WHAT IS THE ROLE OF THE ATTORNEY GENERAL AS A CHILD ADVOCATE IN THE WORLD OF CYBER LAWS?


The role of the Attorney General is to uphold the laws of the state while protecting the people of the state, particularly children. The Attorney General has the duty to prosecute and protect the dignity of the laws and people of the State of Mississippi, and he must balance the legal issues with the moral issues that accompany online crimes against children.

At times, the Attorney General must defend the constitutionality of laws and prosecute under
laws that may be antiquated and understandably did not anticipate the following: sexual solicitation of a child via a webcam, text message or x-box; social network postings from a cell phone of sexually explicit images of children which under the letter of the law are child pornography; the peer-to-peer file sharing of child pornography and incest training files; cloud computer storage; forensic searches of encrypted computer files; cyberbullying on campus; teen driving while texting resulting in deaths; or online impersonations and harassment resulting in youth suicide. Law is, of course, retrospective and reactive, and technology changes the kinds of crimes that the Attorney General must address. Many crimes involve some kind of electronic media. The question of which law applies is not necessarily whether the punishment fits the crime, but whether the facts can be prosecuted under the existing law.

Who could have foreseen that ownership of online information, such as music, videos, or streaming media would be an issue or that teens would think nothing of downloading songs without paying the artist? For example, should sexting and texting be charged under the “posting” statute if done with the intent to harm, or should they be charged under the Obscene Electronic Communications statute if committed with a cell phone? The challenge of protecting our children and using the existing laws is great.

At least 75 percent of the cases prosecuted by the Attorney General’s Office are child exploitation, which under the Mississippi statute (one of the strongest in the nation), is defined as the solicitation, seduction, enticement, persuasion of an actual child under the age of eighteen to meet for sex. Prosecution may be for production, receipt, transmission or possession of child pornography. The mandatory penalty is five to 40 years incarceration per convicted offense.

Criminals are not just sharing images – they are committing hands-on offenses against children. According to research reported in 2009 by the University of New Hampshire’s Crimes Against Children Research Center, the number of reported solicitations to children increased by 21 percent between 2000 and 2006. From 2000 to 2006, online predator solicitations to undercover law enforcement increased 381 percent, leading to the conclusion that predators ARE talking to children online. As early as 1987, Dr. Gene Abel at the University of Mississippi Medical Center looked at the number of offenses per self reporting sex offender in a study of 561 males who admitted that together they had offended a total of 27,777 child victims. The offenders admitted to multiple victims and multiple offenses. An example in Mississippi of a multiple offender is that of John Boyles who pled guilty in Marion County to possession of child pornography and to the fondlings of two children in a case worked by the Attorney General’s Internet Crimes Against Children Unit (ICAC). Boyles is serving seven years on the child pornography possession and two years each on the two fondlings.

Consequently, the Attorney General’s attack on online crimes against children must be multi-dimensional: 1) investigations, 2) forensic analyses, 3) prosecutions, 4) trainings of law enforcement, 5) legislative initiatives, and, 6) a public Internet awareness campaign. This article looks at how the Attorney General’s office works as an advocate for children who are victims of online crime and joins with federal and state partners to do so. The task is too great for a single agency, and cooperation is a must. Flint Waters, programmer for TLO and the creator of the Wyoming Toolkit/Child Protection System, commented on the primary goal of saving children and the immensity of the task, stating, “There are so many things we do to try to combat this problem. It is hard to imagine a recent technological breakthrough that some bandit hasn’t tried to leverage to their advantage. Through it all, it seems the best guidance comes from those we serve. I have never rescued a child that wanted to know if I was local, state or fed or wondered which agency would prosecute.”

Recognizing the need to fight cyber crimes
against children, former Attorney General Mike Moore started a high tech unit in 2002 with the help of a Department of Justice (DOJ) grant through the University of Mississippi’s National Center for Justice and the Rule of Law (NCJRL), a partnership which continues today. Attorney General Jim Hood also has made the fight against online child crimes his priority.

In 2007, the Attorney General’s cyber unit qualified as an Internet Crimes Against Children grantee and became one of 61 ICAC task forces across the United States, which interact daily on child investigations. Congress strengthened ICAC’s in the Child Protect Act of 2008, and the coordinated, unified work of the ICAC units is now the cornerstone for crimes against children investigations in the United States. The Mississippi unit forensically analyzes electronic media, prosecutes and educates the public on internet crimes. ICAC affiliates are trained in investigative techniques and prosecutions. Affiliates also are interconnected and interactive. In January of 2009, with the addition of Operation Fairplay, now known as the Wyoming Tool Kit / Child Protection Software (WTK/CPS), a proactive software that detects peer-to-peer file sharing of identified child pornography, the unit has changed from reactive to proactive investigations, greatly increasing the number of cases opened by the Mississippi ICAC and its statewide affiliates. In a unified, multi-jurisdictional and multi-disciplinary cooperative effort, the Mississippi ICAC task force has 26 local law enforcement affiliate agencies who have signed a Memorandum of Understanding (MOU) to abide by ICAC investigation standards and protocols. Our affiliates have been trained in use of WTK/CPS and Digital Forensics Write Blockers. Initial and advanced training for affiliates and Mississippi law enforcement investigators on WTK/CPS will be provided at the Fall Mississippi Prosecutors’ Conference. Basic cyber crimes training will be sponsored in conjunction with the U.S. Attorney’s Office, S.D. of Mississippi, in November 2010.

Mississippi ICAC law enforcement affiliates who have signed an ICAC MOU include as of this printing: Office of the District Attorney, (9th District) Richard Smith, D.A.; Office of the District Attorney, (19th District), Anthony Lawrence, D.A.; Cleveland Police Department; Columbus Police Department; Copiah County Sheriff’s Office; DeSoto County Sheriff’s Office; D’Iberville Police Department; Florence Police Department; Fulton Police Department; George County Sheriff’s Department; George County School District Police Department; Harrison County Police Department; Hinds County Sheriff’s Office Child Protection Unit; Horn Lake Police Department; Itawamba County Sheriff’s Office; Iuka Police Department; Jackson County Sheriff’s Department; Laurel Police Department; The Mississippi Lawyer August-October 2010 43 Lee County Sheriff’s Office; Long Beach Police Department; Mississippi Bureau of Investigations; Olive Branch Police Department; Petal Police Department; Prentiss County Sheriff’s Office; Richland Police Department; Ridgeeland Police Department; Ripley Police Department; Tippah County Sheriff’s Office; Tupelo Police Department; Warren County Sheriff’s Office; Waveland Police Department; the U.S. Department of Justice, Northern District Mississippi, William Martin, Acting U.S. Attorney and the U.S. Department of Justice, Southern District Mississippi, Donald Burkhalter, U.S. Attorney. Other federal partners of the ICAC task force include the F.B.I., I.C.E., the U.S. Postal Inspection Service, and the U.S. Secret Service. The ICAC task force provides technical assistance, investigative and prosecutorial support, and forensic examination of all crimes involving computer technology within the entire state of Mississippi.

University ICAC task force affiliates include Mississippi State University, the University of Mississippi and Jackson State University. Through a DOJ grant, Mississippi State has furnished much of the forensics laboratory equipment and has participated in teaching Mississippi law enforcement how to capture, preserve and forensically analyze electronic evidence. MSU’s continued support has enabled the affiliates to work physically side-by-side in the Sillers
Building as a fusion center – the first joint venture of its kind in the nation.

Following the initial ICAC grants, the unit was awarded an ICAC American Recovery Act Grant which allowed the hiring of an additional prosecutor and an educational director plus enhanced the job performance of other staff members through job-related educational trainings and certifications such as IACIS, ACE and FTK. The unit also has received support in 2009 from the Mississippi Legislature with the imposition of a $1 fine for each traffic ticket dedicated to the AG Cyber Crime investigations and prosecutions.

Article continued on page 18....

ATTORNEYS GENERAL FIGHTING CYBERCRIME

ARIZONA

Attorney General Terry Goddard announced that Eric Weinstein was sentenced to five years in prison on Internet fraud charges. Weinstein used fraudulent names and credit cards to open numerous eBay accounts to sell items on the company’s website. While the credit cards he used showed sufficient credit to open a seller’s account, they were actually one-time user cards, resulting in the accounts becoming invalid after eBay’s authorization test was complete. Weinstein then sold thousands of items on eBay using these fraudulent accounts, and eBay was unable to collect the auction fees as a result of the invalid cards on file. Ebay sustained hundreds of thousands of dollars in auction fee losses. Weinstein pleaded guilty to two counts of fraudulent schemes and artifices, both class 2 felonies. In addition to the prison term, he was sentenced to two years of intensive supervised probation following his release and was ordered to pay restitution of $900,000 to eBay. The case was investigated by the U.S. Secret Service and the Scottsdale Police Department and prosecuted by Assistant Attorney General Theodore Campagnolo.

CONNECTICUT

Attorney General Richard Blumenthal submitted testimony calling on Congress to prevent the tracking of consumers’ online activity without their express permission and restrict the use and storage of data collected by companies. The testimony was submitted to the House Subcommittee on Commerce, Trade and Consumer Protection, which held a hearing on do-not-track proposals. Attorney General Blumenthal called on Congress to: 1) require the Federal Trade Commission to adopt rules governing the conduct of any entity collecting data that can be directly linked to a computer or other electronic device; 2) require any such entity collecting personal information to provide clear and concise notice of the collection and its use; 3) prohibit such entity from collecting personal information unless affirmatively authorized by the consumer; 4) prohibit any entity that has previously collected personal information from using or disseminating it unless affirmatively authorized by the consumer; and 5) enact the same penalties for the unauthorized collection or use of personal information as in the Do Not Call law – an unfair or deceptive trade practice and a fine of up to $16,000 per violation.

DELWARE

Attorney General Joseph Biden Ill’s Child Predator Task Force conducted a proactive undercover investigation, which led to the arrest of Michael Mathews, a college student, on child pornography charges. Task Force officers and the Dover Police Department executed a search warrant on Mathews’ apartment and seized a laptop computer and other digital media, which contained numerous files of child pornography. Mathews was charged with 29 counts of using a computer to unlawfully depict a child engaging in a prohibited sex act.
**FLORIDA**

Attorney General Bill McCollum joined Mark Ober, State Attorney for the 13th Judicial District, to announce that a jury found Marcus Morgan guilty on charges of 26 counts of possession of child pornography. Attorney General McCollum’s CyberCrime Unit investigators located images of child pornography during a routine undercover investigation and traced the images back to Morgan’s computer. A search warrant was served at his home and digital evidence was seized for forensic analysis. Many of the images were of children appearing to be between the ages of five-13 years old. Morgan could face a minimum of 24 years in prison according to Florida’s sentencing guidelines. The U.S. Immigration and Customs Enforcement (ICE) and the Hillsborough County Sheriff’s Office, also members of the Central Florida Internet Crimes Against Children (ICAC) Task Force, assisted in the investigation. Morgan was prosecuted by the State Attorney’s Office.

**KENTUCKY**

Attorney General Jack Conway’s Office implemented an electronic warrant management system (eWarrants) in the 19th Judicial Circuit, bringing to the number of counties that have received the system under a $3.9 million American Recovery and Reinvestment Act (ARRA) awarded to Attorney General Conway’s Office. His office, in partnership with the Administrative Office of the Courts, the Kentucky State Police, the Kentucky Office of Homeland Security and Open Portal Solutions, Inc., provided training and support for the new system. Counties that have the system now have service rates on arrest warrants of up to 80 percent, compared to about 25 percent with paper warrants. More than 62 percent of bench warrants entered into the system have been served, compared to about 10 percent under the old system. The eWarrant system facilitates the sharing of information among law enforcement entities concerning active warrants via the Law Enforcement Information Network of Kentucky. The grant was awarded by the U.S. Department of Justice, Bureau of Justice Assistance.

**Massachusetts**

Attorney General Martha Coakley’s Cyber Crime Division partnered with the National White Collar Crime Center (NW3C) to deliver the Secure Techniques for Onsite Preview (STOP) training to more than 100 local, state and federal law enforcement assigned to departments throughout the Commonwealth. The STOP course enables law enforcement or probation and parole to view a suspect computer for evidence in a forensically sound manner. Although it is a two-day course, this training was delivered in an intense eight-hour day. All attendees passed the written and practical exams and received Certificates of Training. The instructors were all from local and state law enforcement agencies in the Commonwealth and Rhode Island who had been certified by NW3C during a train-the-trainer program.

**Mississippi**

Attorney General Jim Hood’s Internet Crimes Against Children (ICAC) Task Force investigators arrested Michael Hitchcock, who is charged with three counts of child pornography possession. Hitchcock was arrested at his home. The Marshall County Sheriff’s Office assisted with the execution of search warrants and arrest.

**New Jersey**

Attorney General Paula Dow joined Criminal Justice Director Stephen Taylor to announce that Daniel Goncalves pleaded guilty to stealing a company’s Internet domain name and selling it on eBay for more than $110,000 to an unsuspecting buyer; this is the first known conviction for a domain name theft. The true owners of P2P.com, LLC, which has
an estimated worth of between $160,000 to $200,000 because of its relation to P2P file sharing, discovered that the domain name had been transferred without their knowledge or consent. They contacted the State Police Cyber Crimes Unit, which began an investigation eventually leading to Goncalves. They executed a search warrant at Goncalves’ residence and seized a large volume of business and computer records. Goncalves admitted that he illegally accessed the domain name account and transferred it to his account, later offering it for sale on eBay. He pled guilty to theft by unlawful taking, theft by deception and computer theft, all in the second degree. The Division of Criminal Justice will recommend that he be sentenced to five years in prison and be ordered to pay restitution. Deputy Attorney General Kenneth Sharpe prosecuted the case and represented the Division’s Major Crimes/Computer Analysis & Technology Unit at the plea hearing. Detective Sgt. John Gorman of the State Police led the investigation.

OHIO

Attorney General Richard Cordray entered into a settlement with prepaid wireless provider Start Wireless Group Inc., d/b/a Page Plus Inc., resolving concerns that the company misrepresented its services and failed to disclose important terms and conditions. Page Plus purchases available mobile phone plans from a national provider and makes them available to consumers through prepaid phone card plans. Attorney General Cordray’s Office received more than 60 complaints against the company, many of them involving their Unlimited Talk ‘n Text plan. Consumers said ads for the plan promised unlimited minutes and text messages and 20 megabytes of data for a flat monthly rate, but the company automatically transferred consumers to a standard pay-per-minute plan after they “abused” the system. Attorney General Cordray’s Office discovered that Page Plus did not give consumers details on how they “abused” the plan and that many ads failed to provide terms and conditions. Under the settlement, Page Plus agreed to clearly disclose all terms and conditions in ads and at the point of purchase and make specific changes to improve its customer service. The company will also provide $200 to eligible consumers with unresolved complaints regarding the matters discussed in the settlement.

PENNSYLVANIA

Attorney General Tom Corbett’s Child Predator Unit agents arrested John Lehosky, who is accused of sending multiple nude and sexually explicit webcam videos to what he believed was a 14-year-old girl, but was actually an undercover Unit agent using the online profile of an underage girl. Agents also seized Lehosky’s computer, which will be analyzed by Attorney General Corbett’s Computer Forensics Unit. Lehosky is charged with seven counts of unlawful contact with a minor and one count of criminal use of a computer, all third-degree felonies each punishable by up to seven years in prison and $15,000 fines. The State Police assisted in the investigation. Lehosky will be prosecuted by Deputy Attorney General Christopher Jones of the Child Predator Unit.

SOUTH CAROLINA

Attorney General Henry McMaster announced that Jeremy Dakin was arrested in an Internet predator sting conducted by the City of Charleston Police Department, a member of Attorney General McMaster’s Internet Crimes Against Children (ICAC) Task Force. Dakin was arrested on two counts of Criminal Solicitation of a Minor, a felony punishable by up to 10 years imprisonment on each count, and one count of Attempted Criminal Sexual Conduct with a Minor, a felony punishable by up to 20 years imprisonment. Arrest warrants allege that Dakin solicited sex online from an individual he believed to be a minor girl, but he was actually solicit-
ing an undercover police officer. He arranged to meet the “girl” at a predetermined location and was arrested upon his arrival. The Berkeley County Sheriff’s Office assisted in the case. Dakin will be prosecuted by Attorney General McMaster’s office.

**TEXAS**

Attorney General Greg Abbott joined state Senator Kirk Watson to propose legislation designed to prevent sexting. Under current state law, anyone who transmits an explicit image of a teen can face felony charges of possessing or trafficking in child pornography. Under the proposal put forth by Attorney General Abbott and Senator Watson, teen sexting would become a misdemeanor punishable by probation and restricted cell phone usage. Judges would be authorized to sentence minors to participate in an education program about sexting’s long-term harmful consequences.

**VIRGINIA**

Attorney General Ken Cuccinelli announced that Ronald Dawson, who tried to order child pornography from an undercover agent from the U.S. Postal Inspection Service (USPIS), was sentenced to 72 months of prison and 25 years of supervised release. He must also pay a $2,500 fine. Dawson purchased videos from the agent, and the USPIS prepared a package for controlled delivery to him at the post office. When Dawson signed for the package, he was confronted by agents. Assistant U.S. Attorney Nancy Healey and Lawrence “Chip” Muir of Attorney General Cuccinelli’s Computer Crime Section prosecuted the case.

**WASHINGTON**

Attorney General Rob McKenna announced that the owners of an e-commerce company that his office sued for repeatedly failing to deliver on their promises to help businesses nationwide sell their products online has been ordered by a court to pay for their actions. The suit was filed against Jeremy Avey, Alexander Martin and Brent Stanphill, as well as their businesses, Cybercom Technologies, d/b/a Wizy-Wiz eCommerce; TNT Cart, d/b/a Strada Technologies; and White Crane Technologies. The defendants will pay a $226,000 civil penalty and approximately $137,500 to reimburse the state’s investigative and legal costs. They will also pay more than $108,000 in restitution to 35 customers nationwide who complained about the issues identified in the suit. The court order also includes injunctive provisions that prevent the defendants from making misrepresentations in connection with an Internet business. Failure to comply with the terms would trigger an additional civil penalty of up to $25,000 per violation. The case was handled by Senior Counsel Paula Selis and Attorney General McKenna’s Consumer Protection High-Tech Unit.

**WISCONSIN**

Attorney General J.B. Van Hollen’s Division of Criminal Investigation special agents joined the Rothschild and Wausau Police Departments to arrest Ronald Housworth at his home on charges of Use of a Computer to Facilitate a Child Sex Crime. A search of Housworth’s home was conducted and evidence was seized. The arrest was the result of an undercover investigation by an officer from the Village of Pewaukee Police Department. Housworth later admitted to having online communication with a person whom he believed was a 14-year-old girl and traveling to meet “her” for sexual acts. He also admitted that he had what he identified as child pornography on his home computer.
ACTION IN THE SUPREME COURT

ARGUMENTS HEARD

On November 2, the Court heard arguments in Schwarzenegger v. Entertainment Merchants Ass’n, No. 08-1448, a case in which a California law designed to prevent juveniles from buying or renting violent video games is challenged. The law designates a video game as violent if it “appeals to a deviant or morbid interest of minors,” lacks “serious literary, artistic, political or scientific value for minors,” and allows minors to “inflict serious injury” that is “especially heinous, cruel or depraved.” Interestingly, these passages are similar to those the Court used to uphold laws banning the sale of pornography to underage youth.

The law also requires violent video games to be labeled “18,” designating that no one under the age of 18 can buy or rent them. Retailers who sell them to minors could be fined $1,000 per violation, although they can avoid penalties if they are duped by a minor with a fake ID. However, parents or legal guardians can buy these games for their children, since the law doesn’t address adult access nor does it prohibit manufacturers from producing or marketing them.

The law has not taken effect because federal courts in California struck it down, finding that it amounted to censorship in violation of the First Amendment. They also found that the legal standard used by the Supreme Court to uphold laws banning the sale of pornography to minors did not apply to the sale of violent video games.

In addition to the First Amendment argument, opponents of the law argue that the video game industry’s voluntary rating system and its agreement with major retailers to enforce a ban on the sale of violent video games to minors already achieves the state’s goal. They also note that many game consoles also contain parental controls that could be set to block violent video games.

CERT GRANTED

On November 29, the Court granted certiorari in Microsoft v. i4i Limited Partnership, an appeal concerning the evidentiary standard for invalidating patents. The case centers on a judgment against Microsoft in favor of i4i, a Toronto-based software developer. The Chief Justice did not participate in the consideration of Microsoft’s petition.

According to 35 U.S.C. § 252, a patent is presumed valid, and the courts must defer to the U.S. Patent and Trademark’s Office decision to grant the patent. This presumption can be overcome only by “clear and convincing evidence” to the contrary, even if the challenge is based on information that was not considered by the Patent Office.

Here, i4i accused Microsoft of infringing U.S. Patent No. 5,787,449, which addresses systems and methods for the separate manipulation of the architecture and content of a document, particularly for data representation and transformations. The trial court found certain versions of Microsoft Word incorporating XML technology infringed the ‘449 patent, and Microsoft was ordered to pay $200 million and to stop making, selling or using the infringing software. A federal district court raised the amount to $290 million when it affirmed the decision.

Microsoft argued that the ‘449 patent was invalid in view of the prior art, i.e. that the claimed invention was not new, or at least was obvious, when compared to pre-existing technology and, thus, the Patent Office should not have granted the patent. It asked a federal appeals court to review the case, but it declined to do so.

In its appeal, Microsoft argues that the burden of proof necessary to invalidate a patent should be much lower when the allegedly invalidating prior art was not considered by the Patent Office when it granted the patent. Instead, Microsoft contends that a “preponderance of the evidence” standard should apply under this circumstance. Under this
lower standard, a jury would have to decide whether it was “more likely or not” that the patent should be invalidated.

CERT DENIED

On November 29, the Court denied certiorari in Harper v. Maverick Recording Co., sometimes referred to as the “innocent infringer” case. It is the first music-downloading copyright appeal to go to trial and eventually reach the Court. At issue was whether the “inadvertent innocent infringer” defense to copyright violations should be eliminated for all music downloading. Whitney Harper admitted to using Kazaa, a peer-to-peer file-sharing program, to download and share digital audio files when she was a teenager. The industry sued her and her family for 37 copyrighted songs she had downloaded. Harper argued she was too young to understand the nature of her actions and that the music files she downloaded bore no copyright notice. “Innocent infringers” may be liable under federal law for up to $200 per track, while non-innocent infringers may be liable for up to $150,000 per track. Justice Samuel Alito dissented from the denial, saying there is a “strong argument” that federal law protections do not apply to digital music files.

Also on November 29, the Court denied certiorari in Tiffany & Co. v. eBay, Inc., refusing to overturn a decision finding that eBay is not violating Tiffany’s trademarks by offering items that might be counterfeit for sale on its website. Tiffany had claimed that eBay engaged in trademark infringement and dilution because most items that sellers list for sale on the auction site as genuine Tiffany silver jewelry are actually fakes. The lower courts noted that eBay took down the listings when Tiffany informed them they were counterfeit and ruled that eBay could not be held responsible for counterfeit goods being sold on their site if they didn’t know the items were fake.

LEGISLATIVE NEWS

ONLINE INFRINGEMENT/ COUNTERFEITING

PASSED COMMITTEE. On November 18, the Senate Judiciary Committee passed S. 3804, a bill sponsored by Senator Patrick Leahy (D-VT), that would authorize an in rem action against a domain name located outside the U.S. that offers goods or services in violation of the federal copyright law or sells and promotes counterfeit goods or services. The bill authorizes a court to issue a temporary restraining order, preliminary injunction or injunction against such domain. It also requires an ISP that is served with a court order in such action to take technically feasible or reasonable measures to prevent the infringement.

ONLINE SHOPPING PROTECTION

PASSED BOTH HOUSES. On December 15, S. 3386, a bill sponsored by Senator John Rockefeller (D-WVa) with the intent of making online shopping safer for consumers, passed the House after unanimously passing the Senate on November 30. The bill makes it unlawful for a third party seller to charge a consumer’s credit card or bank account unless the seller has disclosed all material terms and the seller has received the buyer’s express informed consent. It also makes it unlawful for the seller to disclose a buyer’s financial information. The bill makes it unlawful for an Internet seller to charge a consumer for goods or services through a negative option feature (where the consumer’s failure to take action to reject the goods or services is regarded as an acceptance). It authorizes a state attorney general to bring an action for injunctive relief in federal court.
INTERNET GAMBLING

PASSED TWO COMMITTEES. On November 30, H.R. 2267, a bill sponsored by Representative Barney Frank (D-MA) that proscribes requirements for Internet gambling, passed the House Committee on Energy and Commerce, having passed the Committee on the Judiciary on November 19. The bill prohibits operating an Internet gambling facility without a license issued by the Secretary of the Treasury. Under the bill, licensees are required to institute safeguards to prevent fraud, money laundering, terrorist financing and compulsive gambling, as well as pay taxes. It requires any qualified state to prescribe regulations for development of a program for problem or compulsive gamblers and develop a list of persons who are excluded from Internet gambling. The bill also allows a state to opt out of Internet gambling activities.

STUDY: MOST PARENTS MONITOR KIDS’ SOCIAL NETWORKING

Seventy-two percent of parents monitor their teens’ social networking accounts on a regular basis, according to a study on parent-teen attitudes towards online privacy conducted by privacy group Truste. Thirty-five percent of those monitoring do so on a daily basis, and another 10 percent are even secretly logged into their teens’ accounts. Eighteen percent of teens said they have been disciplined or “embarrassed” by their parents online. The study also found that 89 percent of the 1,037 parents in the study wanted the social networking sites to have default privacy settings that limited profile access to their teens’ accounts. Another 82 percent wanted the ability to delete their teens’ posts. Truste also released privacy recommendations for teens and parents; the advice for parents is talk, chat and email with your teen about privacy; the advice to teens is befriend your parents online. The study can be accessed at http://www.truste.com.

NEWS YOU CAN USE

PA BAR ALLOWS VIRTUAL OFFICE

The Pennsylvania Bar Association decided that state lawyers may forego a physical office and provide legal services exclusively over the Internet, provided they take steps to safeguard confidential electronic communications and ensure that clients whom they may never meet personally fully understand the relationship under the Rules of Professional Conduct. Under Ethics Opinion No. 2010-200, the attorney is not required to list a physical address in his or her advertisements, but must disclose the city or town where the lawyer who will perform the services is located. The Opinion can be accessed at http://lawyersusaonline.com/wp-files/pdfs-2/f2010-200.pdf.

BOTNETS INFECT 2 MILLION US PCS

The U.S. leads the world in number of Windows PCs that are part of botnets, according to a 240-page report by Microsoft. More than 2.2 million U.S. PCs were found to be part of botnets, networks of hijacked home computers, during the first six months of 2010. The research revealed that Brazil had the second highest level of infections at 550,000. Infections were highest in South Korea, where 14.6 out of every 1,000 computers were found to be part of botnets. High tech criminals use botnets to send out spam and phishing emails and launch attacks on web sites. Botnets also search infected computers for information that can be sold on underground auction sites and online markets. From April to June 2010, Microsoft said it cleaned up more than 6.5 million infections, twice as much as in the same period in 2009. The statistics in the report were gathered from the 600 million com-
puters enrolled in Microsoft’s update services or that use its Essentials and Defender security packages. The report can be accessed at http://www.microsoft.com/sir.

WHITE HOUSE FORMS INTERNET, PRIVACY COMMITTEE
The Obama administration formed a subcommittee from federal government agencies to advise them on regulatory and legislative issues for the Internet, especially online privacy. The subcommittee will include members of the Commerce, Justice, Homeland Security and State departments, as well as the Federal Trade and Federal Communications Commissions. The White House will have representatives from its Domestic Policy and National Economic Councils, the U.S. Trade Representative office and the National Security Staff Cybersecurity Directorate. The goal of the subcommittee is to develop consensus on the direction of U.S. laws and regulations on Internet privacy.

NYC BAR ISSUES OPINION ON SOCIAL NETWORKING EVIDENCE
The New York City Bar Association issued Ethics Opinion 2010-2, deciding that a lawyer may not attempt to gain access to a social networking website under false pretenses, either directly or through an agent. The Bar noted that it is easier to deceive a person in the virtual world than in the real world. However, the Bar did conclude that a lawyer may use his or her real name and profile to send a “friend” request to obtain information from an unrepresented person’s social networking website without disclosing the reason for the request. The opinion may be accessed at http://www.abcny.org/Ethics/eth2010.htm.

And see the State Bar’s Opinion...

NY BAR: ATTS CAN SEARCH NET FOR IMPEACHMENT INFO
The New York State Bar Association issued Ethics Opinion No. 843, finding that a lawyer representing a client in pending litigation may access the public pages of another party’s social networking website, such as Facebook or MySpace, for the purpose of obtaining possible impeachment material for use in the litigation. The Bar concluded that as long as the lawyer does not “friend” the other party or direct a third person to do so, accessing the social networking pages of the party would not violate the Rules of Professional Conduct. The Opinion may be accessed at http://www.nysba.org.

STUDY: TEENS TEXT EVERY 10 MINUTES
A study by Nielsen found that, on average, cell phone users aged 13 to 17 years receive or send a text message every 10 minutes. They averaged 3,339 texts a month, up eight percent from the second quarter of 2009. The study also found that teenage girls averaged 4,060 texts, compared to 2,539 for boys. Additionally, 43 percent of respondents said that text messaging was their main use for cell phones because of its ease of use and fast transmission. The study also found that more teens are using Internet applications, picture messaging, gaming and email. The average data consumed by teens rose to 62 megabytes in the second quarter compared to 14 megabytes in the second quarter of 2009. A blog post about the study can be accessed at http://blog.nielsen.com/nielsenwire/online_mobile/u-s-teen-mobile-report-calling-yesterday-texting-today-usingapps- _tomorrow/.

REPORT: WEB ATTACKS BECOMING MORE SOPHISTICATED
A security research report shows that cyber-criminals are developing more sophisticated attacks
on computer networks. The report highlighted the following key security risks: the increased consumerization of enterprise computing, the prolonged and persistent targeting of web applications, the increased organization and sophistication of attackers and the continuing presence of legacy threats. According to the report, the problem is that many companies have not responded to this change in tactics. While organizations are quick to patch vulnerabilities in Microsoft Windows OS, they are slow to patch vulnerabilities in third party software, such as Adobe Reader. In fact, research by Qualys shows that 50 percent of Windows machines applied patches within 15 days on average, but it takes 60 days to implement an Adobe Reader patch. The report may be accessed at http://www.networkcomputing.com/wan-security/web-attacks-get-moresophisticated_-says-report.php.

**REPORT: ANDROID APPS SHARE SENSITIVE DATA**

A collaborative study by Duke University, Penn State and Intel Labs found that 15 of 30 popular Android applications sent users’ geographic location to remote advertisement servers – even though users may have only granted the app permission to access that data for the sake of unlocking location-based features. Further, the researchers found that seven of the 30 applications tested sent unique phone (hardware) identifier and, in some cases, the phone number and SIM card serial number to developers. In total, the researchers reported that two-thirds of the applications in the study showed suspicious handling of sensitive data. Generally speaking, Android app developers are able to collect a good bit of this data because mobile phone operating systems currently provide only coarse-grained controls for regulating whether an application can access private information, but little insight into how that private information will be used. The report can be accessed at http://www.appanalysis.org.

**FLORIDA TO JURIES: NO TWEETING, BLOGGING, RESEARCH**

The Florida Supreme Court adopted new jury instructions: “During deliberations, jurors may communicate about the case only with one another and only when all jurors are present in the jury room. You are not to communicate with any person outside the jury about this case. Until you have reached a verdict, you may not talk about this case in person or through the telephone, writing or electronic communication, such as a blog, Twitter, email, text message or any other means. Do not contact anyone to assist you during deliberations. These communications rules apply until I discharge you at the end of the case. If you become aware of any violation of these instructions or any other instruction I have given in this case, you must tell me by giving a note to the bailiff. In reaching your decision, do not do any research on your own or as a group. Do not use dictionaries, the Internet or any other reference materials. Do not investigate the case or conduct any experiments. Do not visit or view the scene of any event involved in this case or look at maps or pictures on the Internet. If you happen to pass the scene, do not stop or investigate. Jurors must not have discussions of any sort with friends or family members about the case or the people and places involved. So, do not let even the closest family members make comments to you or ask questions about the trial. In this age of electronic communication, I want to stress again that just as you must not talk about the case face-to-face, you must not talk about this case by using an electronic device. You must not use phones, computer or other electronic devices to communicate. Do not send or accept any messages related to this case or your jury service. Do not discuss this case or ask for advice by any means at all, including posting information on an Internet website, chat room or blog.
AG OPINION: TEXAS BAR CAN WITHHOLD EMAIL ADDRESSES

According to an opinion by the Office of the Texas Attorney General, the State Bar does not have to release most attorneys’ email addresses in response to Public Information Act requests. The opinion said that to the extent that the information at issue constitutes membership records that the State Bar maintains for the state supreme court, it is not subject to the Act but is governed by Rule 12 of the Rules of Judicial Administration. As noted in the opinion, Texas Government Code §552.1176 requires the Bar to withhold the email addresses of all lawyers who have notified the Bar they want to restrict access to their information. The opinion further noted that §552.137 of the Government Code provides, with some exceptions, that an email address of a member of the public that is provided for the purpose of communicating electronically with a governmental body is confidential and not subject to disclosure under that chapter. The opinion requires the Bar, under Government Code §552.137, to withhold from disclosure any remaining email addresses – any not covered by Rule 12 or §552.1176 – except those that are government email addresses of government lawyers. Government lawyers can request to keep confidential their home addresses and home email.

IBM SURVEY: SOCIAL, MOBILE, CLOUD ARE HIGH RISK

IT executives rate social networking the riskiest activity facing companies today, according to a survey sponsored by IBM and conducted by The Economist Intelligence Unit. Specifically, of five key technology categories measured, 64 percent of respondents rated social networking tools an extreme risk. Mobile platforms and cloud computing were not far behind with 54 and 43 percent of those, respectively, reporting the technology to be extremely risky. Even 44 percent of those surveyed said that private clouds were much riskier than traditional IT services. Much of the cause for concern has to do with the accessibility, use and control of data, especially regarding social networking and the danger of having access to confidential, proprietary information. According to the study, many organizations have not established processes and methods to integrate this new technology into their infrastructure and workflow. Yet, only 26 percent of survey respondents indicated that virtualization posed significant threat to their organizations. Likewise, Service-Oriented Architecture (SOA) was a concern for only 25 percent. The survey may be accessed at http://www.935.ibm.com/services/us/gbs/thoughtleadership/ibv-global-it-risk-study.html.

STUDY: ID THEFT REPORTED BY ONE-THIRD OF HEALTH PROVIDERS

A study conducted by Healthcare Information and Management Systems Society revealed that 33 percent of respondents (composed of IT and security professionals at hospitals and medical practices) said that their organizations had at least one known case of medical identity theft and some cases may never be reported. Additionally, the report highlighted that only 17 percent of those individuals working for medical providers would likely report an instance of medical id theft, compared to 38 percent of those working in a hospital. The report also noted that 75 percent of all respondents performed a risk assessment at their organization, similar to last year’s findings. However, this year’s survey included a greater representation of medical practices, where 33 percent reported that they do not conduct a risk analysis, compared to only 14 percent who work at hospitals. The report also noted that hospital workers were more likely to report they had a chief security officer. In fact, more than 15 percent of those working in a medical practice indicated that their organization handled security exclusively through external sources. Additionally, about 85 percent of respondents said that their organization shares patient data in an electronic format, and 83 percent of
hospital respondents said they would likely share more data in the future, compared to 77 percent of their medical practice counterparts. A link to the report may be accessed at http://ahier.blogspot.com/2009/11/new-himss-report-healthcare.html.

**FCC PROPOSES FREEING UP AIR-WAVES FOR WIRELESS**

The Federal Communications Commission (FCC) voted unanimously to seek public comment on proposals that include the use of some broadcast television airwaves for wireless devices. The proposals rely on broadcasters such as CBS Corp. and owners of affiliates like Sinclair Broadcast Group and LIN TV Corp. to voluntarily give up spectrum to better enable consumers to download data on smart phones and other wireless devices. The Obama administration has endorsed making 500 megahertz of spectrum available for wireless use. The National Association of Broadcasters said it did not oppose “truly voluntary” incentive auctions, but has taken issue with spectrum fees in the FCC’s national broadband plan that it believes could force broadcasters to surrender their licenses and could threaten the transmission of free local television.

**FTC BACKS PLAN FOR ONLINE PRIVACY**

The Federal Trade Commission (FTC) advocated a plan that would let consumers choose whether they want their Internet browsing and buying habits monitored. Finding that online companies have failed to protect the privacy of Internet users, the FTC recommended a broad framework for commercial use of web consumer data, including a simple and universal “do not track” mechanism that would give consumers the type of control offered by the “do not call” registry. It hopes to adopt an approach it calls “privacy by design,” where companies are required to build protections into their business practices. Many of the practices the FTC is trying to tackle involve third parties that use technology to surreptitiously follow a consumer around the web, collecting data and then selling it, usually without the consumer’s knowledge. The FTC recommends that companies adopt simpler, more transparent and streamlined ways of presenting users with their options rather than the “long, incomprehensible privacy policies that consumers typically do not read, let alone understand.” The report also recommends that data brokers give consumers “reasonable access” to any data they have collected.

**ICANN DELAYS TLD EXPANSION**

The Internet Corporation for Assigned Names and Numbers (ICANN) postponed approval of a mechanism to let groups apply for and manage new Internet domain extensions called generic Top Level Domains (gTLDs), such as the existing .com and .net. ICANN wants to give its Governmental Advisory Committee (GAC) a chance to weigh in on key issues such as trademark protection, malicious conduct, root-zone scaling, economic impact, geographic names and morality-based objections. There are currently 21 gTLDs, but if and when the Applicant Guidebook is finalized and approved, interested groups will be able to propose new extensions and apply for permission to manage them. There are also more than 270 country-based TLDs. The program under consideration is expected to significantly increase the number of gTLDs.

**IN THE COURTS**

**SATELLITE-BASED MONITORING: EX POST FACTO**

State v. Bowditch, 2010 N.C. LEXIS 741 (October 8, 2010). The North Carolina Supreme Court ruled that requiring sex offenders to participate in a satellite-based monitoring (SBM) program, even though their crimes predated the enactment of the SBM statute, does not violate the constitutional prohibitions against ex post facto laws. Kenney Bowditch, whose crimes were committed before
2006 when the SBM statute became law, persuaded the trial court that SBM is punitive, and thus an unconstitutional ex post facto punishment as applied to him. The State appealed, and the state supreme court granted the State’s petition for discretionary review. While acknowledging that SBM has an impact on offenders’ lives, the Supreme Court concluded it was less harsh than restraints such as occupational debarment, license revocation and involuntary commitment, all of which have been deemed nonpunitive by the U.S. Supreme Court. Further, the court found that the SBM requirement of 90-day visits by Department of Corrections officials was not an unnecessary burden on offenders’ Fourth Amendment rights because as convicted felons, they have a diminished expectation of privacy. The Supreme Court reversed the trial court’s decision.

Ed. Note: Joseph Finarelli, Assistant Attorney General in the Office of the North Carolina Attorney General, argued the case for the State.

SEX OFFENDER REGISTRATION: INTERNET IDENTIFIERS
Doe v Shurtleff, 2010 U.S. App. LEXIS 21988 (10th Cir. October 26, 2010). The 10th Circuit Court of Appeals ruled that the law requiring convicted sex offenders to register their online identities did not violate the First and Fourth Amendments. John Doe, a registered sex offender, appealed a decision by the U.S. District Court for the District of Utah enforcing Utah Code Ann. § 77-27-21.5, requiring all sex offenders living in the state to register their Internet identifiers and corresponding websites. Doe first argued that the required disclosure of Internet identifiers chills his First Amendment right to anonymous speech, but the 10th Circuit found that the law had sufficient safeguards to protect Doe’s information from public disclosure. Doe also argued that the statute violates his Fourth Amendment right to be free from unreasonable searches and seizures, but the court rejected that argument, noting its previous finding in U.S. v. Perrine, 518 F.3d 1196 (10th Cir. 2008) that a defendant had no reasonable expectation of privacy in information he voluntarily gave to third party Internet providers. The court upheld the district court ruling.

Ed. Note: Assistant Attorneys General Nancy Kemp and Sharel Reber of the Office of the Attorney General of Utah represented the State.

STORED COMMUNICATIONS ACT: THIRD PARTY SUBPOENAS
Chasten v. Franklin, 2010 U.S. Dist. LEXIS 113284 (N.D. Cal. October 14, 2010). The U.S. District Court for the Northern District of California quashed a subpoena sent or received from the defendant’s email account because it violated the Stored Communications Act (SCA). Janice Chasten sued Eric Franklin and other corrections officers at the prison where her inmate son was killed. She learned from a deposition that one of the defendants had a Yahoo email account, and she sent a subpoena to Yahoo seeking all of the emails sent or received from that account for a period of more than two years. The defendant moved to quash the subpoena, arguing that the subpoena violated his rights under the SCA. As the court noted, the SCA, subject to specific exceptions, prohibits electronic communications providers from knowingly divulging their customers’ electronic communications or the records relating to their customers. The court found that no such exception applied in this case.

SEARCH WARRANT: PARTICULARITY
U.S. v. Rosa, 2010 U.S. App. LEXIS 22099 (2nd Cir. October 27, 2010). The Second Circuit Court of Appeals found that the search warrant was invalid, but it still affirmed the lower court’s refusal to exclude the resulting evidence. Police suspected Efrain Rosa of molesting children and obtained a search warrant for his apartment. Although the materials supporting the warrant specified the particular items sought and the offenses of which Rosa was
suspected, the warrant itself did not contain that information and did not incorporate the supporting materials. Rosa was charged in the U.S. District Court for the Northern District of New York with three counts of producing child pornography based on the materials recovered from the search. Rosa moved to suppress the evidence obtained from his apartment, arguing that the police violated the Fourth Amendment by executing an overbroad and defective search warrant. The district court denied the motion and sentenced Rosa to 120 years’ imprisonment, and he appealed. The 2nd Circuit agreed that the search warrant lacked the requisite specificity to allow for a tailored search of Rosa’s electronic media. It found that the warrant directed the police to seize and search certain electronic devices with no guidance as to the type of evidence sought. The court said that the unincorporated supporting documents could not cure the defective warrant. However, the court found that there was no evidence that the police relied on the defective warrant in executing the search, so therefore there was no requisite deliberateness to justify suppression.

FOURTH AMENDMENT: GOOD FAITH EXCEPTION

U.S. v. Koch, 2010 U.S. App. LEXIS 23629 (8th Cir. November 17, 2010). The Eighth Circuit of Appeals held that agents investigating illegal gambling were acting in good faith when they opened defendant’s flash drive and found child pornography. State agents investigating illegal gambling seized Jonathan Koch’s computer equipment pursuant to a search warrant. Although the agents planned to return Koch’s flash drive to him if it did not contain evidence of illegal gambling, they opened the drive and found it contained images of what appeared to be child pornography. The agents closed the drive and got a new search warrant, which led them to discovery of child pornography on both the flash drive and the computer. At trial in the U.S. District Court for the Southern District of Iowa, Koch argued that the evidence violated his Fourth Amendment rights, but the court denied the objection. Koch was convicted of possession of child pornography and sentenced to 78 months imprisonment and five years of supervised release. Koch appealed, but the appeals court found that the good faith exception to the Fourth Amendment exclusionary rule applied, because the agents were acting in good faith when they opened the drive and unexpectedly discovered child pornography. Evidence that the pornographic images were stored in folders that had to have been created by Koch was sufficient to show that Koch “knowingly” possessed the images.

CHILD PORNOGRAPHY DISTRIBUTION: USE OF P2P NETWORKS

State of New Jersey v. Lyons, 2010 N.J. Super. LEXIS 227 (November 30, 2010). The Superior Court of New Jersey, Appellate Division, found that defendant offered and distributed child pornography by actively placing the images in a shared folder. Richard Lyons was charged with possessing, offering and distributing child pornography through the use of LimeWire, a peer-to-peer file sharing network. The trial court granted Lyons’ motion to dismiss the offering and distributing counts because the State did not present any evidence to the grand jury that Lyons intended to transfer or distribute the images contained in his shared folder, even though he admitted to police that he knew the images were accessible to others. The State appealed, and the appellate court reversed, rejecting Lyons’ argument that his conduct was only “passive.” The court found that he acted with complete awareness that shared folders were available to other LimeWire users and with the practical certainty that his conduct would result in other users’ viewing and downloading his images.

Ed. Note: Frank Ducoat, Deputy Attorney General, Office of the Attorney General of New Jersey, represented the State on both the brief and at oral argument.
ENTICEMENT OF A MINOR: CHAT WITH ADULT GUARDIAN

U.S. v. Douglas, 2010 U.S. App. 24024 (10th Cir. November 23, 2010). The Tenth Circuit Court of Appeals affirmed the lower court decision, finding that defendant committed criminal enticement by communicating with the adult guardian of a minor. Following a jury trial in the U.S. District Court for the District of Vermont, Thomas Douglas IV was convicted of one count of attempting to entice a minor to engage in illegal sexual activity under 18 U.S.C. §2422(b) and one count of knowingly transporting child pornography in interstate commerce under §2252A. Douglas appealed the enticement conviction, arguing that the district court was wrong in concluding that he could commit criminal enticement under the statute by communicating with an adult guardian of a minor. The appeals court disagreed, noting that a conviction under the statute only required a finding of an attempt or intent to entice and not an intent to actually perform the sexual act following the enticement. Douglas was wrong in that his speech had to be made directly to a minor in order for enticement to occur. The statute criminalizes obtaining or attempting to obtain a minor’s assent to illegal sexual activity, and that assent could be obtained through a minor’s adult guardian.

NEW RESOURCES

“Expanding Services to Reach Victims of Identity Theft and Financial Fraud”

This e-publication offers practical tools to prepare victim service providers to help victims of identity theft and financial fraud. Launched during National Cyber Security Month, it includes information about developing case protocols, training staff and staging campaigns. It also provides self-help materials to enable victims to become better self-advocates. It can be accessed at http://www.ovc.gov/pubs/ID_theft/welcome.html.

Children's Exposure to Violence

This issue of “OJJDP News @ a Glance” features an article about DOJ’s Defending Childhood Initiative. It also reports on a meeting of the Coordinating Council on Juvenile Justice and Delinquency Prevention, arts programs for at-risk youth and the SMART Office, which supports efforts to register and monitor sex offenders. It can be accessed at http://www.ncjrs.gov/html/OJJDPnews_at_glance/232007/index.htm.

Justice Resource Update

This issue of “Justice Resource Update” features an article on grant awards made in FY 2010 and forecasts for 2011. Other articles discuss child exploitation and children exposed to violence., South Dakota’s implementation of the Sex Offender Registration and Notification Act and a criminal justice technology needs assessment. It may be accessed at http://www.ncjrs.gov/OJPNeter/newsletter/october2010/justinfo.htm.
WHAT IS THE ROLE OF THE ATTORNEY GENERAL AS A CHILD ADVOCATE IN THE WORLD OF CYBER LAWS?

Lead article continued from page 4...

The Attorney General conducts state-wide investigations, forensic exams and prosecution of online crimes against children

As an advocate for child victims, the Attorney General is particularly interested in prosecuting cases through the Cyber Crime Unit, which has grown exponentially in the number and types of crimes investigated and prosecuted throughout the state. This past year, the unit opened over 100 new cases which were identified through complaints from the general public, referrals from state and federal law enforcement agencies, technical assistance referrals for forensic analysis of electronic media from other law enforcement agencies statewide, Cyber-tips from the National Center for Missing and Exploited Children (NCMEC), and through our own investigative tools. With the introduction of the Wyoming Tool Kit in December of 2008, investigations with child victims became proactive. In FY’08, ICAC investigators made 33 new ICAC cases involving a child. Since January 2010, a total of 38 arrests have been made by the AG’s unit and state affiliate ICAC agencies.

In FY’09, the ICAC unit made 51 new ICAC cases, and in FY ‘10 the ICAC unit opened 88 new child-related cases. Of AG-initiated cases, six persons were indicted by the cyber crime unit, and five persons were convicted in FY’10. Continuing vigorous investigations statewide during the same period, the unit also provided technical assists in the form of forensic analyses to Mississippi law enforcement agencies – certified forensics examiners performed 103 examinations on 52 separate requests for technical assistance, analyzing the media of 57 computers, 47 cellular devices and 579 optical disks. Images recovered from forensic exams are verified by NCMEC by hash values in comparison to the national database of known victims of child pornography.

Technology changes rapidly, and the forensic examiners must train frequently. Equipment and software must be updated in order to analyze new media. Five years ago, an exam might include a review of a small hard drive and a few floppy discs; now perpetrators are likely to have multiple terabytes of information on new media, requiring more forensics hours and up-to-date software licenses. Not only do these forensic investigators practice in the laboratories, but also, they participate in searches pursuant to warrants. The unit now has three forensic examiners and two ICAC-trained investigators. 2009-2010 AG ICAC convictions include:

- Benjamin Dale Russell pled guilty, Lincoln Co., possession of child pornography; 20 years with five to serve.
- Scott Lowery pled guilty, Rankin Co. online enticement of a child; 20 years with seven to serve.
- George Duke pled guilty, Hinds Co. 2nd Dist., possession of child pornography, 15 to serve.
- Willie Lee Hazlewood-pled guilty, Grenada Co., possession of child pornography; 10 years with four to serve.
- Michael Knight, pled guilty, Clarke Co., possession of child pornography; 30 years with 12 to serve.

Cybertips from the NCMEC are received weekly and are shared with ICAC affiliates. Based on a Cybertip, ICAC affiliate U.S. Attorney’s Office, S.D., Mississippi, prosecuted Robert Morris of Copiah County, and Morris pled to possession, production, receipt and distribution of child pornography and was sentenced in August 2010 to serve 35 years. Another Cybertip led to the federal plea of Bryan Niehaus to production and possession of child pornography in
the Southern District of Mississippi; he was sentenced to 35 years. Niehaus was further prosecuted on related state charges of hands-on offenses by ICAC affiliate Warren County District Attorney’s Office, and Niehaus received a state sentence of 80 years consecutive to the federal sentence.11

**The Attorney General is dedicated to a strong cyber crime education and public awareness program**

With the rise in criminal activity on the Internet, the Office of the Attorney General has made it a priority to educate Mississippians about the dangers of cybercrime. The safety of children on the internet is seen as a matter of critical importance, and Attorney General Jim Hood has devoted the resources of his office to insure that Mississippi’s children will be safe from Internet predators. In an effort to reach adults and children with critical messages about Internet safety, members of the ICAC unit have traveled across the state making presentations to civic, school and church groups, as well as training professionals on the dangers inherent in technology.

From July 2009 through June 2010 members of the ICAC Unit gave a total of 71 presentations to communities across the state. Internet safety presentations and trainings were given to 4,133 students; 1,684 professionals working with children; 671 law enforcement officers; and 1,411 members of the general public. That is a total of 7,887 persons across Mississippi who were educated on the critical issues of cyberbullying; sexting and texting; online grooming; child and adolescent vulnerabilities to online victimization; Internet safety (NetSmartz.org) for elementary, ‘tweens and teens; illegal downloads; human trafficking; ICAC investigative protocols; and, the Wyoming Tool Kit.12

Proverbs teaches us that a child who is taught well will not depart from his ways as an adult. To that end, the Attorney General is dedicated to a strong education initiative for teens, stating: “As the father of three young children, my focus is on protecting our children from the unprecedented electronic barrage our children are under from sexting, cyber bullying, reputational damage by lies on social networks, sexual predators, and child pornography. I am concerned about the long-term impact these cyber attacks will have on our children. I don’t want us to look back in 10 years and wonder why we did not better educate parents and children of the dangers brought by cell phones and the Internet.”

Concerning the continued rise in crimes against children, Sgt. Latasha Holmes, Hinds County Sheriff’s Office, Child Protection Unit’s Top Cop in 2010 stated, “I see children raising children. Some young parents do very well, but some leave the children for the grandparents to take over. The grandparents cannot keep up with the kids, and the kids run the streets. Then the cycle continues.”

Our children, particularly teens, who have always known computers, cell phones, the Internet, are extremely adept at multi-tasking online and getting instant results. Teens can “friend” you on Facebook and can text without looking at the keys about what they are doing, often using a vernacular of hieroglyphic acronyms that leaves adults befuddled. Pop culture has crept into teens’ writing.13 Catherine Dixon, Ph.D., educational specialist in the Attorney General’s Office stated, “When children use cell phones or computers to access the Internet, they have little concept of the dangers they may encounter. Sadly, most of their parents understand even less. The Office of the Attorney General has made a statewide effort to provide education to thousands of Mississippians, dedicated staff and resources to this task. Because of this effort, children are being spared from victimization and equipped to make safer choices online.”

Online ads to children intrude and color homework searches and challenge teens to test how well they can interact with the opposite sex. Gaming devices are interactive online so that a child in one state can compete with a child in another state in real time or talk to a predator. Reality and fantasy can become blurred easily.
Camera phones have contributed to the easy exchange of pictures, and kids find it common to send or receive sexually suggestive images and messages, a practice known as sexting; those images can be instantly uploaded to Facebook. Up to forty percent of teens have sent suggestive messages, and about twenty percent say they have posted naked pictures of themselves online. Because teens are giving out too much personal information such as where they go to school, where they live and their phone numbers, they easily can be traced through school webpages, reverse phone lookups, Google maps, loopt or a zaaba search. Phones may give parents and perpetrators the location of the phone; phones with a Facebook “places” application will show where a teen is at the mall or Starbucks if not disconnected. If the teen posts pictures of his location, a perpetrator can upload the pictures online and geolocate the teen.

Rankin County Youth Court Judge Tom Broome stated, “Teens value their cell phones and driver's licenses above all else. Parents should look at their children's cell phones to see what their teens are doing.” Judge Broome also looks at social network postings to get a true picture of what is happening with the child, finding: “It is not unusual for a child to have more than one Facebook page, one to show parents and one for their friends.” Taking risks is natural and part of the growing process, but the prevailing lack of judgment by many teenagers in this new cyber world may lead to regrettable decisions.

Judge Broome continued, “We used to warn our children not to talk to strangers, but now parents have given virtual strangers access to their children via cell phones and social networks.” While the child may think that only his “friend” can see his posts and his most intimate thoughts, when a “friend” shares with another “friend”, privacy may evaporate.

**Agreements have been reached with social networks My Space and Facebook**

Heman Nigam, former MySpace counsel, reported to the NAAG Presidential Initiative on Cyber Crimes in February 2010 that MySpace humanly reviews every one of the 2 million images on its site daily. If the image appears to be child pornography, it is hashed, reported to NCMEC and removed from MySpace. Nigam praised the Attorneys General for the agreement reached with My Space which has led to tighter controls that prevent access to persons under 16 by an adult. An adult user must now know the last name and email address of a new contact under 16 in order to add that child as a “friend”. MySpace regularly scrubs its sites of known, registered sex offenders in an effort to maintain the integrity of its site using Sentinel Safe to compare user names and emails to those of the National Sex Offender Registry.

Likewise, Facebook also has reached a joint agreement with the Attorneys General and has made changes for ready reporting of abuse. Facebook has grown exponentially since the agreement and has since changed its privacy setting policies so that users must make overt changes to their privacy settings to limit access and to prevent Facebook using their information for advertisers. Facebook told the Attorneys General in February 2010 that it had 400 million users and that three billion photos are uploaded daily. Facebook has removed 4,000 registered sex offenders from its site.

**Attorneys General have reached agreements with Topix and Craigslist**

Along with Attorneys General from 16 other states, the Mississippi Attorney General’s office also has reviewed the posting practices of Topix.com, Craigslist and backpage.com for ads of prostitution, child prostitution and human trafficking. Topix has filed a joint statement with the AG’s that it will scour its sites of any child victimization. Attorney General Hood is one of 17 Attorneys General who jointly
called for Craigslist to take down its “adult content” section, which had become a haven for prostitution ads as well as human trafficking and child prostitution. Craigslist complied and has closed its lucrative “adult services”. Craigslist’s drastic action also was influenced by the open letter to the advertising site of two underage girls who described in detail how they answered the ads on Craigslist daily to prostitute themselves.17

Another educational concern to parents and children is the online gaming industry which hosts live interactive chats between players with no age verification of users. Phil Tertian of Activision/Blizzard, the company which created Modern Warfare, Call to Duty, World of Warcraft and Guitar Hero, told Attorneys General and the NAAG Presidential Initiative in February 2010 that there are over 11.5 million subscribers worldwide who game real time. Recognizing the dangers of online gaming, the company has developed parental controls which can be set regarding the amount of time a child plays as well as the level of play.18

The Internet has also exposed our children to other kinds of criminal activity such as illegal downloads and counterfeit goods. In order to protect America’s intellectual property, we must educate our children and parents that it is illegal to download music, movies and software without paying for it and that it is illegal to purchase counterfeit products like designer goods or dangerous items like drugs online.” Attorney General Hood stated.

The Attorney General is joining with the Department of Education in a bullying and cyberbullying initiative

On September 29, 2010, the Attorney General and Tom Burnham, Superintendent of Mississippi Department of Education, are joining together with other partners to train a select group of seventh graders and their teachers by giving them new thinking skills to take back to their fellow students. The theme is “Fear Stops Here: Students Against Bullying”19, and students will focus on the roles of the bully, the victim and bystanders. John Neal, Director of the Hinds County Community Relation and Dropout Prevention, commented, “...[T]his initiative will serve as another means of developing that much needed collaboration between the school, parents and community.”

Purposeful, hurtful postings on a social network page can result in a child’s reluctance to attend school. Under S.B. 2015 (2010), Mississippi schools must implement a bullying policy by December 2010. Observers, victims, volunteers and school officials must report bullying on campus. Cyberbullying may begin off campus, but teachers are finding that the result often is seen at school.20 Cyberbullying typically starts at about 9 years of age and usually ends after 14 years of age—after 14, the contacts progress to cyber harassment.21

A tragic example of online bullying was the victimization of Megan Meier, who formed an online relationship with a person whom she thought to be “Josh Evans” but who in reality was Lori Drew, the jealous mother of one of Megan’s friends. Megan trusted and confided in Josh, and when ‘Josh’ told her the world would be a better place without her, thirteen year –old Megan hanged herself in her closet. Drew’s conviction for violation of MySpace’s Terms of Service agreement under the Computer Fraud and Abuse Act was thrown out, and Congress has not yet passed the proposed legislation, The Megan Meier Cyber Prevention Act, nor does our state have an online impersonation crime.

The Attorney General is working with Internet Service Providers and other Attorneys General to halt the transmission of child pornography on the Internet

“Child pornography and sexual exploitation of children is a worldwide epidemic. Fortunately, we [at TLO] have developed sophisticated tools to catch the predators and have deployed those tools as well as trained law enforcement in 40 countries. Jim Hood and his office were among the first to engage
these new weapons to protect children, and his office is setting the pace for other law enforcement agencies all across America, rescuing children and prosecuting those who prey on them. I don't believe most people understand we are talking about children under eight who are the victims, it's truly shocking what we are seeing,” stated Mike Moore, former Mississippi Attorney General. ISP's and the growth of peer to peer networks and file-sharing software have created a public danger, the gravity of which has increased with the readily available means of electronic transmission of images. To address the problem, action utilizing many avenues of attack is of urgent necessity. Although ECPA mandates that ISP's report child pornography to NCMEC, it provides no consequences for failure to take subsequent action to clean up and remove the illegal images from their services, thus doing little to prevent the further transmission of the reported images. ISP's generally use ECPA's lack of duty provision to rationalize their stance of nonremoval of the illegal images.

Research shows that offenders not only possess, receive and distribute child pornography; but also, they progress to become hands-on offenders. Perpetrators cannot be classified as being from a particular age, sex or ethnic group, and their preferences may be for underage boys or girls. They may collect, trade and make child pornography. Research shows that predators progress from viewing images on a computer to actually physically interacting with a child. Retired F.B.I. Investigator and profiler Ken Lanning tells us that perpetrators compulsively “groom” children with games, toys, attention in order to gain the child’s trust. Once that trusting relationship is established, the perpetrator often manipulates the child, threatening to withhold the love and attention so craved by the child that the child will comply with the perpetrator in order to maintain that so-called “love”. The child is sworn to secrecy, and the child is often reluctant to tell anyone for fear of getting the perpetrator in trouble and losing the relationship. An abused child will assume that he or she is to blame.

The Electronic Communications and Privacy Act of 1986 and amendments.18 USC 2501 et seq., (ECPA) tried to address the growing problem of transmission of child pornography on the Internet and has been amended to require Internet Service Providers to report images of apparent child pornography to the NCMEC which in turn can report hash values and identifying information to the ISPs. ECPA specifies that the reporting process by NCMEC is to be done with the intent to prevent further transmission of the illegal images; however, ECPA does not impose a duty on ISPs to seek out, find, monitor and delete the images. The lack of self-regulation by ISP's and the growth of peer to peer networks and file-sharing software have created a public danger, the gravity of which has increased with the readily available means of electronic transmission of images. To address the problem, action utilizing many avenues of attack is of urgent necessity. Although ECPA mandates that ISPs report child pornography to NCMEC, it provides no consequences for failure to take subsequent action to clean up and remove the illegal images from their services, thus doing little to prevent the further transmission of the reported images. ISP's generally use ECPA's lack of duty provision to rationalize their stance of nonremoval of the illegal images.

Using file detection software, law enforcement now can report with great accuracy that an IP address has possession of files, which hash values are the same as identified images of child pornography at NCMEC, and that the owner of an IP address has shared that identified image peer-to-peer with another person using shareware. Law enforcement can report “actual knowledge” to Internet Service Providers that an IP address has identified images through hash values with more accuracy than DNA testing that the images are of child pornography. To address the problem that ISP's need to step up and participate in the prevention of the further transmission of child pornography, Mississippi’s Attorney General has met with ISPs and with the Department
of Justice’s Child Exploitation Section and will continue to work with them to find a solution to the transmission and removal of child pornography from the Internet.

Additionally, the Attorney General’s office has worked with the Mississippi Legislature to pass initiatives to address various other problems including youth suicide and teens texting while driving.

Conclusion

Each aspect of the joint effort to fight crimes against children as described herein is only a part of the whole which is necessary to investigate, prosecute, educate and prevent. The level of cooperation and communication between and among the various agencies mentioned above is vital to this cause. The continuance of these crimes and the damage they create will cripple our children and darken their futures as adults. Fighting cyber crimes against children is a monumental task calling for new weapons and new strategies. We must continue to fight the good fight and to do what some say cannot be done in this new world of vast technology. We must continue to use every avenue possible and to work together in a concerted effort to seek justice and protection for the children of Mississippi.

1 The U.S. Supreme Court found in New York v. Ferber, 458 U.S. 747 (1982) that states have a compelling interest in protecting children from sexual exploitation and also that each transmission of an image of child pornography is new victimization of the child in the images.

2 Miss. Const. of 1890, Art.6, § 173 and Miss. Code Ann. 1972, as amended, § 7-5-1 et. seq.


5 www.unh.edu


7 In addition to sponsoring the founding of the AG’s cyber crime unit, the University of Mississippi joined with the National Association of Attorneys (NAAG) to train prosecutors nationwide; NCJRL has also received an ICAC grant to train judges in conjunction with the National Judicial College.

8 The Child Protect Act of 2008, S. 1738, required “… the Department of Justice to develop and implement a National Strategy Child Exploitation Prevention and Interdiction, to improve the Internet Crimes Against Children Task Force, to increase resources for regional computer forensic labs, and to make other improvements to increase the ability of law enforcement agencies to investigate and prosecute child predators.” The Child Protect Act gave new monetary life to ICAC’s nationwide with grants requiring 25% of the funding to through to law enforcement affiliates.

9 www.icac.training

10 International Association of Computer Investigation Accessdata Computer Examiners and Forensic Tool Kit Certification.


12 A speaker request form may be found at www.jimhood.ago.state.ms.us.

13 Ibid.

14 www.missingkids.com


17 ABC Evening News Reports, September 6, 2010.

18 www.ersb.org/about/resources (Activision/Blizzard’s parental gaming guide)

19 www.fearstopshere.com


21 Aftab, Parry. www.wiredsafety.org


23 Ibid.

24 Holder, Eric, Attorney General, supra.