

**Issue 31**

**News Highlights in This Issue:**

High Court Upholds Child Pornography Law	2
50 AGs, Facebook Reach Agreement	4
Border Laptop Search is Constitutional	8
Minnesota Enacts Law re Online Tax Sales	11
8 Million Records Breached in 1 <sup>st</sup> Quarter	13
“Online Crimes and Juveniles” – Don’t Miss It	20
Entrapment Defense Fails in E-Wine Sting	9
Senate Enhanced Offender Registration Bill	11
Net Scams Cost Consumers \$ 240 Million	14
High Court Decline Baseball License Case	10
Blocking of Spam by ISP Valid Under CDA	9
Senate OKs National Net Safety Program	11
Competition Drives Market for Stolen Data	15
Electronic Crime Scene Manual Revised	19
NJ: Right of Privacy for ISP=Stored Data	10
House Passes Copyright Crime Bill	12
Most Users Have One Password for All	15
No Special Effort for e-Discovery Producer	10
Triple Times More Trojans Detected	16
Terrorists Increase Internet Use	17

**Table of Contents**

<b><u>Features</u></b>	
High Court Upholds Child Porn Law	2
Senior Counsel Position Available	18
Cybercrime Training Set for August	20
<b><u>AGs Fighting Cyber Crimes</u></b>	4
50 AGs Settle With Facebook	
AG Goddard Settles Online Fraud Suit	
California AG Asks ISPs to Block Porn	
AG Biden Supports Enhanced Penalties	
Florida AG Says Predator Sentenced	
AG Madigan’s Team Checks Offenders	
Kentucky AG Launches Cyber Division	
AG Caldwell’s Unit Arrests Predator	
Maryland AG Speaks on Net Safety	
AG Coakley Hosts Trafficking Training	
Michigan AG: 11 Predators Arrested	
AG Hood Announces Wire Fraud Plea	
New Mexico AG: Predator Guilty	
AG Cuomo Settles With USSearch	
North Carolina AG’s Agent Honored	
AG Edmondson: Online Fraud Charged	
Pennsylvania AG Settles Fraud Case	
AG Lynch’s Initiative: Year of Child	
South Carolina AG: Predator Arrested	
AG Abbott: Pornographer Sentenced	
Vermont AG Settles With Online Co.	
AG McKenna Settles With Spammer	
Wisconsin AG Settles With Net Cos.	
<b><u>In the Courts</u></b>	8
Border Laptop Search Constitutional	
Site Immune From 3 <sup>rd</sup> Party Post Claim	
Sting Proper and Not Entrapment	
ISP Can Block Spammer Under CDA	
NJ Finds Right of Information Privacy	
E-Discovery: No Special Effort Needed	
<b><u>Supreme Courts</u></b>	10
<b><u>Legislation Update</u></b>	11
Minnesota Enacts Net Ticket Law	
Senate Passes Sex Offender Bill	
Judiciary OKs Child Exploitation Bill	
Enhanced Penalties Bill Introduced	
IP Bill Passes House	
Orphan Works Bill Moves Up	
Broadband Practices Bill Introduced	
Computer Fraud Bill Introduced	
2 Internet Safety Bills Introduced	
Cyberbullying Bill Introduced in House	
Spyware Bill Introduced in Senate	
<b><u>News You Can Use</u></b>	13
8 Million Records Breached – 1 <sup>st</sup> Qtr	
Registration Fees Rise for 3 Domains	
E-Scams Cost Consumers \$240 Million	
Competition for Stolen Data Fierce	
Most Use 1 Password for All	
Warning Issued re E-Health Records	
Number of Trojans Triples	
Social Network Sites Best in Crisis	
ISPs Increase User Tracking	
Terrorist Use of Internet Expands	
Piracy Cost Industry \$48 Billion	
US Complains About Tech Tariffs	
New Ways to Steal Data Researched	
<b><u>Tools You Can Use</u></b>	19
Electronic Crime Scene Manual Ready	
How Child Saved From Predator	

The Cyber Crime Newsletter is developed under the Cyber Crime Training Partnership between the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL) at the University of Mississippi School of Law. It is written and edited by Hedda Litwin, Cyber Crime Counsel ([hlitwin@naag.org](mailto:hlitwin@naag.org), 202-326-6022).

This project was supported by Grant No. 2000-DD-VX-0032 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the authors and do not represent the official position of the United States Department of Justice.

The views and opinions of authors expressed in this newsletter do not necessarily state or reflect those of the National Association of Attorneys General (NAAG). This newsletter does not provide any legal advice and is not a substitute for the procurement of such services from a legal professional. NAAG does not endorse or recommend any commercial products, processes, or services. Any use and/or copies of the publication in whole or part must include the customary bibliographic citation. NAAG retains copyright and all other intellectual property rights in the material presented in the publications.

In the interest of making this newsletter as useful a tool as possible for you, we ask that you keep us informed of your efforts. Additionally, we would like to feature articles written by you. Please contact us with information, proposed articles and comments about this newsletter. Thank you.

---

## **SUPREME COURT UPHOLDS CHILD PORNOGRAPHY LAW**

By Dan Schweitzer<sup>1</sup>

In *U.S. v. Williams*, No. 06-694, the Supreme Court, by a 7-2 vote, held that Congress' latest effort to combat child pornography, 18 U.S.C. §2252A(a)(3)(B)(the Act) – which criminalizes in certain specified circumstances the pandering or solicitation of child pornography – was neither overbroad under the First Amendment nor impermissibly vague under the Due Process Clause. Previously, the Court held that two provisions of the Child Pornography Protection Act of 1996 (CPPA) were facially overbroad because they banned the possession and distribution of any material that “is, or appears to be,” child pornography, regardless of whether the material actually contained only youthful-looking adult actors or computer-generated images. *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002). In response to this decision, Congress passed the pandering and solicitation statute at issue which, in relevant part, criminalizes the conduct

of any person who “knowingly...advertises, promotes, presents, distributes or solicits...any material or purported material in a manner that reflects the belief, or is intended to cause another to believe, that the material or purported material is, or contains,” child pornography.

Michael Williams pled guilty in federal district court to this offense and others, but reserved the right to challenge the constitutionality of the pandering conviction. The district court rejected his challenge and sentenced Williams to two concurrent 60-month sentences. The Eleventh Circuit reversed the pandering conviction on appeal, holding that the statute was both overbroad and impermissibly vague.

In an opinion by Justice Scalia, the Court reversed. The Court stated that, under its First Amendment overbreadth doctrine, a statute is facially invalid if it prohibits a substantial amount of protected speech. In determining whether the Act reaches too far, the Court noted that it prohibits offers to provide and requests to obtain child pornography. By contrast, the

CPPA had prohibited the actual underlying material. In addition, the statute's definition of "material or purported material" that may not be pandered or solicited precisely tracks the material that has previously been held to be proscribable – obscene material depicting (actual or virtual) children engaged in sexually explicit conduct, and any other material depicting actual children engaged in sexually explicit conduct. The Court concluded that the statute does not criminalize a substantial amount of protected expressive activity because "offers to provide or requests to obtain child pornography are categorically excluded from the First Amendment." The Court explained that the exclusion's rationale is based not on the less privileged status of commercial speech but on the principle that "offers to give or receive what is unlawful to possess have no social value and thus, like obscenity, enjoy no First Amendment protection." The Court observed that, given that it has "held that the government can ban *both* fraudulent offers *and* offers to provide illegal products," there is "no logic" to holding (as the Eleventh Circuit did) that government may not punish "*fraudulent offers to provide illegal products.*" Commenting on the "endless stream of fanciful hypotheticals," raised by Williams as examples of the Act reaching too far, the Court found that most of them did not state violations of the Act; and the "mere fact that one can conceive of some impermissible applications of a statute is not sufficient to render it susceptible to an overbreadth challenge."

The Court then ruled that the Act was not impermissibly vague under the Due Process Clause. A conviction may violate due process if the statute under

which it is obtained fails to provide a person of ordinary intelligence fair notice of what is prohibited. In the First Amendment context, this problem arises when it is unclear whether a statute regulates a substantial amount of protected speech. Here, the lower court mistakenly believed that the Act's phrases "in a manner that reflects the belief" and "in a manner...that is intended to cause another to believe" were overly vague and standardless, leaving the public with no objective measure of conformance. But, explained the court, "[w]hat renders a statute vague is not the possibility that it will sometimes be difficult to determine whether the incriminating fact it establishes has been proved, but rather the indeterminacy of precisely what that fact is." The Court found that there was no such indeterminacy in the Act because the statute's requirements are clear questions of fact. Just because it may not be difficult in some cases to determine whether these clear requirements have been met does not render the statute vague, particularly given that courts and juries every day evaluate litigants' state of mind and the reasonable import of their statements.

Justice Stevens, with whom Justice Breyer joined, filed a short opinion concurring in the judgment. Justice Souter, joined by Justice Ginsberg, dissented. The dissent contended that the majority's opinion undermines the Court's previous ruling in *Free Speech Coalition* by failing to confront the tension between protecting certain material (fake child pornography) while approving prosecution of the pandering of that same material. According to the dissent, because a transaction in material that does not show images of real children could not

be prosecuted consistently with the First Amendment, that same protection of expression should require a limit to the law's criminalization of pandering such material.

<sup>1</sup>Dan Schweitzer is Supreme Court Counsel at the National Association of Attorneys General.

## AGs FIGHTING CYBER CRIMES

---

### MULTI-STATE

**Fifty Attorneys General** reached an agreement with Facebook.com, the second largest social networking site in the world, under which Facebook agreed to implement changes designed to better protect children on its site from child predators and inappropriate content. The agreement calls for Facebook to participate in a task force designed to facilitate the development of identity and age verification software. The agreement also 1) provides for automatic warning messages to be given to children in danger of furnishing personal information to adults, 2) limits users' ability to change the age information in their profiles, 3) provides for more aggressive removal from the site of content inappropriate for underage viewers, and 4) requires third parties offering services to users to adhere to Facebook's safety and privacy guidelines. The agreement is similar to the recent agreement reached between MySpace and the Attorneys General. Attorneys General of the following jurisdictions participated in the agreement: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin and Wyoming.

### ARIZONA

**Attorney General Terry Goddard** announced that a settlement had been reached with Bill Heard Chevrolet, Inc. for \$225,000, resolving allegations that Bill Heard's advertisements, including those on the Internet, had been deceptive. Specifically, the suit alleged that Bill Heard did not sell its cars consistent with the terms of its advertisements and did not disclose important terms and conditions in its advertisements. The settlement agreement requires Bill Heard to refrain from engaging in future deceptive advertising practices. The funds received from the settlement will be used for consumer fraud education programs and to support Attorney General Goddard's Consumer Protection Division.

### CALIFORNIA

**Attorney General Edmund Brown, Jr.**, together with Governor Arnold Schwarzenegger, wrote a joint letter to the California Internet Service Provider Association, the largest ISP association in the country representing over 100 ISPs, asking state Internet service providers to follow the lead of Verizon Communications, Sprint and Time Warner Cable in removing child pornography from servers and blocking channels that disseminate it.

### DELAWARE

**Attorney General Beau Biden** announced his support for legislation that would enhance penalties for sexual offenses involving minors. The legislation would increase the penalties imposed

against persons convicted of unlawful sexual contact with a minor and for possession of child pornography. The bill would account for all forms of child pornography, including material stored in a camera phone or iPod.

## **FLORIDA**

**Attorney General Bill McCollum** announced that Jordan Eikenberry was sentenced to 25 months in prison for traveling to meet someone he thought was a child for sex. Eikenberry was arrested during an undercover Internet operation after he traveled from his home intending to meet a 14-year-old girl for sex. He was also charged with the graphic behavior he engaged in using a webcam. Eikenberry was prosecuted by Attorney General McCollum's Office of Statewide Prosecution. He pled guilty to using a computer to seduce a child and transmitting materials harmful to a child.

## **ILLINOIS**

**Attorney General Lisa Madigan's** office and the Illinois Sex Offender Registry Team (I-SORT) performed a compliance check to ensure that registered sex offenders were living at their registered addresses. Out of 89 registered offenders checked, 73 were confirmed to be compliant, 10 were determined to be non-compliant, and six were left with notice instructing them to immediately contact I-SORT or enforcement action would commence.

## **KENTUCKY**

**Attorney General Jack Conway** launched a new Cybercrimes Division in his office that will pursue Internet-based crimes, train state law enforcement officials on how to handle evidence taken from computers and cell phones and teach parents to keep children safe from Internet predators. The new division will be part of the Department of Criminal Investigations, formerly the Kentucky Bureau of Investigations. Six investigators from other divisions will be reassigned to the new division, so there will be no additional costs.

## **LOUISIANA**

**Attorney General James Caldwell's** High Technology Crime Unit, along with local law enforcement, arrested Kapil Agnihotri on charges of two counts of computer-aided solicitation of a minor and one count of indecent behavior with a minor. Agnihotri allegedly contacted an investigator whom he believed to be a 14-year-old girl and sent the "girl" text messages of a sexual nature. He also allegedly sent various sexual images and videos of himself over the Internet.

## **MARYLAND**

**Attorney General Doug Gansler** spoke to a fourth grade computer class at a Maryland elementary school about online dangers as part of his campaign to promote Internet safety. Attorney General Gansler's campaign is called Community Leadership in Cyber Knowledge and Safety (CLICKS).

## **MASSACHUSETTS**

**Attorney General Martha Coakley's** office hosted the state's second statewide training on human trafficking. The training was available to local prosecutor's offices, law enforcement officials and employees of social service agencies throughout the state. The program focused on the sexual exploitation of children, and it included training on techniques to bring cases against perpetrators of such crimes and strategies to assist victims.

## **MICHIGAN**

**Attorney General Mike Cox** announced that 11 alleged Internet predators were arrested in Phase II of a joint Internet child predator sting conducted by his office, the Wayne County Sheriff's Department and the Van Buren Township Police Department. Phase I had resulted in 27 arrests of people who had traveled to a decoy location, but Phase II resulted in arrests of individuals who did not travel. The 11 Phase II

arrestees have been charged with soliciting sex from a minor and transmitting sexually explicit materials to a minor.

## MISSISSIPPI

**Attorney General Jim Hood** announced that Ricky Coleman pled guilty to two counts of wire fraud following an investigation which found that Coleman accepted money for a Porsche and a motorcycle, neither of which existed, through an eBay transaction. He was sentenced to a five-year suspended sentence and to five years of supervised probation. Additionally, Coleman has been ordered to pay restitution to the victims of the online fraud and to pay fines to the local victims' compensation fund and to Attorney General Hood's Cyber Crime Center.

## NEW MEXICO

**Attorney General Gary King** announced that Travis Brown pled guilty to sexual exploitation of a child and child solicitation by a computer. Brown could be sentenced for up to four and one half years, and will be required to register as a sex offender. During the investigation, an investigator within Attorney General King's Internet Crimes Against Children unit had posed as a 12-year-old girl, and Brown had asked the "girl" to perform sexual acts and to e-mail photos to him.

## NEW YORK

**Attorney General Andrew Cuomo's** office entered a settlement with Internet company USSearch.com which will prevent the company from continuing its alleged practice of illegally selling the private financial information of thousands of consumers all across the country. Under the agreement, USSearch will also be required to pay \$250,000 in costs and penalties. The complaint alleged that USSearch allowed users to search its databases for personal information otherwise available to the public, such as court records. For an added fee, however, USSearch also provided business consumers access to people's personal information from credit reporting agencies

and financial institutions, and falsely claimed to have a lawful purpose in providing this additional information to the businesses.

## NORTH CAROLINA

**Attorney General Roy Cooper** announced that Special Agent Christopher Haas, a member of Attorney General Cooper's State Bureau of Investigation (SBI), was recognized for his efforts to investigate and help shut down a national child pornography ring. Haas began chatting online with an individual in Florida who allegedly shared a video of himself abusing his six-year-old daughter. The SBI contacted the FBI and the Florida Internet Crimes Against Children Task Force, resulting in the arrest of the Florida offender and other members of the ring. The award to Haas was presented in Washington, DC as part of an annual effort by the National Center for Missing and Exploited Children, the Fraternal Order of Police and the U.S. Department of Justice's Office of Juvenile Justice and Delinquency Prevention to honor officers' work on investigations involving missing and exploited children.

## OKLAHOMA

**Attorney General Drew Edmondson** charged Stephen Lewis with 14 consumer fraud counts. The state alleges that Lewis accepted payment for several items that he placed for sale online on an auction site but never delivered. The allegations further include that Lewis conducted business under multiple business names, including USA Cowboy and Cowboy and Company, and scammed victims into buying numerous items from these business designations.

## PENNSYLVANIA

**Attorney General Tom Corbett** announced that a settlement had been reached with Innovative Media, Inc., a Pennsylvania company that allegedly misrepresented to the consumer various aspects of its "photo blocking" product, which purported to allow users of the product to avoid being identified by traffic cameras used by law enforcement. The

settlement with Innovative Media, which conducts business operations on various websites, including [www.PhantomPlate.com](http://www.PhantomPlate.com), [www.PhotoBlocker.com](http://www.PhotoBlocker.com) and [www.InvisiblePlate.com](http://www.InvisiblePlate.com), requires the company to pay civil penalties, to cease doing business in Pennsylvania and to clearly disclose to consumers that using its products is illegal under Pennsylvania law.

## **RHODE ISLAND**

**Attorney General Patrick Lynch**, unanimously elected in June as the National Association of Attorney's General's (NAAG's) 101<sup>st</sup> President, announced that his presidential initiative, *The Year of the Child*, will focus on enhancing protections for young people, with a concentration on increasing safeguards in relation to technology.

## **SOUTH CAROLINA**

**Attorney General Henry McMaster** announced that Norman Beberg was arrested on two counts of soliciting a minor in an undercover sting conducted by local law enforcement who were members of Attorney General McMaster's Internet Crimes Against Children Task Force. Allegedly, Beberg solicited sex online from an undercover officer whom he believed to be a 13-year-old girl. The case will be prosecuted by Attorney General McMaster's office.

## **TEXAS**

**Attorney General Greg Abbott** announced that Thurman Hearn, who pled guilty to two counts each of child pornography possession and transportation, was sentenced to 188 months in federal prison. Attorney General Abbott's Cyber Crimes Unit began investigating Hearn after a tip from the National Center for Missing and Exploited Children indicating Hearn was uploading child pornography to an online photo album. Hearn denied the Unit's request to search his computer and subsequently dumped two desktop computers, several zip disks, CDs and other peripherals in a cemetery. The Unit recovered Hearn's computer

equipment and performed a forensic examination of the materials, revealing more than 9,000 sexually explicit images and approximately 45 pornographic videos of children. Hearn will also remain on supervised release for life after serving his prison sentence. The case was prosecuted by the U.S. Attorney's Office for the Western District of Texas.

## **VERMONT**

**Attorney General William Sorrell** reached a settlement with Creative Fusion Concept, Inc. ("CFC"), a Canadian company that sold information on governmental grants, and its owner. Under the settlement, CFC must provide a full refund to all purchasers of its service who request one, and must pay \$75,000 to the state, which includes civil penalties and investigation costs. CFC allegedly had offered instructions on the Internet of how to obtain a government grant for approximately \$300 per order, and gave assurances that it could ease the process of becoming eligible for a grant. Attorney General Sorrell had alleged that CFC's program did not directly aid consumers in becoming eligible for government grants, and CFC did not have any data to the contrary. He alleged that the promises made in CFC advertisements were without sufficient factual substantiation and violated the state's Consumer Fraud Act. Under the settlement, CFC is permanently barred from conducting business in Vermont.

## **WASHINGTON**

**Attorney General Rob McKenna** reached a settlement agreement with Ron Cooke, who had allegedly coerced consumers into purchasing software that transformed their computers into "spamming machines." Attorney General McKenna sued Cooke for violation of the state's Computer Spyware Act and Consumer Protection Act. Cooke had allegedly bombarded computers with pop-up advertisements of pornography and sexual enhancement products, followed by a second round of pop-ups claiming that the computer was vulnerable to security attacks. Cooke's scheme then provided a link to a web site that purported to allow the PC user to discontinue the pop-ups and offered

an opportunity to download Messenger Blocker or another like program. Once downloaded, Messenger Blocker caused the computer to send pop-ups to other computers. Under the settlement, Cooke must pay \$5,000 in attorney's fees and costs and \$202 to reimburse nine purchasers, and he must also pay a \$100,000 civil penalty if he fails to fully comply with the settlement agreement. The agreement also restricts the manner in which Cooke can market software in the future.

## WISCONSIN

Attorney General J. B. Van Hollen reached a settlement with two Delaware corporations, iMergent, Inc. and StoresOnline, which had allegedly violated Wisconsin law by using fictitious business names rather than the actual names of the businesses in marketing their services, and failing to sufficiently identify the purpose of their services. Under the settlement, StoresOnline and iMergent must pay \$50,000, which includes forfeitures, civil penalties and investigation costs. The agreement further requires the companies to disclose their identity and the nature of the goods or services offered to the consumer.

# IN THE COURTS

---

## FOURTH AMENDMENT: BORDER SEARCH OF LAPTOP

*U.S. v. Arnold*, 523 F.3d 941 (9<sup>th</sup> Cir. 2008). The 9<sup>th</sup> Circuit Court of Appeals reversed a lower court and held that border customs agents may examine the electronic contents of a passenger's laptop without reasonable suspicion. Michael Arnold was pulled aside for secondary questioning upon arriving in Los Angeles on a flight from the Philippines. Customs agents examined the contents of his laptop and found images of what they believed to be child pornography. A federal grand jury charged Arnold with possessing and transporting child pornography. At trial, Arnold moved to suppress the evidence, arguing that his Fourth Amendment right to unreasonable searches was violated. The U.S. District Court for the Central District of California agreed, finding that the agents did not have a particularized suspicion for the search. On appeal, the 9<sup>th</sup> Circuit reversed, finding that the district court's particularized suspicion

requirement was erroneous. It based its opinion on what it said was Supreme Court precedent holding that the right of the U.S. to protect its border is foremost, although not unlimited. The two recognized exceptions for border searches without reasonable suspicion are searches causing "exceptional damage to property" or that are conducted in a "particularly offensive" manner, neither of which was applicable to the instant case.

## THIRD PARTY-CREATED PROFILE: COMMUNICATIONS DECENCY ACT

*Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288 (D.N.H. 2008). The U.S. District Court for the District of New Hampshire ruled that the Communications Decency Act (CDA) immunizes an adult social networking site from non-intellectual property claims resulting from a profile posted by an anonymous third party. An anonymous plaintiff, "Jane Doe,"

complained to Friendfinder, the operator of several online “adult” dating services, that an anonymous third party had created a profile falsely portraying her and causing her emotional injury and harm to her reputation. Friendfinder removed the profile from the site, but the profile subsequently appeared on other Friendfinder web sites. In addition, Doe alleged that Friendfinder used the profile in promotional materials. She filed suit, charging the Friendfinder network with violating her right of publicity, defamation, intentional affliction of emotional distress and willful or wanton conduct, as well as violations of the New Hampshire Consumer Protection Act. Friendfinder moved to dismiss, arguing that Doe’s claims were barred by the CDA because the contents of the profile were created by a third party. The court granted in part, and denied in part, Friendfinder’s motion. It held that the CDA barred Friendfinder from liability for claims arising out of the posting and reposting of the profile, whether on web sites or in advertisements, even if they knew the profile was false and unauthorized. However, the court noted that Section 230(e) (2) of the CDA provides that immunity does not extend to intellectual property claims, and therefore Doe had stated a valid claim that her right of publicity was violated.

**INTERNET WINE SALES:  
ENTRAPMENT DEFENSE**

*eVineyard Retail Sales-Massachusetts, Inc. v. Alcoholic Beverage Control Comm.*, 2008 WL 681901 (Mass, Sup. Ct. March 18, 2008). eVineyard, a subsidiary of wine.com, was licensed to sell alcoholic beverages online in Massachusetts. Believing that eVineyard was selling to underage

customers, the Office of the Attorney General of Massachusetts set up a sting operation by having a 19-year-old, who claimed to be 22-years-old, order from wine.com. Her order was processed by eVineyard and delivered by Federal Express, which is paid a two dollar premium to verify that recipients are at least 21 years of age. eVineyard was charged with violating state law against sales to minors, and the state Alcoholic Beverages Control (ABC) Commission suspended its license to sell for 10 days and that of FedEx to deliver alcohol for three days. eVineyard appealed, and the trial court reversed the Commission, which then appealed. The state Supreme Court reversed the trial court, finding that the Commission had authority to suspend eVineyard’s license as it violated the law regarding alcohol sales to minors. The court said the sting operation was properly executed and the fact that a government agent solicited the sale was insufficient to show inducement for purposes of an entrapment defense.

**COMMUNICATIONS DECENCY  
ACT: GOOD SAMARITAN  
CLAUSE**

*E360Insight, LLC v. Comcast Corp.*, 2008 WL 1722142 (N.D. Ill. April 10, 2008). Internet marketer and accused e-mail spammer e360Insight (“e360”) sued ISP Comcast, alleging that Comcast harmed them by unjustifiably blocking all or most of e360’s e-mails with filtering software. Comcast moved for judgment on the pleadings, arguing that the Good Samaritan clause of the Communications Decency Act provided them absolute immunity because they had voluntarily filtered the e-mails to restrict access to what they believed was objectionable content. The U.S. District Court for the Northern District of Illinois

agreed, granting the motion and holding that the Good Samaritan Clause allowed the ISP to make a good faith judgment to filter what they deemed objectionable e-mails.

**RIGHT OF INFORMATIONAL  
PRIVACY: INTERNET  
SUBSCRIBERS**

*State v. Reid*, 945 A.2d 26 (N.J. 2008). The New Jersey Supreme Court extended the right of privacy to include information stored by an Internet service provider (ISP) about a subscriber's Internet activity. A disgruntled employee, Shirley Reid, was accused by her employer of accessing the company's shipping database and changing the ship-to address for suppliers. The company gave the IP address of the person making the changes to the police, and they obtained a subpoena requiring Comcast to reveal the account holder of that IP address. Comcast complied, and Reid was charged with computer-related theft. At trial, Reid moved to suppress the information from Comcast, and the trial court granted the motion, finding that Reid had a reasonable expectation of privacy in her subscriber information. The state appealed, and the appeals court

affirmed, as did the New Jersey Supreme Court.

**E-DISCOVERY: PRODUCTION  
FORMATS**

*Autotech Techs, Ltd. P'ship v. Automationdirect.com, Inc.*, 248 F.R.D. 556 (N.D. Ill. 2008). Automationdirect.com ("Automation") moved to compel Autotech to produce an electronic copy of a word processing document which Autotech had already produced in .PDF format on both a compact disc and on paper. Autotech had also provided a "document modification history" containing a chronological list of all changes made since the document was created. Automation argued that the formats provided were unacceptable, claiming that they wanted the document in its "native format," including the metadata. The U.S. District Court for the Northern District of Illinois first noted that Automation had not specified it wanted metadata in its production request. Second, the court looked to the Sedona Conference Working Group Series, noting their statement that there should be a modest legal presumption in most cases that the producing party need not take special efforts to produce or preserve metadata. Accordingly, the court denied the motion.

## SUPREME COURT

---

**BASEBALL STRIKES OUT AT  
SUPREME COURT**

Major League Baseball (MLB) struck out in trying to get the U.S. Supreme Court to resolve a fantasy baseball dispute. The high court

declined to hear the case between MLB and Missouri-based C.B.C. Distribution and Marketing Inc., a fantasy baseball company, over the use of players' names and statistics.

Essentially, MLB.com and the players' union had exerted exclusive control over the use of the names. C.B.C. sought a license from MLB, but was rebuffed, so C.B.C. filed suit. The denial of certiorari leaves in place a ruling by the 8<sup>th</sup> U.S. Circuit Court of Appeals which held that C.B.C. does not require a license to use the players' names in its fantasy leagues. Because of the wide impact of the case, the NFL Players Association, NBA Properties,

WNBA Enterprises, NASCAR and the PGA Tour all filed amicus briefs in the 8<sup>th</sup> Circuit in support of MLB.

To put the case in perspective, approximately four million Americans played fantasy baseball last year, according to the Fantasy Sports Trade Association. It also estimates that about 19.5 million people spend up to \$500 million a year on fantasy sports.

## LEGISLATION UPDATE

---

### Internet Ticket Sales

**ENACTED - MINNESOTA.** Minnesota Governor Tim Pawlenty signed into law S.F. 3139, which criminalizes intentionally using software to interfere with Internet ticket sales, such as by circumventing the security measures of Internet ticket sellers. The newly created offense is a misdemeanor. The bill is effective on August 1, 2008.

### Sex Offender Registration

**PASSED IN U.S. SENATE.** S. 431, a bill sponsored by Senator Charles Schumer (D-NY), passed unanimously in the Senate. The bill would require sex offenders to disclose for inclusion in the national sex offender registry any e-mail address or "other similar Internet identifier" used to communicate on the Internet, with failure to do so subject to a fine and a prison term of up to 10 years. It requires the U.S. Attorney General to make this information available to social networking sites for comparison of online identifiers. Jurisdictions that

maintain information on sex offenders and social networking sites would be required to exempt public disclosure of their e-mail addresses or online identifiers. The bill would impose a fine and prison term of up to 20 years for intentionally misrepresenting age online for the purpose of enticing minors to engage in illicit sexual behavior.

### Online Child Exploitation

**PASSED SENATE.** The Senate unanimously approved S. 1965, sponsored by Senator Ted Stevens (R-AK), a bill which would direct the Federal Trade Commission to institute a nationwide program on Internet safety. It would require elementary and secondary schools with Internet access to educate minors about appropriate online behavior. The bill would also impose a forfeiture penalty on Internet service providers who fail to report online child pornography.

**PASSED SENATE COMMITTEE.**

The Senate Judiciary Committee passed S. 1738, sponsored by Senator Joseph Biden, Jr. (D-DE), which would permit wiretapping in the investigation of crimes against children. It would establish a special counsel for child exploitation within the Office of the Deputy Attorney General, create a national ICAC task force of one task force from each state, and create a national ICAC data network center to support the task force program. The bill would authorize the Attorney General to award grants to state and local ICAC task forces. It would also require the Attorney General to establish additional computer forensic capacity to address the current backlog in investigations involving computer forensics. The companion House bill is H.R. 3845.

**INTRODUCED IN SENATE.** Senator Chuck Grassley (R-IA) introduced S. 3014, which would increase criminal penalties for sexual exploitation of children, child pornography and sex trafficking of minors. The companion bill in the House is H.R. 6167, introduced by Representative Ric Keller (R-FL).

**Intellectual Property**

**PASSED U.S. HOUSE.** H.R. 4279, sponsored by Representative John Conyers, Jr. (D-MI), passed the House by a vote of 410 – 11. The bill would enhance criminal penalties and civil and criminal forfeiture provisions for copyright infringement, as well as provide for restitution to victims. The legislation would also modify computer crime grant programs to include infringement of copyrighted works over the Internet. It would direct the Office of Justice Programs to make grants to state and local law enforcement agencies

to combat intellectual property theft and infringement crimes.

**PASSED SENATE COMMITTEE / HOUSE SUBCOMMITTEE.**

On the Senate side, S. 2913, sponsored by Senator Patrick J. Leahy (D-VT) passed the Judiciary Committee. The bill, which deals with orphan works, would limit the available recovery for the infringement of a copyright of an orphan work upon showing of good faith by the infringer. It would also prohibit any compensation if the infringer is a nonprofit educational institution, museum, library, archives or a public broadcasting entity. The bill also provides a means for obtaining injunctive relief, subject to some limitations. The House companion bill, H.R. 5889, sponsored by Representative Howard L. Berman (D-CA), was approved by the Judiciary Committee's Subcommittee on Courts, the Internet and Intellectual Property.

**Discriminatory Broadband Practices**

**INTRODUCED IN HOUSE.** H.R. 5994, introduced by Representative John Conyers, Jr. (D-MI), was referred to the House Judiciary Committee. The bill would require broadband network providers to provide services or interconnect with another provider, and would ban blocking or interfering with another's ability to use the network to access legal content and failing to clearly disclose terms of service.

**Computer Fraud/Identity Theft**

**INTRODUCED IN HOUSE.** H.R. 6060, introduced by Representative Adam Schiff (D-CA), was referred to the House Judiciary Committee. The bill would permit courts to order restitution for identity theft crimes to reflect the

value of the time spent by the victim in attempting to remediate the harm. It would also provide for an enhanced sentence for recidivist offenders who intentionally access a “protected computer” without authorization and cause damage. The bill would expand the punishable conduct under the current computer fraud statute to include conspiring to violate any of the statute’s provisions and it would expand the conduct that falls within the crime of cyber extortion. The bill would add a forfeiture provision to require violators of the statute to forfeit property used in commission of the crime.

### **Internet Safety Education**

**INTRODUCED IN SENATE.** Senator John Kerry (D-MA) introduced S. 3016, a bill that would provide federal funding for i-SAFE to conduct programs related to Internet crime prevention. It would also create a competitive grant program to fund educational programs on preventing Internet crimes. The bill has been referred to the Senate Judiciary Committee.

**INTRODUCED IN SENATE.** Senate Robert Menendez (D-NJ) introduced S.

3074, a bill that would provide grants to law enforcement and school administrators for Internet crime prevention.

### **Cyberbullying**

**INTRODUCED IN HOUSE.** Representative Linda Sanchez (D-CA) introduced H.R. 6123, which would impose criminal penalties for sending a communication by electronic means that is intended to coerce, intimidate, harass or cause emotional distress to another.

### **Spyware**

**INTRODUCED IN SENATE.** Senator Mark Prior (D-AR) introduced S. 1625, a bill which would prohibit a non-authorized user from installing software on a protected computer that takes control of the computer, changes its settings or prevents user efforts to disable or uninstall the software. It also prohibits installation of software that collects personal information about a user without clear disclosure or that causes advertising pop-ups to appear.

## **NEWS YOU CAN USE**

---

### **8 MILLION RECORDS BREACHED IN 1<sup>ST</sup> QUARTER 2008**

At least 8.3 million consumer data records were potentially compromised by data breaches in the first quarter of 2008, according to statistics released by the Identity Theft Resource Center. The center said that

approximately 4.2 million of the breached records were the result of digital intrusions at the Hannaford supermarket chain. Overall, the statistics showed that businesses were responsible for 36 percent of the breaches, followed by schools and universities, 25 percent; government and military, 18 percent; medical/health care, 14 percent; and

banking and financial institutions, seven percent. Only 13 percent of the breaches were found to be the result of hacker intrusions. According to the report, most of the data breaches appear to have resulted from lost or stolen laptops, hard drives or thumb drives, but insider access and inadvertent posting of sensitive data to a web site or through e-mail were also cited. The center tracked 167 data breaches, and in about 40 percent of those, the organizations involved have not disclosed the number of records that might have been compromised or the number of consumers affected.

### **DOMAIN FEES FOR .COM AND .NET RAISED AGAIN**

VeriSign, the registrar for domain names ending in .com and .net, raised the registration fee for the second time since it took control of those domains in 2006. The fee for .com will increase to \$6.86 from \$6.42, and the fee for .net will increase to \$4.23 from \$3.85, and are expected to be effective on October 1. VeriSign justified the increase by the continuing increase in traffic volume as a result of consumer-driven services, the growing number of web-connected wireless devices and the proliferation of technologies and services using the Domain Name System (DNS). The company claims it processes more than 33 billion DNS inquiries per day under normal circumstances. In addition, VeriSign is deploying new security upgrades and monitoring tools to prevent cyber attacks. It plans to increase the capacity of its global Internet infrastructure by ten times its current level by 2010, as well as increase its daily DNS query capacity to more than four trillion from 400 billion currently.

And see...

### **FEES FOR .ORG TO INCREASE 10 PERCENT**

The Public Interest Registry, which operates the .org domain name, announced that fees for registering a .org domain will increase 10 percent on November 9. The raise was announced in a letter to the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet's key oversight agency, and does not need ICANN's approval. The per-name fee is what the Registry collects annually from registrars that sell domain names on their behalf, and is generally incorporated into the prices paid to register names. The fees apply to new registrations, transfers and renewals. The increase brings the annual fee to \$6.75, up from \$6.15. The .org domain is the world's sixth most popular suffix, with almost seven million names registered. Although it was originally intended for non-profit organizations, it is now open to anyone.

### **INTERNET SCAMS COST CONSUMERS \$240 MILLION**

Consumers lost approximately \$240 million in Internet scams last year, an increase of \$40 million over 2005, according to a report released by the FBI and the National White Collar Crime Center. Demographically, the report noted that men lost more than women at an average loss of \$765 compared with an average of \$552 for women. Additionally, the amounts lost increased with age, with victims in their twenties averaging \$385 per loss compared with an average of \$760 per scam for people over 60 years of age. The most common crime reported was Internet auction fraud in which sellers did not deliver the

merchandise bid and won. The second most common crime was failure to deliver goods purchased online, followed by confidence fraud, in which scammers convince consumers to rely on them, resulting in a financial loss. Approximately one-half of the losses involved amounts less than \$1,000, and one-third involved amounts between \$1,000 and \$5,000.

### **REPORT: COMPETITION DRIVES MARKET FOR STOLEN DATA**

Strong competition among identity thieves has driven the prices for stolen data sharply down, with credit card numbers selling for as low as 40 cents each and access to a bank account priced at \$10, according to the latest bi-annual report from security firm Symantec. The data is usually sold through instant messaging groups or web forums that exist only for a few days or hours, according to the report. Symantec researchers said that web site-specific vulnerabilities are also desirable for attackers because few are fixed quickly. Of 11,253 “cross-site scripting” vulnerabilities found on specific sites during the second half of 2007, only 473 were actually patched. Symantec detected 711,912 new threats last year, which was 468 percent more than in 2005 and accounts for almost two-thirds of all 1,122,311 threats Symantec has catalogued since 2002. The survey was based on malicious code gathered from more than 120 million computers running Symantec anti-virus software and two million decoy e-mail accounts that collect spam.

### **SURVEY: MOST PEOPLE USE ONLY ONE PASSWORD**

Almost one-half of the Internet users queried use just one password for all of their online accounts, according to a survey of Internet users in the United Kingdom and the U.S. by the Accenture consultancy. Company researchers said the problem with repeating passwords is that a hacker who successfully breaks into one account can easily get into the others. Another finding was that 70 percent of respondents in the United Kingdom said they did not write down their passwords, compared to 49 percent in the U.S. Only seven percent of respondents said they change their password often, use password management software or use a fingerprint reader to access their computers and accounts. The survey respondents were made up of people who used a computer at home, had high-speed Internet access and who go online at least twice a week for something other than e-mail. Respondents were selected at random, with a mean age of 46, and were questioned over the telephone.

### **RESEARCHERS ISSUE WARNINGS ABOUT E-HEALTH RECORDS**

In a recent article in the New England Journal of Medicine, Drs. Kenneth Mandl and Isaac Kohane warn that the entry of big companies into the field of storage of personal health records could raise new challenges to the privacy of patient records. The article focuses on the recent offering of web-based personal health records by both Microsoft and Google, under which the patient decides with whom to share the information and under what terms. The

authors note that neither company is bound by the privacy restrictions of the Health Insurance Portability and Accountability Act (HIPAA), the primary law that regulates personal data handling and patient privacy. They fear that unregulated web systems could open the door to marketing and false advertising, and they see a need for safeguards, including extending HIPAA to online patient records hosts. Drs. Mandl and Kohane are physicians and researchers at Children's Hospital Boston, the primary pediatric teaching hospital of the Harvard Medical School. The full article may be accessed at <http://content.nejm.org/cgi/content/short/358/16/1732>.

### **MICROSOFT REPORT: THREE TIMES MORE TROJANS DETECTED**

The number of Trojans removed from computers around the world in the second half of 2007 rose by 300 percent over the first half of the year, according to a report by Microsoft. The report attributed the rise to the fact that more computers are fitted with software that detects malicious programs and that criminals are choosing trojans as their "tool of choice." Trojans can log keystrokes to gather passwords, send spam from private computers and harvest e-mail addresses or personal information for criminal purposes. The report found that the most common family of trojans last year was "Win32/Zlob," malicious software that users unwittingly downloaded because its designers tricked them into believing that they needed the software to watch video online. Once installed, it bombarded them with pop-up messages

and bogus flashing warnings that their computer was infected.

### **REPORT: SOCIAL NETWORKING SITES BETTER IN EMERGENCIES**

Social networking sites are more effective than emergency services and the media in dealing with disasters, according to a report published in New Scientist Magazine. The research, led by Lysia Palen, Assistant Professor of Computer Science at the University of Colorado, also found that blogs, maps, photo sites and instant messaging systems were better at providing warnings, help and list of how individuals were affected than traditional sources. The research was based on surveys of the use of social media during the California wildfires last October and the Virginia Tech shootings last April. Within 90 minutes of the first Virginia shootings, a web page accurately describing the events appeared on Wikipedia, and 20 minutes later, Facebook users had set up a group called "I'm OK at VT," which allowed students and staff to reassure the community that they were safe. During the California fires, web users on sites such as instant messaging forum Twitter kept the community informed of their condition, while Google Maps was used to track the progress of the fire and mark areas where schools and businesses had closed.

### **ISPS INCREASE TRACKING OF USER ACTIVITY**

Internet service providers (ISPs) have increased access to users' online activity, from sending e-mail to visiting web sites, according to a report by the

Washington Post. The purpose of this tracking is to sell the information to advertisers, who in turn advertise on the web sites visited by users. The report describes the tracking technology used, called “deep pocket inspection,” that allows the ISP to view any web site visited, in addition to e-mails sent and search terms used. The deep pocket tracking is more sophisticated than previous systems, which were only able to track web sites visited. Most consumers do not know they are being monitored, and tracking firms have declined to reveal the ISPs who have hired them. The full report can be accessed at <http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule>.

### **TERRORISTS INCREASE USE OF INTERNET**

Al Qaeda and other radical groups have increased their use of the Internet to lure and train recruits worldwide, according to a report by the U.S. Senate Homeland Security Committee. The report noted that the groups run production houses and distribution centers that digitally send anti-American messages to thousands of web sites. The report, entitled “Violent Islamic Extremism, the Internet and the Homegrown Terrorist Threat,” is part of the panel’s investigation into Islamic extremism. The report cited recent cases of “home-grown terrorism,” and noted that many such groups have become experts in going online with their message. It concluded that the U.S. must respond with a stepped-up communication outreach effort.

### **SOFTWARE INDUSTRY LOST \$48 BILLION TO PIRACY**

The software industry lost almost \$48 billion in sales last year because of piracy, even as most countries experienced declines in their piracy rates, according to an annual study commissioned by the Business Software Alliance. The report noted that overall losses rose by \$8 billion and worldwide piracy increased by three percentage points to 38 percent. At the same time, piracy rates declined in 67 of the 108 countries included in the report. Countries with the highest piracy rates are Armenia, Bangladesh, Azerbaijan, Moldova and Zimbabwe. The U.S., Luxembourg, New Zealand, Japan and Austria had the lowest rates. Notably, piracy in Russia declined seven percentage points to 73 percent, a 14-point drop over the last five years. The figures are derived by considering analyst expectations of how much software was installed on PCs versus how much software was paid for or “legally acquired.” The difference is then used to calculate a country’s piracy rate, and that rate is multiplied by revenue from legitimate sales to arrive at estimated losses. The report can be accessed at <http://global.bsa.org/idcglobalstudy2007/>

### **U.S. COMPLAINS ABOUT TECHNOLOGY TARIFFS**

The U.S. filed a complaint with the World Trade Organization (WTO) over European tariffs on technology goods, such as computer monitors and printers. According to the Information Technology Industry Council, a trade association, the duties, which are as high as 14 percent, make American

technology goods less competitive. The complaint argues that the duties violate a 1996 WTO agreement that eliminated tariffs on information technology equipment. The European Union has argued that it can charge duties on the goods, which include cable and satellite boxes for using the Internet and printers which can also scan, fax and copy, because they incorporate new technologies. The WTO confirmed it received the complaint, which starts a 60-day consultation period with the European Union. When that elapses, the U.S. could ask a WTO panel to rule on the dispute.

#### **RESEARCHERS FIND NEW WAYS TO STEAL DATA**

Researchers at Saarland University in Germany and the University of California, Santa Barbara, have found innovative technologies designed to steal data. The Santa Barbara report discusses a tool called

Clear Shot, which analyzes a video of a person typing on a computer to guess what was being typed. While the software only gets the word right about 40 percent of the time, it also suggests alternative words, and usually the typed word is one of these words. The Saarland report discusses how researchers trained telescopes on reflective objects, such as teapots and glasses, to capture screen shots of computers. Using a \$500 telescope, the researchers got a clear picture off a teapot from a distance of five meters to read a 12-point font Word document. Using a \$27,500 telescope, they got the same quality from a distance of 30 meters. The Saarbrucken report may be accessed at <http://www.infsec.cs.unisb.de/%7Eunruh/publications/reflections.pdf>. The Santa Barbara report may be accessed at [http://www.cs.ucsb.edu/%7Eemarco/data/papers/ssp08\\_clearshoy.pdf](http://www.cs.ucsb.edu/%7Eemarco/data/papers/ssp08_clearshoy.pdf).

## **OPENING**

---

#### **SENIOR COUNSEL/VISITING PROFESSOR POSITION AVAILABLE**

The National Center for Justice and the Rule of Law, a program at the University of Mississippi School of Law, anticipates an opening for the position of Senior Counsel/Visiting Professor. The Center could fill that opening on either a temporary basis, as a one or two year visitor, or as a permanent position. The position is non-tenure track and is dependent on the Center's ability to obtain continued funding.

The successful candidate will have visiting faculty status at the law school and will teach advanced criminal law and procedure classes. A second focus of the position is to help develop national conferences and to lecture at those conferences. The Center has two initiatives that produce approximately 12 conferences each year.

The Center's *Cyber Crime Initiative* develops educational programs targeting computer-related crime. To implement this

initiative, the Center allies with other national organizations. In partnership with the National Association of Attorneys General (NAAG), the Center has a cyber-crime training program for Attorneys General offices from all 50 states. The Center also develops unique and nationally important projects to further the goals of this initiative. The Center's *Fourth Amendment Initiative* promotes awareness of search and seizure principles through conferences, judicial and prosecution training and support for selected publications. The Center has an annual symposium focused on the Fourth Amendment and sponsors the *James Otis Lectures*, both of which attract noted scholars. The Center associates with the National Judicial College, located in Reno, NV, to provide educational programs for state trial and appellate judges regarding search and seizure principles. Through its partnership with NAAG, the Center offers training about the search and seizure of computers to state Attorney General offices. The Center also has computer search and seizure conferences for trial and appellate judges.

Applicants must have a J.D. degree from an ABA-accredited school and be admitted to a bar. Preferred accomplishments include substantial criminal litigation experience, strong interpersonal skills, a record of academic achievement, advanced writing, oral, and editing skills, teaching experience and interest in and experience in cyber crime and search and seizure.

Informal inquiries may contact Professor Thomas K. Clancy, Director, National Center for Justice and the Rule of Law, University of Mississippi, School of Law, P.O. Box 1848, University, MS 38677-1848. For more information about the Center, please visit our website at [www.NCJRL.org](http://www.NCJRL.org). The University of Mississippi is an EEO/AA/Title VI/Title IX/Section 504/ADA/ADEA employer. All applicants must formally apply online at <https://jobs.olemiss.edu/>. Applicant must submit a cover letter, resume and writing sample. The position will remain open until filled.

## TOOLS YOU CAN USE

---

### **Electronic Crime Scene Investigation: A Guide for First Responders, 2<sup>nd</sup> Edition.**

This updated guide is designed to assist state and local law enforcement who are responsible for preserving an electronic crime scene and for recognizing, collecting and safeguarding digital evidence. Originally written by Technical Working Group for Electronic Crime Scene Investigation, it can be accessed at <http://www.ncjrs.gov/pdffiles1/nij/219941.pdf>.

### **The AMBER Advocate**

The latest issue of the AMBER Advocate includes an article on how a Florida AMBER Alert saved a child from an Internet predator. It can be accessed at [http://www.amberalert.gov/newsroom/pdfs/advocate\\_0804.pdf](http://www.amberalert.gov/newsroom/pdfs/advocate_0804.pdf).

**NAAG, NCJRL TO HOST INTERNET CRIMES AND JUVENILE:  
CUTTING EDGE ISSUES**

The National Association of Attorneys General (NAAG), in partnership with the National Center for Justice and the Rule of Law (NCJRL) at the University of Mississippi School of Law, will host a training conference for prosecutors and civil enforcement attorneys from Attorneys General offices on “Internet Crimes and Juveniles: Cutting Edge Issues,” at the University on August 12-14. Travel expenses for attendees are eligible for reimbursement.

The conference will focus on such issues as cyberbullying; juveniles involved in virtual worlds, such as Second life; Considerations in Charging and Sentencing Juvenile Offenders and Online Self-Exploitation by Juveniles.

Contact Hedda Litwin, Cybercrime Counsel, at 202-326-6022 or [hlitwin@naag.org](mailto:hlitwin@naag.org) to check on availability.