the technology's use to include all types of sex offenders. In the future we intend to expand the technology's use beyond just sex offender management." (Rick Parsons, Deputy Chief of Offender Service, Montgomery County, Pennsylvania)*

Countless examples of how remote computer management technology provides critical information that otherwise would have gone undetected were enumerated during interviews. Following are some examples:

- A 34-year-old offender, convicted of child luring, posted a picture of himself when he was 19 on a dating website;
- A sex offender made several virtual visits to the San Diego Zoo's web site, but claimed his real-world visit to the zoo was a spontaneous event and a momentary lapse in judgment;
- To evade his conditions, an offender used the Internet to purchase a prepaid cell phone with Internet capabilities;
- A juvenile offender's chat logs exposed his mental deterioration and need for additional treatment;
- A defendant purchased airline tickets for an unauthorized trip out of state;
- A sex offender contacted his daughter via email despite a no-contact condition.

Daily Use. Officers can receive alerts and log into the system to review recent and ongoing activity, generate reports, and investigate alerts for offenders in their caseload. This information is used by officers to provide positive feedback to compliant offenders, to prioritize when to schedule office and home visits, to identify possible targets for home inspections, and to know when intervention may defuse a potentially risky situation.

For example, one morning one officer that was interviewed logged in and noticed that an offender had sent numerous chats to his girlfriend. Further review revealed an escalating argument. He checked the chat communications periodically throughout the morning and became increasingly concerned. Rather than subsiding, the anger escalated and violence seemed imminent. The officer consulted with the treatment provider and fearing a potential murder-suicide intervened with an unannounced home visit. The situation was defused.

Some systems include statistical analysis reports that include comparisons and trends over time by offender, officer, or office. These can be used to evaluate supervision strategies as well as treatment

Figure 3 Report generated from IPPC's Impulse Control remote computer management software

Case # 0432-10 – Top-100 Internet Activities Report

Print Date: 04/25/2008 Date Range: 02/22/2008-02/28/2008

Report Description: Displays the top-100 Internet activities of a case for a certain period of time.

Internet Address	Viewing Time	Percentage
www.kiddieacres.com	10 hours	15.90 %
www.incestcartoons.com	4 hours	7.00 %
www.myspace.com	3 hours	4.70 %
www.google.com	2 hours	3.80 %
www.youtube.com	2 hours	3.40 %
search.yahoo.com	2 hours	3.40 %
images.search.yahoo.com	2 hours	3.10 %
www.bored.com	2 hours	3.00 %
comics.incest-art.com	2 hours	2.90 %
www.allcomicsex.com	1 hours	2.20 %
www.toysrus.com	1 hours	2.10 %
gallery.magicincest.com	1 hours	2.10 %
www.porsche.com	1 hours	1.70 %
www.usps.com	1 hours	1.70 %
www.facebook.com	1 hours	1.70 %
gallery.magicincest.com	57 minutes	1.50 %
shopping.yahoo.com	55 minutes	1.50 %
www.walmart.com	49 minutes	1.30 %

progress or to track the agency's progress in achieving department goals.

One agency reported extraordinary results. Analysis of computer use among all program participants revealed over 2,000 hits per month for XXX activity. XXX activity was identified as a performance measure that needed to be improved program-wide. One month after initiating procedures to reduce these violations the number of hits per month dropped to 25, a reduction of more than 98%.

Deterrent Effect. Officers report that computer management supervision can reinforce in the mind of the offender the idea that they are being watched. This can be effective in deterring inappropriate and prohibited computer use. Agencies use management reports to analyze compliance, target areas for improvement, and develop strategies to deter problem behaviors. In addition, the probationers sign agreements authorizing or acknowledging that their computer and Internet use will be monitored and may be subject to a forensic examination; in many cases their home can be searched. This awareness adds to the deterrent effect of computer monitoring.

Fees can also act as a deterrent. The cost of remote computer management programs is minimal when compared to other technologies used for sex offender supervision. For example, tracking an offender with Active GPS for one year costs between $2,000 and $3,500 dollars, while full service remote computer management costs only $300–$400. Furthermore, officers aren't burdened with technical trouble shooting, nuisance alerts, and inventory management responsibilities. When offender fees are applied, the offender pays about one dollar a day for remote computer management.

Finally, we note that monitoring systems can bring efficiencies to the development of evidence-based practices (EBPs). Traditionally, collecting, analyzing, and reporting on an offender's historical data is a costly process, and it often is cost prohibitive for community corrections, reducing the likelihood that interventions, supported by EBPs, will be implemented. Well-tailored, remote monitoring programs provide structured data that support EBPs. Activity data gathered reduce the need for costly research teams to search through case notes to perform qualitative, quantitative, or statistical analysis and interpretation. Moreover, by having an offender pay for the monitoring technologies that generate the data for EBP, the offender himself shoulders some of the burden for developing more effective practices. This ensures effective and efficient use of public funds, while increasing public safety.

Positive Responses From the Field. Officers interviewed for this paper were enthusiastic about the use of remote computer monitoring systems and their effectiveness. From their perspective, these systems are relatively straightforward to use in comparison with more traditional computer forensics and management systems. Remote computer management systems do not require time-consuming analysis of the computer's hard drive, nor do they require deep knowledge of computer operating systems, hands-on access to the offender's home or office computer, or access to computer forensics laboratory resources. Computer management systems are built for use by the typical officer in the field. Officers relish the fact that remote computer monitoring technology provides access to information that reflects the offenders' activities in real time and includes safeguards against the offender devising methods to defeat the system. One State of Nevada Public Safety Lieutenant summarized it well: "Things are a thousand times better now that we have [remote] computer monitoring." Another officer stated, "I review the data to get valuable insight into my cases' risk. If I see things that concern me about a particular case, I shuffle my field visits such that I make certain I get to that case first."

The range of benefits from remote monitoring is as broad as one can imagine and includes improved officer safety. Although most of the discussion in this article is focused on sentenced offenders, computer management tools are also used in pretrial settings. According to one officer:

> *"I had a pretrial diversion case where community service was imposed and the individual was dishonest with the amount of hours he completed. I discovered his dishonesty when I reviewed his monitored computer and Internet activities revealed that he was at home and could not have completed the hours he indicated on his time sheet. Although the reality is that he is not going to prison for this activity, it does reinforce that this is no joke and that these are activities that will not go unnoticed."*

Another officer commented:

> *"The goal of any type of supervision case is to reduce the likelihood of reoffense and to enhance the safety of the community. Computer monitoring assists in ensuring individuals arrested on bond are not reoffending. Computer monitoring assists individuals to learn responsible Internet usage. . . . I've had several cases where I've seen each of these examples to be true. I learned about a defendant's unauthorized trip to New Jersey. On a separate pretrial diversion case, I learned of unauthorized communication with a codefendant through an email which revealed they had been communicating all along despite the Court's directives not to. I also had a sex offender who was caught downloading new child pornography while on pretrial release."*

Policy Responses to Date

As much as some might hope otherwise, the Web has become so much a part of our lives that many courts have found it unreasonable to completely deny sex offenders access to the Internet.[19] While situations vary by jurisdiction, the courts generally have overturned total bans on computer access, finding such bans to be overly restrictive given the increasingly computer-dependent and Internet-oriented nature of our society. At the other end of the spectrum, the prevalence of, and easy access to, material on the Internet that stimulates many offenders' desires make it risky for convicted offenders to have completely unmanaged access to computers and other devices. Thus computer management

software that monitors activities and limits Internet access has come to the fore as offering the right balance, at least in principle.

The courts have upheld selective monitoring of probationers' computer and Internet access on the basis of "reasonableness" and the government's "special need" to promote public safety. More details on these court holdings can be found in this issue under "Legal Issues: Limiting Computer and Internet Use" (see page 25).[20]

The courts have upheld selective monitoring of probationers' computer and Internet access on the basis of "reasonableness" and the government's "special need" to promote public safety.

Policymakers and courts have tended to take good first steps to combat the rise in known victimization of children, but better follow-through is needed. The trend has been towards passing more legislation and imposing more conditions on offenders. But much of this work falls on the shoulders of law enforcement and probation or parole officials who, unfortunately, have not been provided the resources they need to handle the new mandates.

New Legislation. Take 2005 as a recent example. That year state legislatures passed more than 100 laws regarding sex offender management, requiring law enforcement agencies to carry out a wide range of measures including:

- Using Global Positioning Systems to continuously record sex offenders' locations;
- Increased penalties for failing to register in sex offender registries;
- Mandatory sentences for certain offenses (most often crimes against children);
- Adding offenses that are subject to registration requirements;
- Requiring more information to be made publicly available;
- Creating lifetime registration; and
- Adding DNA information to public registries of those convicted of certain sex crimes.[21]

In addition to numerous state laws, the United States Congress passed the Adam Walsh Child Protection and Safety Act in 2006 (Adam Walsh Act), which still has not received funding to carry out its many provisions. Some of the relevant provisions of this well-intended law include:

- Increases in mandatory minimum sentences for sex offenders;
- Upgrades to sex offender registration and tracking provisions;
- Strengthening of child pornography prevention laws;
- Creation of the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART Office) in the Department of Justice to administer national standards for managing registries and to coordinate related training and technical assistance; and
- Establishing a Bureau of Justice Assistance grant program for local law enforcement for hiring and training personnel, for conducting investigations, and for purchasing technology that can help combat child sexual abuse.

As the result of some high-profile cases over the past three to four years, many state legislatures also are arguing for increased use of electronic monitoring of the real-world movements of high-risk sex offenders. For instance, the tragic case of Jessica Lunsford —who as mentioned earlier was kidnapped and murdered by a convicted sex offender who lived in her neighborhood— prompted the Florida State Legislature to pass the Jessica Lunsford Act in 2005. It increases penalties for crimes against children, mandates sex offenders (under formal supervision or not) to report twice a year in-person to local law enforcement, and requires lifetime location-monitoring (e.g., via GPS) for certain high risk offenders.[22]

In addition, a number of states have passed laws that empower (or require) probation systems to remotely monitor the Internet and computer activity of convicted sex offenders. A sampling of these laws can be found in this issue under "Sex Offender Computer Use: Relevant State Statutes (see page 27)."

In sum, there is no shortage of new law to ensnare sex offenders and, in the abstract, to prevent future harm.

Tougher Conditions. Another trend is the growth in the number and complexity of supervisory conditions imposed on convicted sex offenders. These conditions are variously created by judges and releasing authorities as well as legislatures. Some are discretionary. Many are mandatory. In general, they tend to apply one standard to all situations. As an example, some courts require mandatory drug testing, whether or not the offender's offense was related to drugs or the offender has a history of drug use.

While the list of conditions flows from good intentions, they often do not take into consideration the individual situation of each probationer, or his relative level of risk of reoffending. In an ideal world, conditions of release would be highly tailored to the situation at hand. They would recognize that not all offenders are alike —that they vary in their age, gender, seriousness of offense, risk factors, and servicing needs. But we do not live in an ideal world. The reality is that for a range of idiosyncratic reasons, judges and releasing authorities vary widely in terms of the conditions they place on offenders and in the number, complexity, and workload demands they place on supervising officers.[23]

As a result, supervision agencies have been given a daunting task of enforcing and monitoring provisions like those described above, and yet in many cases are required to accomplish such tasks with the same or fewer resources. One senior officer from the Federal District (Pretrial Services) of New Jersey who was interviewed for this article stated that with the passage of the Adam Walsh Act, the caseload and workload of the probation officers increased exponentially. However, the supervision offices have not received resources necessary to act on these mandates, nor has training for officers kept pace.

Challenges From the Frontlines. Three primary challenges were experienced by agencies when they implemented computer management strategies to address sex offenders' computer use:

- Increased officer caseloads and workloads;
- Inadequate officer training; and
- Inadequate judicial training.

Caseloads and Workloads. At the heart of the sex offender monitoring dilemma is the long-standing matter of officer caseloads and workloads. The Bureau of Justice Statistics correctional survey reveals that overall probation and parole populations have grown dramatically since 1980. Nationwide, probation and parole systems are responsible for approximately five of the seven million adults under correctional control.[24] This growth has had serious implications for probation and parole agencies regarding caseload and workload management, and the American Probation and Parole Association (APPA) has struggled to address the issue of what is the ideal caseload for years.[25]

Consider the cases reported in an article in the *Detroit News* in 2002, "Felons on Probation Often Go Unwatched," which describe an overburdened and understaffed probation department in one county. The county had 30,000 probationers supervised by about 250 officers, which comes to an average of 120 offenders per officer.

In one case, an officer was fired after a probationer was arrested for attempted murder and engaging in a shootout with police. The probationer had been a fugitive; he had missed several office visits, but was never reported either as an absconder or as a fugitive. The article recounted how the probation officer was so overworked that she failed to get an arrest warrant for the probationer when he became a fugitive. The same newspaper story reported several similar incidents and cited the case of another officer placed on sick leave for stress-related illness. In a letter to her union steward she wrote, "I am currently actively supervising in excess of 156 probationers and my workload units for October 2002 were 177. I am trying to do the work of two people and find it virtually impossible to perform all duties assigned to me within the time frames set forth and in accordance with departmental policy and procedure."[26] The anecdotes in the article illustrate the importance of manageable workloads and proper assessment of offender needs and risks.[27]

The question that has been inadequately addressed to date is: What is the ideal caseload size?[30] Of the nine officers interviewed for this article, there seemed to be a consensus that about 25 to 30 sex offenders per officer is optimal.[31] The APPA guideline recommends 35 maximum for high-risk offenders; with more than 35 cases per officer, monitoring and supervision become reactive and minimally effective. The state of Connecticut recently passed a law stipulating that the maximum caseload should be 25. Of course, geography and demographics play an important role, too. In many western states, an officer may have a three- to four-hour drive to visit an offender. So, caseloads in those jurisdictions should be smaller.

Whereas computer monitoring captures information about how the computer is being used, control allows agencies to establish parameters that restrict how it is used.

But unfortunately the trend is headed in the wrong direction. State and local law enforcement and probation and parole officials are increasingly tasked with investigating and arresting all types of criminals, many of whom are violent and require more intense supervision. As prison crowding becomes an even bigger problem, the burden falls on probation and parole officers, who are tasked to monitor and manage offender behavior and activity in more complex ways in order to prevent further risk to public safety.

Of course, this issue is critical not only in the field of corrections in general but also as it relates specifically to the monitoring of sex offenders.[28] Interviews with officers for this article revealed that when caseloads are too heavy, contact with each offender drops to about once per month. In the officers' view, that simply is not enough.

One experienced officer from the Federal District of Nevada commented that, in the past sex offenders were the most cooperative and least problematic of probationers. However, in recent years, to alleviate prison crowding, judges and corrections officials are placing serious criminals, including more serious sex offenders, on probation or parole status. This point is made by Taxman, Shepherdson, and Byrne in *Tools of the Trade,* in which they assert that probation rolls increasingly reflect the prison population and that "more than half of probationers today are convicted felons."[29] These offenders may be gang members, domestic violence offenders, or sex offenders, but all require more officer time to provide adequate supervision.

To put a fine point on it, caseload and workload issues are pivotal and must be addressed for effective monitoring and management programs to work. Researchers and experts have made comparisons to school teachers and class sizes. Like school teachers, if probation officers have too many "difficult cases" to handle, they cannot possibly do their jobs well—although, of course, when the difficult cases are convicted sex offenders, the jeopardy to society is grave.

Officer Training. In addition to large caseloads and workloads, many probation and parole officers lack the necessary expertise to install and operate the latest software programs available to them.

Jim Tanner, a noted expert and instructor at the National Law Enforcement and Corrections Technology Center (NLECTC), makes the following observation:

> *"Probation and parole officers are up against overwhelming odds now working across the United States. Sixty*

to 70 percent of individuals convicted of sex offenses every year are sentenced directly to probation and supervision in the community . . . . Many times the offenders are more computer literate than the officers attempting to supervise their computer use. . . . Most experts on sex offenders support the theory that there is no known cure for this behavior. Effective programs try to manage offenders by providing treatment to help them identify thinking errors, recognize risk factors in their environment, and develop skills which help control their deviant impulses. [But] management of offender's computer use is an important aspect of this containment."[32]

Joe Russo, program manager at NLECTC notes:

"Computer use by convicted sex offenders is a new and significant challenge to probation and parole folks. . . . They are used to dealing with cases on a personal level, trying to understand and deal with some of the traditional factors that lead to criminal behavior. Most were already stretched too thin trying to manage their caseloads. The Internet, because of its potential dangers, adds a sizable dimension of risk for officers to manage."[33]

To address one important aspect of the problem, NLECTC has created a two-day technical training course for probation officers. The course, originally developed by the American Probation and Parole Association (APPA), is now offered by NLECTC in the field throughout its 10-state region and makes use of computer labs from local agencies. The hands-on training employs about 30 or 40 computers that contain actual caches of information from sex offenders' computers.[34] Interviews of probation and parole officers for this article also revealed that related training is offered at the National White Collar Crime Center (NWC3) in Fairmont, West Virginia, The Federal Judicial Center in Washington, D.C., and the Federal Law Enforcement Training Center in Glynco, Georgia. Probation and parole officers who complete these courses will have a baseline understanding of how to use the computer monitoring programs to a basic level of effectiveness.

Our research also indicates that officers who supervise sex offenders require continuous training at an advanced level to keep up with the changing technology environment.[35] They require more in-depth knowledge of the Internet and in-depth training in computer management strategies for sex offender supervision and containment. Training is essential to ensure the ongoing integrity of the management software. The situation often resembles a "cat and mouse" game where offenders try to circumvent restrictions imposed by the courts, and probation and parole officers try to keep up with often skilled offenders. It takes some sophistication for the "cat" to corner the criminal "mouse."

Experienced officers also are often able to detect cheating during unannounced home visits and sometimes by what they *do not* see on an offender's computer. Training forums allow these experienced officers to share their knowledge. Depending on the technology selected, the reports provided will reveal behavior patterns. Changes in these patterns will alert experienced officers to offender misconduct. Oftentimes agencies will reinforce their computer and Internet monitoring efforts by subjecting the offender to polygraph tests. Moreover, at least one monitoring software package, the Impulse Control tool, regularly performs an integrity check on all of its program files to verify that the programs are properly installed; it reinstalls missing components and notifies the officers if the program has been tampered with or is not functioning properly. Recurring training is paramount to reaping the full benefits offered by these technologies.

Technical training challenges are set against the often incongruous roots from which many probation and parole officers come. Probation and parole officers have a different function than law enforcement. They traditionally are more concerned with managing and monitoring behavior than with responding to an incipient crime. This background is invaluable for developing treatment and prevention strategies. Computer monitoring and Internet-enabled criminal activity are often completely new areas for them. Training on systems and their application are needed to empower supervision agencies to enhance sex offender containment, treatment, and prevention strategies.

NLECTC program manager Joe Russo offers the following observation:

"Officers are used to dealing with offender's addictions, joblessness, and family relationships; now they must also deal with online pornography, sex chat rooms, and discussion boards, and dating services that target more vulnerable, single-mom families with the "right type" of children in the household."

While the training sponsored by NLECTC clearly has been very beneficial to probation and parole officers in the western region, it does not approach the level necessary to meet the overall demand for training of the hundreds of probation and parole officers who currently use monitoring software in 35 states—and for those who will need training down the line.

In short, as good as state-of- the-art computer monitoring tools have proven to be, they also place a burden on already strained and overworked personnel and require a greater level of technical knowledge, training, and resources to implement them. Probation and parole agencies must have more technically skilled and trained officers if they are to get the maximum benefit from the new technology and keep up with often tech-savvy offenders who are highly motivated to defeat the system. In interviews conducted with probation and parole officers at the federal, state, and county level, one recurrent complaint was the lack of technical expertise and access to training on the part of most officers and the inability to perform rudimentary tasks. Many sex offender units rely on one or two officers, often self-taught, who assist others in installing and monitoring the software programs. At this time, when sexual offenses are at an all-time high due in large part to the Internet, it turns out that today's training programs and resources are grossly

insufficient to accomplish the task of monitoring serious offenders effectively and maintaining public safety.

Judicial Training. Our interviews also identified a need for stepped-up training of the judiciary. We ask the reader to scan "Legal Issues: Limiting Computer and Internet Use" (see page 25), which discusses various questions courts have raised about the degree of computer monitoring permissible under privacy and constitutional law. As mentioned earlier, courts have taken a dim view of lifetime bans on computer use and Internet access, but they have approved carefully tailored supervision plans that include remote computer monitoring as a component—especially in the context of preventing recidivism among sex offenders. That having been said, the standards being applied to determine what is and is not a "well-tailored" supervision plan remain in flux. As with the supervisory system, the judicial system is populated by professionals whose understanding of computers, software, and interactions on the Internet can be quite limited. Vendors of remote monitoring software and systems strive to ensure that their products not only are sensitive to constitutional and privacy considerations, but also can be explained in a rather straightforward manner to those imposing monitoring as a condition of release (or reviewing such conditions). That said, the technology underlying these systems is complicated, and the computing environment in which released offenders operate is dynamic. Hence, the dialogue within the confines of a courtroom or other chamber can be difficult for the uninitiated to parse.

Rather than impose this burden on members of the judiciary on a case-by-case basis—and suffer the inevitable vagaries of inconsistent comprehension leading to inconsistent standards and case law—those interviewed for this article recommend a more holistic approach. With court approval of *some* type of remote monitoring seemingly assured, the educational challenge can be simplified by sharing with the judiciary, in more collective settings, the basics of how remote monitoring technology works and how it can be tailored to fit within the legal boundaries of the courts.

Recap and Policy Recommendations

Probation was once a place for relatively low-level offenders that posed little threat to public safety, were able to work closely and cooperatively with monitoring officers, and were mostly in need of counseling and guidance. A lot has changed, especially with respect to sex offenders.

One recurrent complaint was the lack of technical expertise and access to training on the part of most officers.

A 2006 report published jointly by the Department of Justice, Bureau of Justice Assistance (BJA), and the International Association of Chiefs of Police (IACP) notes:

> State and local law enforcement agencies are on the front line of a significant and growing public safety challenge: returning sex offenders. The National Center for Missing and Exploited Children (NCMEC) estimates that more than 566,000 offenders are listed in state sex offender registries nationwide (March 2006). Further, the most recent statistics from the Bureau of Justice Statistics (BJS), U.S. Department of Justice (DOJ), estimate that approximately 234,000 sex offenders are under some form of correctional or community supervision. . . . Law enforcement executives must juggle existing resources to ensure that they are equipped to comply with national and state laws requiring their agencies to register, monitor, and track the returning sex offender population in their communities.[36]

For already overburdened probation and parole officers the dramatic proliferation of computers and access to the Internet has created new challenges for which they are woefully ill-equipped. To cope with the growing problem of Internet-based sex offenses and rising rates of recidivism, many states have passed a great deal of legislation over the past three or four years, recommending stricter penalties and more restrictive conditions. One important new tool is the remote monitoring of sex offenders' online activity via sophisticated, privacy-sensitive systems.

However, new laws and new technology are not enough. Closer monitoring for various types of new offenses will undoubtedly fail to increase public safety unless adequate staffing and training accompany these mandates and tools. Officers must have the time to devote to proper monitoring and to review the cache of information on offenders' computers. Officers must have the skills necessary to effectively use the technology given to them. The judiciary must know how to tailor remote monitoring orders to assure they can be effective, but also to address privacy concerns.

Three concrete policy recommendations flow from these realities and the research done for this article:

- Caseloads of probation and parole officers tasked with remotely monitoring the computer and Internet activities of convicted sex offenders should not exceed 35. In most sex offender supervision programs, if those caseloads creep towards 40, the effectiveness of monitoring goes down. In many cases, such as the supervision of juvenile sex offenders, even smaller caseloads are warranted.
- Training budgets need to include travel and per diem funding as well. Many officers interviewed indicated that not only are they too busy to attend training away from the office, but also that travel money either is unavailable or is used for other purposes. Webinars could serve a useful purpose here. The key is that those officers tasked with remotely managing

the computer and Internet activities of convicted sex offenders *know* how to keep up with the offenders' capabilities. This requires ongoing training on the latest trends in the use of technology for containment as well as judicial purposes and training on developments in computer management technologies, as well as techniques offenders attempt to use to circumvent detection. Some supervision agencies designate a corps of tech-savvy sex offender specialists or support units.

- In this leading-edge area, the judiciary and supervision agencies need to be in synch. To facilitate implementation of new remote monitoring laws and to minimize risk of lengthy judicial review, judicial organizations should seek out, or be provided with, training on program functionality and how remote monitoring can be accomplished consistent with legitimate legal limitations.

The authors hope this article is a step towards addressing each of these follow-on needs, so that remote monitoring tools can be used to their fullest and improve our ability to protect children from repeat sex offenders.

Endnotes

[1] Computer forensics is typically a process that involves the seizure of a computer and the re-imaging of the hard drive to allow forensic examination of the contents by a certified examiner. An image of the hard drive is taken to preserve the original evidence for prosecution. Forensic tools are not ideal for monitoring and management of probationers. It is not practical to seize an offender's work computers simply for monitoring purposes, nor is it feasible to routinely remove computers from an offender's home or work for examination or monitoring. Even if probation or parole officers could remove computers, local forensic labs cannot handle the volume of work that would be involved.

[2] See Claburn, T., "Internet Content Filters Fail to Block Sexually Explicit Material," Information Week (Nov. 14, 2006) ("These figures reflect the testimony of Philip Stark, a professor of statistics at the University of California, Berkeley, who submitted his analysis of Internet content filtering [in 2006] on behalf of the federal government's effort to sustain the Child Online Protection Act (COPA)").

[3] Tanner, J., "Rethinking Computer Management of Sex Offenders Under Community Supervision," 15(2) Journal of Offender Monitoring 11 (2002).

[4] Wolak, J., et al., "Predators and Their Victims: Myths, Realities, and Implications for Prevention and Treatment," American Psychologist, vol. 63, 111-128 (Feb.-March 2008).

[5] Hernandez, Andres E. (Director, Sex Offender Treatment Program, Federal Correctional Institution, Butner, North Carolina), "Testimony Before the Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce," (September 26, 2006) (available at http://www.projectsafechildhood.gov/HernandezTestimonyCongress.pdf).

[6] Heimbach, Michael J. (Federal Bureau of Investigations), "Internet Child Pornography—Testimony before the House Subcommittee on Crime, Terrorism and Homeland Security" (May 1, 2002) (available at http://www.fbi.gov/congress/ congress02/heimbach050102.htm); Krone, Tony, "A Typology of Online Child Pornography Offending," Australian Institute of Criminology (July 2004); Kim, Candice, "From Fantasy to Reality: The Link between Viewing Child Pornography and Molesting Children," Child Sexual Exploitation Update (American Prosecutors Research Institute), vol.1, no.3 (2004).

[7] Finkelhor, David et al., "Online Victimization: A Report on the Nation's Youth," Center for Missing and Exploited Children (June 2000); see also Mueller, Mark, "To Catch a Monster, Using Anti-Terror Law,"

The Star-Ledger (August 14, 2005) (available at http://www.nj.com/news/ledger/index.ssf?/news/ledger/stories/patriotact/partfour.html).

[8] Wolak, J., et al., "Predators and Their Victims: Myths, Realities, and Implications for Prevention and Treatment," American Psychologist, vol. 63, 112 (Feb.-March 2008).

[9] Rand, M., Catalano, S., US Department of Justice Office of Justice Programs Bureau of Justice Statics Bulletin Criminal Victimization, 2006, December 2007, NCJ 219413.

[10] Catalano, S., US Department of Justice Office of Justice Programs Bureau of Justice Statistics National Crime Victimization Survey, 2004, September 2005, NCJ 210674.

[11] Center for Sex Offender Management (2000). *Myths and Facts About Sex Offenders.* This report can be accessed at http://www.csom.org/pubs/mythsfacts.pdf.

[12] Duffy, Shannon, "3rd Circuit Overturns Lifetime Computer Ban," The Legal Intelligencer (June 11, 2007) ("the 3rd Circuit Court of Appeals has ruled that the facts of the man's (who confessed to receiving child pornography) did not justify a lifetime ban on using computers and accessing the Internet").

[13] Forensic examination of computers provides excellent evidence for investigations and prosecution, and there are a number of excellent commercially available programs which are commonly used by law enforcement for such analysis. Even if probation or parole officers could remove computers, local forensic labs cannot handle the volume of work presented by current case loads of police and probation officers supervising offenders of all types. Furthermore, as sex offenders increase their computer sophistication and anti-forensics software becomes more available, traditional computer forensics will become easier to defeat and will require a real-time computer monitoring solution. See Tanner, J., "Rethinking Computer Management of Sex Offenders Under Community Supervision," 15(2) Journal of Offender Monitoring 11 (2002).

[14] According to Dr. Jim Tanner, a noted expert in sex offender supervision and forensics and computer management, a thorough forensic examination by law enforcement can take days whereas examinations conducted by supervising agencies using computer management tools can take only 10 to 45 minutes depending on the type of computer management software tools used by the agency. Tanner, Jim, *"Rethinking Computer Management of Sex Offenders Under Community Supervision," 15(2)* Journal of Offender Monitoring 29 *(2002).*

[15] United States v. Balon, 384 F.3d 38 (2d Cir. 2004),

[16] As a security measure some agencies pair officers during on-site installations.

[17] Field Search Software is a field forensics software package available to justice system agencies at no charge through the National Law Enforcement Corrections Technology Center (NLECTC)—Rocky Mountain Region.

[18] Keystrokes (1 way); Keystroke capture reviews everything the offender types into the computer including keystrokes while on the Internet. Keystroke capture is "one-sided"; the only keystrokes captured are those generated by the offender; incoming emails, messages, and the content of information accessed or saved may not be captured. Keystroke capture reveals important information about off-line.and on-line computer use.

Data packets (2-way) are captured when information is transmitted to and from computers. Data packet capture reveals both sides of a "chat" conversation, file transfers, and inbound and outbound email messages. This is a more sophisticated method of data capture and renders greater monitoring and control over the offender's activities.

Screen shots (images). Screenshot capture stores an image of information that is displayed on the offender's computer. The officer sees exactly what the offender saw. These images provide powerful evidence to the judiciary for court proceedings.

[19] Duffy, Shannon, "3rd Circuit Overturns Lifetime Computer Ban," The Legal Intelligencer (June 11, 2007) ("the 3rd Circuit Court of Appeals has ruled that the facts of the man's case (he confessed to receiving child pornography) did not justify a lifetime ban on using computers and accessing the Internet").

[20] Staying abreast of legal developments is a necessary adjunct to implementing any computer and Internet monitoring program. For instance, Connecticut has been at the forefront of enabling the imposition of a range of probationary conditions. And state courts have upheld this authority. *See* State v. Johnson, 75 Conn. App. 643, 649 (2003); State v. Boseman, 87 Conn. App. 9, 19 (2004) (dicta); State v. Smith, 207 Conn. 152, 168 (1988) (dicta). But the situation can be fluid. A recent federal decision overturned a monitoring law passed by the Indiana legislature in early 2008 and created momentary confusion in the supervisory community—until it became clear that the law was only overturned *in part.* The decision does not challenge monitoring of convicted sex offenders *while on parole or probation*, but does bar it, in that jurisdiction, with respect to registered sex offenders who have finished their supervisory terms. Doe et al. v. Marion County, Case no. 1:08-cv-0436-DFH-TAB (S.D. Ind., Hamilton, J.) (slip op. July 24, 2008). As of this writing, it is not known if the government will appeal.

[21] U.S. Department of Justice, Bureau of Justice Assistance, "Managing Sex Offenders," at 4 (2006) (published jointly with the International Association of Chiefs of Police (IACP)).

[22] While the use of location-monitoring technology (e.g., GPS) does give supervising agents the ability to monitor the physical movements of sex offenders, there are drawbacks related to high costs of equipment, additional staffing for monitoring and review, dependence on cell phone connections, etc. And needless to say, some sex offenders have figured out how to defeat GPS monitoring, which indicates where the offender may be but not what he is doing.

[23] Burrell, Bill, "Caseload Standards for Probation and Parole," The American Probation and Parole Association (September 2006).

[24] DeMichele, Matthew, "Probation and Parole's Growing Caseloads and Workload Allocation: Strategies for Managerial Decision Making," The American Probation and Parole Association (May 4, 2007).

[25] It is important to make the distinction that caseload refers to the number of offenders supervised by the officer and workload is the time it takes per day to complete various tasks for each case.

[26] As quoted in "Probation and Parole's Growing Caseloads and Workload Allocation: Strategies for Managerial Decision Making", *supra* note 23, at 20.

[27] A Philadelphia study offers another case in point regarding caseloads. In 2006, over 22 percent of murder arrests and 16 percent of the murder victims were clients of the adult probation and parole department (APPD) of the First Judicial District of Pennsylvania. Virtually all were under 25 years of age and were but a small portion of the 52,000 people assigned to the 285 APPD officers. See Sherman, Lawrence W., "Reducing Homicide by Enhancing High-Risk Probation and Parole," University of Pennsylvania Jerry Lee Center of Criminology (2007).

[28] Burrell, Bill, "Caseload Standards for Probation and Parole," The American Probation and Parole Association (September 2006).

[29] Taxman et al., "Tools of the Trade," DOJ National Institute of Corrections and Maryland Dep't of Public Safety and Correction Services at "Introduction, the State of Supervision" (available at http://training.nctasc.net/toolsofthetrade/ introduction/page4.htm).

[30] DeMichele, Matthew, "Prsssobation and Parole's Growing Caseloads and Workload Allocation: Strategies for Managerial Decision Making," The American Probation and Parole Association (May 4, 2007).

[31] This is supported by the American Probation and Parole Association (APPA) guidelines, although APPA suggests a cap of no more than 35 high risk offenders.

[32] "Monitoring the Sex Offender," TECHBEAT Newsletter, National Law Enforcement and Corrections Technology Center (Winter 2005).

[33] Id.

[34] While the class focuses on managing sex offenders, the techniques are applicable to other types of cybercrime as well.

[35] Officers advise that other areas of emerging technology that are frequently used by offenders include Internet-connected cell phones and gaming consoles that have the capability for live online communications.

[36] "Monitoring the Sex Offender," TECHBEAT Newsletter, National Law Enforcement and Corrections Technology Center (Winter 2005).

[37] U.S. Department of Justice, Bureau of Justice Assistance, "Managing Sex Offenders," at 1 (2006) (published jointly with the International Association of Chiefs of Police (IACP)).

Legal Issues: Limiting Computer and Internet Use

by Richard C. LaMagna and Mark Berejka*

Courts around the United States have been considering the constitutional and other legal limits on law enforcement's power to restrict and monitor Internet access as part of probation or parole. As courts weigh probationers' Fourth Amendment and other rights against the government's need for effective monitoring of convicted sex offenders, certain issues and legal principles are beginning to emerge from the case law.[1] This article discusses those issues and principles. A review of relevant statues follows this article (see page 27).

Overview of the Relevant Legal Principles

The basic principle allowing for monitoring of convicted sex offenders' computer and Internet usage is that an individual on supervised release is not free and does not enjoy the absolute liberty to which other citizens are entitled.[2] Rather, probationers and parolees are entitled only to conditional liberty dependent on special probation restrictions. Accordingly, the government may institute provisions that may otherwise be unconstitutional as applied to citizens in general.

One justification for the diminished Fourth Amendment interests of probationers is that, when agreeing to the terms of probation, the probationer has waived certain constitutional claims related to his Fourth Amendment liberty or privacy rights. In particular, an agreement between a probationer, probation officials, and the court can be viewed as a contract to which the probationer waives Fourth Amendment rights in exchange for not going to prison, or for release from prison in the case of a parolee.[3]

Courts will apply the "special needs" doctrine when determining the appropriate scope of a supervised release provision. The "special needs" doctrine allows—under certain circumstances—law enforcement officers to conduct warrantless searches of those on probation. Thus, while criminal investigative searches normally require a warrant supported by probable cause, routine probationary searches not designed for criminal prosecution fall within the "special needs" exception. More specifically, supervision of offenders while they are on probation or parole is a "special need" of the government that permits "a degree of impingement upon privacy that would not be constitutional if applied to the public at large."[4]

In addition, federal statutes provide a framework for the government's use of the "special needs" doctrine in specific cases. One such statute provides that routine searches and monitoring must be justified by the "nature and circumstances of the offense and the history and characteristics of the defendant," the need to prevent recidivism, and the need to provide the defendant with adequate and effective correctional treatment. 18 U.S.C. § 3553(a)(1)-(2). In addition, searches and monitoring must impose "no greater deprivation of liberty than is reasonably necessary" to achieve these goals. 18 U.S.C. § 3583(d).[5] In sum, when faced with a challenge to a specific monitoring and search plan, courts will apply these generalized standards to determine if the plan complies with the Fourth Amendment and governing statutes.

To date, courts have generally rejected lifetime bans on probationer or parolee access to computers or the Internet.

Summary of Relevant Case Law

Applying these principles, courts have analyzed the constitutionality of various release provisions imposed on persons who exploited children using computers or the Internet. In particular, courts have analyzed the permissibility of outright bans on computer or Internet access as well as the potential for less restrictive provisions that would permit filtering of Internet content or monitoring of the probationer's computer usage.

These courts have held that, because the use of computers and the Internet have become such an integral part of our work and personal lives, convicted sex offenders—even those who habitually use computers to commit their offenses—cannot be subjected to such lifetime bans. For example, in *United States v. Voelker*,[6] the Third Circuit Court of Appeals held that a lifetime ban on computer access fell "woefully short" of the requirement that any restrictions imposed on probationers be "narrowly tailored to impose no greater restriction than necessary." In urging the court to uphold the release provision, the government contended that the restrictions were warranted under a prior case, *United States v. Crandon*, in which the same court upheld a limited three-year ban on Internet access after the defendant in that case used the Internet to seek out and communicate with his victims and traveled to meet a minor he had met online.[7] In distinguishing the two cases, the court relied heavily on both the duration of the proposed ban (lifetime versus three years) as well as the differences in the conduct of the two offenders, finding Crandon's computer-related conduct to be more egregious than that of Voelker.

The *Voelker* court also strongly suggested that for many types of crimes a lifetime ban on all computer use could never be justified, stating that such a ban "is the functional equivalent of prohibiting a defendant who pleads guilty to possession of magazines containing child pornography from ever possessing any books or magazines of any type during the remainder of his or her life." Although the court recognized the difficulty in tailoring release provisions for crimes involving computers and the Internet due to the prevalence of this technology, the court specifically held that these difficulties "do[] not, however, justify the kind of lifetime cybernetic banishment that was imposed here."

** The authors thank Sarah Johnson and Theo Angelis, attorneys at K&L Gates, for their assistance in helping to develop this review of legal issues.*

As *Crandon* demonstrates, however, courts are willing to impose some type of ban on computer or Internet access depending on the nature of the conduct at issue and provided that any such ban is for a defined period of time. For example, in *United States v. Paul,* the Fifth Circuit upheld a three-year ban on computer and Internet access for a convicted child pornographer who used the Internet to facilitate his crimes.[8] The court distinguished a previous case rejecting a similar ban, *United States v. White*,[9] holding that an outright ban on computer and Internet access was not per se impermissible simply because a defendant cannot use the Internet to obtain a weather report or other legal information. Rather, under circumstances such as those present in the *Paul* case, such a time-limited ban was appropriate to ensure public safety and to prevent recidivism.[10]

In addition to time-limited bans on access, courts appear to be willing to permit the mandatory use of filtering or monitoring technologies, finding that such provisions satisfy the "special needs" exception. For instance, in *United States v. Lifshitz,* the United States Court of Appeals for the Second Circuit indicated its willingness to uphold a supervised release provision conditioning the defendant's probation upon the installation of monitoring equipment on his home computer.[11] On appeal, the defendant challenged the probation condition as a violation of his Fourth Amendment right to be free of unreasonable searches. In analyzing these arguments, the Second Circuit stated that the "special needs" of the government to eradicate child pornography combined with the benefits to both society at large and to the defendant himself may justify some form of computer monitoring. The court rejected, however, the specific monitoring plan before it because the vague wording of the release provision made it difficult to determine whether the type of monitoring contemplated was adequately tailored to pass scrutiny. The court expressed concern in using technologies that were "overbroad and invasive." This holding was adopted by the Ninth Circuit in *United States v. Sales.*[12]

Similarly, in *United States v. Balon*, the Second Circuit examined whether a supervised release provision that required computer monitoring was constitutional.[13] In that case, the terms of the defendant's release required him to provide advance notice of all computers he would use during release and consent to the installation of an application that would permit random monitoring of those computers. The release provision also required the defendant to consent to unannounced examinations of his computers and retrieval of data. The court indicated that such monitoring may be permissible given the defendant's reduced expectation of privacy, but the court declined to engage in the necessary analysis of the remote monitoring provision until it was aware of the type of technology available at the time of the defendant's release. The court determined that "the extent to which the 'remote monitoring' provision involves a greater deprivation of liberty than reasonably necessary is governed by technological considerations."[14]

In light of cases such as *Lifshitz* and *Balon*, many states, as well as the Federal Probations Department, have adopted the practice of monitoring sex offenders' computer and Internet usage as a condition of court-ordered probation in order to prevent further offenses.[15] Based on these general legal principles and supporting case law, requiring targeted monitoring of a sex offender probationer's computer and Internet access as a condition of supervised release appears to be on solid legal ground, provided the monitoring is narrowly tailored to be no broader than necessary.[16]

Endnotes

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

[2] Griffin v. Wisconsin, 483 U.S. 868, 874 (1987).

[3] Harold, Marc M., Computer Searches of Probationers – Diminished Privacies, "Special Needs" & "Whilst Quiet Pedophiles"—Plugging the Fourth Amendment into the "Virtual Home Visit," 75 Miss. L.J. 273 (2005).

[4] Griffin, 483 U.S. at 875.

[5] Notably, this statutory standard is applicable to federal release provisions, and different statutory or common law factors may apply to persons who are on probation or parole under state law.

[6] United States v. Voelker, 489 F.3d 139, 144-150 (3d. Cir. 2007).

[7] United States v. Crandon, 173 F.3d 122, 127 (3rd Cir. 1999) (upholding three year ban on probationer's possession of or access to "any form of computer network, bulletin board, Internet, or exchange format involving computers" without express permission).

[8] United States v. Paul, 274 F.3d 155 (5th Cir. 2001).

[9] United States v. White, 244 F.3d 1199 (10th Cir. 2001) (striking down an outright ban on possession of computer with Internet access during period of supervised release based on prior conviction of possession of child pornography; finding that total ban on use of Internet would be overbroad and would prevent probationer's access to legitimate Internet content).

[10] *But see,* United States v. Peterson, 248 F.3d 79 (2d Cir. 2001) (striking down outright ban on possession or use of computer with Internet capabilities or of mass storage devices as not a reasonably related to probationer's offense when release provision was related to prior conviction for incest which did not involve computers or the Internet).

[11] United States v. Lifshitz, 369 F.3d 173 (2d Cir. 2004).

[12] United States v. Sales, __ F.3d __, ___ (No. 06-50219, *1695) (9th Cir., February 9, 2007) ("A computer monitoring condition in some form may be reasonable. However, to comply with the Fourth Amendment, it must be narrowly tailored—producing no greater deprivation of liberty than is reasonably necessary. At present, the text [of the release order] gives no indication as to what kinds or degrees of monitoring are authorized—and, as courts have noted, monitoring software and/or hardware takes many forms, with greatly varying degrees of intrusiveness. *See, e.g.,* United States v. Lifshitz, 369 F.3d 173, 175, 190-92 (2d Cir. 2004); see also United States v. Stephens, 424 F.3d 876, 880-81 (9th Cir. 2005) (discussing the "division of labor," in terms of decision-making, between the district court and probation officer)").

[13] United States v. Balon, 384 F.3d 38 (2d Cir. 2004).

[14] Balon, 384 F.3d at 45–46.

[15] *See, e.g.*, United States v. Tanasi, 2003 WL 328303 (S.D.N.Y. 2003) (release provision providing for installation of systems to enable monitoring or filtering of computer use on a regular or random basis for convicted child pornographer).

[16] As mentioned above, a recent federal decision overturned a monitoring law passed by the Indiana legislature in early 2008 and created momentary confusion in the supervisory community – until it became clear that the law was only overturned *in part.* The decision does not challenge monitoring of convicted sex offenders *while on parole or probation*, but does bar it, in that jurisdiction, with respect to registered sex offenders who have finished their supervisory terms. Doe et al. v. Marion County, Case no. 1:08-cv-0436-DFH-TAB (S.D. Ind., Hamilton, J.) (slip op. July 24, 2008). And as of this writing, it is not known if the government will appeal.

Sex Offender Computer Use: Relevant State Statutes

by Richard C. LaMagna and Mark Berejka

California

CAL. PENAL CODE Section 1203.047 (West 2004). Conviction of computer crime; probation.

A person convicted of certain enumerated computer crimes may be granted probation, but . . . [d]uring the period of probation, that person shall not accept employment where that person would use a computer connected by any means to any other computer, except upon approval of the court and notice to and opportunity to be heard by the prosecuting attorney, probation department, prospective employer, and the convicted person. Court approval shall not be given unless the court finds that the proposed employment would not pose a risk to the public.

Florida

FLA. STAT. ANN. Section 948.03(5)(a)(7) (West 2001). Terms and conditions of probation or community control.

Unless otherwise indicated in the treatment plan provided by the sexual offender treatment program, a prohibition on viewing, owning, or possessing any obscene, pornographic, or sexually stimulating visual or auditory material, including telephone, electronic media, computer programs, or computer services that are relevant to the offender's deviant behavior pattern.

Georgia

SB 474 (signed May 14, 2008). Section 5. Code Section 42-8-35 of the Official Code of Georgia Annotated, relating to terms and conditions of probation, is amended by revising subsection (b) as follows:

(b) In determining the terms and conditions of probation for a probationer who has been convicted of a criminal offense against a victim who is a minor or dangerous sexual offense as those terms are defined in Code Section 42-1-12, the court may provide that the probationer shall be. . .

(2) Required to wear a device capable of tracking the location of the probationer by means including electronic surveillance or global positioning systems. The department shall assess and collect fees from the probationer for such monitoring at levels set by regulation by the department;

(3) Required, either in person or through remote monitoring, to allow viewing and recording of the probationer´s incoming and outgoing e-mail, history of websites visited and content accessed, and other Internet based communication;

(4) Required to have periodic unannounced inspections of the contents of the probationer´s computer or any other device with Internet access including the retrieval and copying of all data from the computer or device and any internal or external storage or portable media and the removal of such information, computer, device, or medium.

(c) The supervision provided for under subsection (b) of this Code section shall be conducted by a probation officer, law enforcement officer, or computer information technology specialist working under the supervision of a probation officer or law enforcement agency.

Illinois

725 ILL. COMP. STAT. ANN. Section 207/40(b)(5)(T) (West Supp. 2005). Commitment.

(b) (5) An order for conditional release places the person in the custody, care, and control of the Department. The court shall order the person be subject to the following rules of conditional release, in addition to any other conditions ordered, and the person shall be given a certificate setting forth the conditions of conditional release. These conditions shall be that the person. . .

(T) neither possess or have under his or her control any material that is pornographic, sexually oriented, or sexually stimulating, or that depicts or alludes to sexual activity or depicts minors under the age of 18, including but not limited to visual, auditory, telephonic, electronic media, or any matter obtained through access to any computer or material linked to computer access use.

Indiana

SB 258 (signed March 24, 2008). section 16. ic 35-38-2-2.2, as amended by p.l.216-2007, section 40, is amended to read as follows [effective July 1, 2008].

Sec. 2.2. As a condition of probation for a sex offender (as defined in IC 11-8-8-4.5), the court shall:

(1) require the sex offender to register with the local law enforcement authority under IC 11-8-8; and
(2) prohibit the sex offender from residing within one thousand (1,000) feet of school property (as defined in IC 35-41-1-24.7), **as measured from the property line of the sex offender's residence to the property line of the school property,** for the period of probation, unless the sex offender obtains written approval from the court;
(3) require the sex offender to consent: (A) to the search of the sex offender's personal computer at any time; and (B) to the installation on the sex offender's personal computer or device with Internet capability, at the sex offender's expense, of one (1) or more hardware or software systems to monitor Internet usage; and
(4) prohibit the sex offender from: (A) accessing or using certain web sites, chat rooms, or instant messaging programs frequented by children; and (B) deleting, erasing, or tampering with information on the sex offender's personal computer with intent to conceal an activity prohibited by clause (A).

Minnesota

MINN. STAT. ANN.' 243.055 (West 2003). Computer Restrictions.

Subdivision 1. Restrictions to use of online services. If the commissioner believes 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, the commissioner may impose one or more of the following conditions:

(1) prohibit the individual from possessing or using a computer with access to an Internet service or online service without the prior written approval of the commissioner;
(2) prohibit the individual from possessing or using any data encryption technique or program;
(3) require the individual to consent to periodic unannounced examinations of the individual's computer equipment by a parole or probation agent, including the retrieval and copying of all data from the computer and any internal or external peripherals and removal of such equipment to conduct a more thorough inspection;
(4) require consent of the individual to have installed on the individual's computer, at the individual's expense, one or more hardware or software systems to monitor computer use; and
(5) any other restrictions the commissioner deems necessary.

Subdivision. 2. Restrictions on computer use. If the commissioner believes a significant risk exists that a parolee, state-supervised probationer, or individual on supervised release may use a computer to engage in criminal activity or to associate with individuals who are likely to encourage the individual to engage in criminal activity, the commissioner may impose one or more of the following restrictions:

(1) prohibit the individual from accessing through a computer any material, information, or data that relates to the activity involved in the offense for which the individual is on probation, parole, or supervised release;
(2) require the individual to maintain a daily log of all addresses the individual accesses through computer other than for authorized employment and to make this log available to the individual's parole or probation agent;
(3) provide all personal and business telephone records to the individual's parole or probation agent upon request, including written authorization allowing the agent to request a record of all of the individual's outgoing and incoming telephone calls from any telephone service provider;
(4) prohibit the individual from possessing or using a computer that contains an internal modem and from possessing or using an external modem without the prior written consent of the commissioner;
(5) prohibit the individual from possessing or using any computer, except that the individual may, with the prior approval of the individual's parole or probation agent, use a computer in connection with authorized employment;
(6) require the individual to consent to disclosure of the computer-related restrictions that the commissioner has imposed to any employer or potential employer; and
(7) any other restrictions the commissioner deems necessary.

Subdivision. 3. Limits on restriction. In imposing restrictions, the commissioner shall take into account that computers are used for numerous, legitimate purposes and that, in imposing restrictions, the least restrictive condition appropriate to the individual shall be used.

Nevada

NEV. REV. STAT. ANN. Section176A. 413 (LexisNexis Supp. 2001). Restrictions relating to computers and use of Internet and other electronic means of communication; powers and duties of court; exceptions.

1. Except as otherwise provided in subsection 2, if a defendant is convicted of stalking with the use of an Internet or network site or electronic mail or any other similar means of communication pursuant to subsection 3 of NRS 200.575, an offense involving pornography and a minor pursuant to NRS 200.710 to 200.730, inclusive, or luring a child or mentally ill person through the use of a computer, system or network pursuant to paragraph (a) or (b) of subsection 4 of NRS 201.560 and the court grants probation or suspends the sentence, the court shall, in addition to any other condition ordered pursuant to NRS 176A.400, order as a condition of probation or suspension that the defendant not own or use a computer, including, without limitation, use electronic mail, a chat room or the Internet.
2. The court is not required to impose a condition of probation or suspension of sentence set forth in subsection 1 if the court finds that:
   (a) The use of a computer by the defendant will assist a law enforcement agency or officer in a criminal investigation;
   (b) The defendant will use the computer to provide technological training concerning technology of which the defendant has a unique knowledge; or
   (c) The use of the computer by the defendant will assist companies that require the use of the specific technological knowledge of the defendant that is unique and is otherwise unavailable to the company.
3. Except as otherwise provided in subsection 1, if a defendant is convicted of an offense that involved the use of a computer, system or network and the court grants probation or suspends the sentence, the court may, in addition to any other condition ordered pursuant to NRS 176A.400, order as a condition of probation or suspension that the defendant not own or use a computer, including, without limitation, use electronic mail, a chat room or the Internet.
4. As used in this section:
   (a) "Computer" has the meaning ascribed to it in NRS 205.4735.
   (b) "Network" has the meaning ascribed to it in NRS 205.4745.
   (c) "System" has the meaning ascribed to it in NRS 205.476.

NEV. REV. STAT. ANN. Section 213.1258 (LexisNexis 2005). Conditions relating to computers and use of Internet and other electronic means of communication; powers and duties of board; exceptions.

1. Except as otherwise provided in subsection 2, if the Board releases on parole a prisoner convicted of stalking with the use of an Internet or network site or electronic mail or any other similar means of communication pursuant to subsection 3 of NRS 200.575, an offense involving pornography and a minor pursuant to NRS 200.710 to 200.730,

inclusive, or luring a child or mentally ill person through the use of a computer, system or network pursuant to paragraph (a) or (b) of subsection 4 of NRS 201.560, the Board shall, in addition to any other condition of parole, require as a condition of parole that the parolee not own or use a computer, including, without limitation, use electronic mail, a chat room or the Internet.

2. The Board is not required to impose a condition of parole set forth in subsection 1 if the Board finds that:
   (a) The use of a computer by the parolee will assist a law enforcement agency or officer in a criminal investigation;
   (b) The parolee will use the computer to provide technological training concerning technology of which the defendant has a unique knowledge; or
   (c) The use of the computer by the parolee will assist companies that require the use of the specific technological knowledge of the parolee that is unique and is otherwise unavailable to the company.
3. Except as otherwise provided in subsection 1, if the Board releases on parole a prisoner convicted of an offense that involved the use of a computer, system or network, the Board may, in addition to any other condition of parole, require as a condition of parole that the parolee not own or use a computer, including, without limitation, use electronic mail, a chat room or the Internet.
4. As used in this section:
   (a) "Computer" has the meaning ascribed to it in NRS 205.4735.
   (b) "Network" has the m eaning ascribed to it in NRS 205.4745.
   (c) "System: has the meaning ascribed to it in NRS 205.476.

New York

A09859 (signed April 28, 2008). Section 7. Subdivision 4-a of section 65.10 of the penal law, as amended by 19 chapter 320 of the laws of 2006, is amended to read as follows:

4-a. Mandatory {condition} conditions for sex offenders. . .

(b) when imposing a sentence of probation or conditional discharge upon a person convicted of an offense for which registration as a sex offender is required pursuant to subdivision two or three of section one hundred sixty-eight-a of the correction law, and the victim of such offense was under the age of eighteen at the time of such offense or such person has been designated a level three sex offender pursuant to subdivision six of section one hundred sixty-eight-l of the correction law or the Internet was used to facilitate the commission of the crime, the court shall require, as mandatory conditions of such sentence, that such sentenced offender be prohibited from using the Internet to access pornographic material, access a commercial social networking website, communicate with other individuals or groups for the purpose of promoting sexual relations with persons under the age of eighteen, and communicate with a person under the age of eighteen when such offender is over the age of eighteen, provided that the court may permit an offender to use the internet to communicate with a person under the age of eighteen when such offender is the parent of a minor child and is not otherwise prohibited from communicating with such child. Nothing in this subdivision shall be construed as restricting any other lawful condition of supervision that may be imposed on such sentenced offender. As used in this subdivision, a "commercial social networking website" shall mean any business, organization or other entity operating a website that permits persons under eighteen years of age to be registered users for the purpose of establishing personal relationships with other users, where such persons under eighteen years of age may: (i) create web pages or profiles that provide information about themselves where such web pages or profiles are available to the public or to other users; (ii) engage in direct or real time communication with other users, such as a chat room or instant messenger; and (iii) communicate with persons over eighteen years of age; provided, however, that, for purposes of this subdivision, a commercial social networking website shall not include a website that permits users to engage in such other activities as are not enumerated herein.

Section 8. Section 65.10 of the penal law is amended by adding a new subdivision 5-a to read as follows:

5-a. Other conditions for sex offenders. When imposing a sentence of probation upon a person convicted of an offense for which registration as a sex offender is required pursuant to subdivision two or three of section one hundred sixty-eight-a of the correction law, in addition to any conditions required under subdivisions two, three, four, four-a and five of this section, the court may require that the defendant comply with a reasonable limitation on his or her use of the Internet that the court determines to be necessary or appropriate to ameliorate the conduct which gave rise to the offense or to protect public safety, provided that the court shall not prohibit such sentenced offender from using the internet in connection with education, lawful employment or search for lawful employment.

North Dakota

N.D. CENT. CODE Section 12.1-32-07(4)(r) (Supp. 2005). Supervision of probationer. Conditions of probation. Revocation.

4. When imposing a sentence to probation, probation in conjunction with imprisonment, or probation in conjunction with suspended execution or deferred imposition of sentence, the court may impose such conditions as it deems appropriate and may include any one or more of the following: r. Refrain from any subscription to, access to, or use of the Internet.