



Issue 20

**News Highlights in This Issue:**

AGs of 28 States Settle With PayPal	3
Warrantless Laptop Searches at Border OK	8
Spyware, Viruses Cost Users Almost \$8 Billion	12
California Law Requires Wi-Fi Warning Labels	16
Cyber Awareness Month Supported by 42 AGs	3
Virginia Anti-Spam Statute Upheld	11
Free Parental Control Software in Beta Test	13
Internet Gambling Bill Signed Into Law	17
No Jurisdiction for One Internet Auction Sale	9
Silicon Valley Picks Wireless Network Provider	14
House Passes Social Networking Site Bill	17
Suit for Inaccessible Web Site Can Proceed	11
Number of Browser Bugs Found Rises Sharply	15
Alleged Risks From Data Breach Too Vague	12
Spam Touting Penny Stocks Affect Market	15
Good Faith Exception Saves Warrant	13
U.S. Senate Ratifies Cybercrime Treaty	18
Late Discovery to Both Sides is Permissible	12
More Brands Now Bring Targeted by Phishers	16
Web Site Postings Found to be Defamatory	12
DHS Report on Cyber Storm Exercise Released	16

**Table of Contents**

Multiplying Resources Against Predators	2
Cyber Crimes Against Children Conference	19

**AGs Fighting Cyber Crimes**

AGs of 28 States Settle With PayPal	3
42 AGs Support Cyber Security Month	
AG King Proposes Sexual Predator Laws	
Arizona AG Says Predator Sentenced	
AG Lockyer Charges ID Theft, Pretexting	
Colorado AG: First Luring Law Arrest	
AG Crist Announces Arrest of Predator	
Illinois AG Gives Computer Grant to PD	
AG Miller Delivers Internet Safety Speech	
Kentucky AG's Agents Seize Internet Drugs	
AG Foti Joins in Undercover Internet Action	
Massachusetts AG: Pornographer Guilty	
AG Cox Charges Offender With ID Theft	
Missouri AG Enjoins Phone Record Scam	
AG Bruning Hosts Internet Safety Meeting	
New Mexico AG: Sex Offender Arrested	
AG Cooper Discusses Sex Offender Laws	
North Dakota AG Forms Net Luring Unit	
AG Corbett Kicks Off Operation Safe Surf	
South Carolina AG: Predator Arrested	
AG Abbott Says Internet Predator Indicted	
Virginia AG Says Pornographer Found Guilty	
AG McKenna Implements Netsmartz Program	

**In the Courts**

Warrantless Border Search of Laptop OK	8
No Privacy Expectation in Company Computer	
Court Split: Jurisdiction on Net Auction Sales	
Jurisdiction in Online Defamation Case Upheld	
Virginia Anti-Spam Law Constitutional;	
Suit Over Web Site Accessibility Can Proceed	
Late Discovery for Both Sides OK	
Risks From Data Breach Not Concrete	
Web Site Postings Found Defamatory	
Good Faith Exception Saves Warrant	

**News You Can Use**

Teens Inundated With Net Pornography	14
Spyware, Viruses Cost Users \$8 Billion	
Search Engines Unite Against Click Fraud	
Spam Pushing Penny Stocks Sways Market	
Net Matching OK for Texas Attorneys	
Parental Control Software in Beta Test	
Broadband Over Power Line Rules Issued	
Consortium to Build Silicon Valley Network	
More Brands Targeted by Phishers	
Cyber Storm Exercise Findings Available	
Redirect Function for .Travel Proposed	
IBM Will Post Patent Filings on Web	
Social Networking Users Change	
Senate Ratified Cybercrime Treaty	

**Legislation Update**

New Wi-Fi Warning Law in California	18
Internet Gambling Bill Signed Into Law	
House Passes Social Networking Bill	

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.

---

## **MULTIPLYING RESOURCES IN THE FIGHT AGAINST CYBER PREDATORS**

**By Sam Thompson<sup>1</sup>**

In the New Mexico Office of the Attorney General, the Internet Crimes Against Children (ICAC) Unit is not alone in its battle against the menace of online predators. Members of the Public Information Office are also dedicated to raising the awareness of both parents and youth to dangers in cyber space.

The Public Information Office has been active in using the media to reach the people of New Mexico. Frequently, reporters are invited to sit with ICAC investigators for live trolling inside Internet chat rooms. Giving reporters one-on-one time takes an investigator's time away from other duties, but there is a positive payoff when powerful stories capture the attention of the public. In New Mexico, an ICAC investigator has conducted a live trolling for one of the late night news shows. Obviously there was much that could not be shown on a live newscast, but the investigator talked about what she was experiencing during the chat session. The live trolling coincided with the networks' sweeps period and was heavily promoted, giving the

public additional exposure to the notion of dangers from cyber predators.

To show the work of the ICAC Unit, a news cameraman followed the Unit as it served search warrants and conducted sting operations over many months. In this way, there was no same-day coverage of search warrants being served. The importance of eliminating same-day coverage is that investigators have the time to determine the presence of child pornography before the potential predator is named by the press.

In August 2005, the Public Information Office began work on an Internet Safety Guide. The intent was to develop a single publication that would teach parents how to protect their children and teach teenagers how to protect themselves from the dangers encountered online. While the text of the guide was developed by the Public Information Office, creating the eye-catching guidebook was assigned to a contractor, Griffin & Associates of Albuquerque, New Mexico. Their graphic designers crafted an amazing 28-page Internet Safety Guide, with one side for parents and the flip side for teens. This guide received the highest award for a government publication from the New Mexico Chapter of the Public Relations Society of America. After printing a run of 85,000 Internet Safety Guides, only 2,000 remain as of this writing. The guides have been

distributed to schools around the state, parent organizations, community centers and even retail outlets. Some schools are integrating the guides into their Life Skills classes. Law enforcement agencies are distributing the guides to the public as well.

In an effort to reach younger Internet users, the Public Information Office also developed a mousepad that lists dangerous online activities and contact information for reporting potential online predators. Mousepads have been provided to schools, libraries and community centers as well as directly to the public by Radio Disney.

The Public Information Office has also taken on the task of making Internet safety presentations to public groups. PowerPoint presentations were developed in several versions, each one targeting the specific age group and length specified by the requestor. Presentations have been made to local parent-teacher organizations, local businesses, church groups and civic organizations. As part of

the Internet safety presentations, they have also prepared a presentation educating audiences about cartoon artists in cyber space.

Most recently, the Public Information Office assisted the ICAC Unit in developing a presentation for New Mexico's Legislative Finance Committee. The presentation was graphic in nature and served as a wake-up call to key legislative leaders about the dangers our youth face online. This presentation also helped assure the ICAC Unit's funding for the future, since federal funding is unlikely to continue indefinitely.

As detailed above, the Public Information Office can provide valuable assistance to the vital work of ICAC units.

<sup>1</sup>Sam Thompson is Communications Director for the Office of the Attorney General of New Mexico.

## AGs FIGHTING CYBER CRIMES

---

### MULTI-STATE

The **Attorneys General of 28 states** settled with PayPal, Inc., an Internet-based payment system through which its members can transfer payment for online purchases or auctions. Consumers had complained that PayPal was unclear about funding sources for purchases, often withdrawing money from a bank account when the consumer had submitted a credit card for payment. In addition, PayPal froze funds in the user's account during pending disputes, and consumers were confused about PayPal's dispute resolution programs and chargeback rights. The settlement requires PayPal to spell out terms and conditions prior to membership; make information more accessible by changing its use of hyperlinks and multi-page documents; provide members with a clear choice as to method of payment; and provide clear access to web pages explaining differences between its

dispute resolution programs and federal law chargeback rights. The settling states are Alabama, Arizona, California, Delaware, Florida, Georgia, Hawaii, Illinois, Indiana, Iowa, Louisiana, Maryland, Minnesota, Mississippi, Nebraska, Nevada, New Jersey, New York, North Carolina, Ohio, Oklahoma, Oregon, South Dakota, Tennessee, Texas, Vermont, Washington and West Virginia.

**Attorneys General of 42 jurisdictions** signed a declaration of support for the goals of National Cyber Security Awareness Month, the third annual awareness campaign sponsored by the National Cyber Security Alliance (NCSA), a non-profit public-private partnership to promote online security awareness. During October, the National Association of Attorneys General (NAAG) and NCSA are encouraging the public to "Make Cyber Security a Habit." The signatory jurisdictions are

Alabama, Alaska, Arizona, California, Colorado, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Mississippi, Missouri, Montana, Nevada, New Hampshire, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, Wisconsin and Wyoming.

## ALABAMA

**Attorney General Troy King** met with law enforcement agencies from northern Alabama to discuss the state's new law on community notification for sex offenders. He also announced the following proposed amendments to the state's sexual predator laws that he would like to see enacted: (1) expand predator-free zones to include such sites as the YMCA and Boys and Girls Clubs; (2) institute the death penalty for serial child rapists, molesters and sodomizers; and (3) allow children to testify through closed circuit television.

## ARIZONA

**Attorney General Terry Goddard** announced that Robert Bixler of New Mexico was sentenced to 17 years in prison after pleading guilty to one count of sexual exploitation of a minor and one count of luring. By statute, he is required to serve the entire 17 years. Bixler communicated with someone he thought was a 13-year-old girl in an Internet chat room, but in fact was a sergeant with the Mariposa County Sheriff's Office (MCSO). Bixler traveled from New Mexico to Mesa, Arizona to meet the "girl," where he was arrested by MCSO officers. The arrest followed a joint investigation with **New Mexico Attorney General Patricia Madrid's** office, which executed a search warrant on Bixler's residence where child pornography was found. Following Bixler's sentence, he will be placed on lifetime probation and will be required to register as a sex offender. The case was prosecuted by Assistant Attorney General Gail Thackeray.

## CALIFORNIA

**Attorney General Bill Lockyer** filed charges against former Hewlett-Packard (HP) Chairwoman Patricia Dunn, ousted HP senior counsel and ethics director Kevin Hunsaker, private investigator Ronald DeLia, records dealer Joseph DePante and Bryan Wagner, who worked for DePante. The charges were filed under a section of the Penal Code that makes it illegal to seek "utility" records under false pretenses. All face felony charges of fraudulently obtaining confidential records, identity theft, accessing computer data without authorization and conspiracy. All four counts carry a maximum prison sentence of three years under current law. Investigators hired by HP allegedly used pretexting (using a ruse or false identity) to obtain the phone records of 24 people. A new law that becomes effective on January 1, 2007 punishes those who use pretexting to obtain or sell phone records with fines of up to \$2,500 or one year in county jail.

## COLORADO

**Attorney General John Suthers** announced the first arrest for Internet Luring of a Child under House Bill 06-1011, which was the cornerstone of his Safe Surfing Initiative launched in 2005. Richard Hobart was arrested by the Douglas County Sheriff's Office for allegedly engaging a law enforcement officer he believed to be a 12-year-old girl in a sexually explicit Internet conversation and then attempting to meet her for sexual purposes. Under the new law, it is a class 5 felony to engage a person under the age of 15 in a sexually explicit online conversation and then attempt to meet that person for any purpose. If the stated purpose of the meeting is sexual in nature, the felony rises to a class 4.

## FLORIDA

**Attorney General Charlie Crist** announced the arrest of Kennison Boyer on 10 counts of possession of child pornography, a third degree felony, and one count of promoting the sexual performance of a child, a second degree felony.

Kennison had placed pornographic videos and images on the Internet, which were discovered by one of Attorney General Crist's Cybercrime Unit investigators during an online undercover investigation. A search warrant was executed on Boyer's residence and his computer was seized, resulting in the discovery of more than 2,000 images and videos of child pornography. If convicted on all charges, Boyer faces up to 65 years in prison. The Bat County Sheriff's Office and the U.S. Air Force Office of Special Investigations assisted in the arrest.

## ILLINOIS

**Attorney General Lisa Madigan** announced the grant of computer hardware, forensic software and training to the Waterloo Police Department provided by a federal grant awarded to the Illinois Internet Crimes Against Children (ICAC) Task Force. Attorney General Madigan joined Waterloo Mayor Terry Kipping in applauding the commitment of Chief Joseph Brauer and Captain Suzanne Sweet of the Department in using the equipment and training to protect children from sexual predators. Illinois ICAC, which is housed in Attorney General Madigan's office, will provide funding for Captain Sweet to attend training on the use of new forensic analysis software. Attorney General Madigan also recognized Detectives Michael Bazzell of the Alton Police Department and David Vucich of the Madison County Sheriff's Department, who will also attend the training.

## IOWA

**Attorney General Tom Miller** delivered an introductory message at "Internet Safety: Information for Teachers, Parents and Communities," a session designed to introduce teachers and administrators to Internet safety issues and prepare them for student-oriented sessions on the same topic. The session is part of Iowa Public Television's educational telecommunications services. Mike Ferjak, an investigator with Attorney General Miller's Area Prosecutions Division and a leader of Iowa's Internet Crimes

Against Children Task Force, conducted the interactive session.

## KENTUCKY

**Attorney General Greg Stumbo's** Bureau of Investigation agents seized more than \$580,000 worth of drugs sold over the Internet, including \$150,000 in anabolic steroids and ingredients to make steroids. The steroids had been ordered by an illegal Internet pharmacy in Florida, and prescriptions were being filled by Advanced Pharmacy Services LLC in Louisville. Agents also seized more than 137,000 illegal Internet narcotics, with a conservative street value of \$430,000.

## LOUISIANA

**Attorney General Charles Foti, Jr.'s** High Technology Crime Unit participated in a multi-agency undercover Internet operation that targeted adults who solicited juveniles for sexual purposes on the Internet. The Louisiana State Police, Bureau of Investigations, Detective Section; the Alexandria and Pinesville Police Departments; the Rapides Parish Sheriff's Office, Children's Advocacy Center and District Attorney's Office; and the U.S. Attorney's Office also participated in the four-day operation. Detectives arrested McArthur Raymo, Adam Gaspard, Harvey Brodnax III, Larry Ray and Daniel Fairbanks, all of whom allegedly arranged a meeting with a juvenile female for sex. They were charged with Computer-Aided Solicitation of a Minor for Sexual Purposes. There are also several ongoing investigations resulting from the operation.

## MASSACHUSETTS

**Attorney General Tom Reilly** announced that Robert Rich pleaded guilty to two counts each of attempt to disseminate child pornography, possession of child pornography and possession with intent to disseminate obscene matter. The case was investigated by State Police assigned to Attorney General Reilly's office and state troopers assigned to the Internet Crimes Against Children (ICAC) Task Force, who discovered that Rich was using a peer-to-peer network to view and attempt to

disseminate images of children engaged in sexual activity. A search warrant was executed at Rich's home, at which time approximately 12 videos of child pornography involving underage boys were discovered on his computer. He was sentenced to two and one-half years in the House of Corrections, to be suspended for five years, at which time he was to be on probation with special conditions. Assistant Attorneys General Denise Barton and Julie Ross prosecuted the case.

## MICHIGAN

**Attorney General Mike Cox** announced that **Bradford Storti**, a convicted child pornographer, was charged with identity theft, forgery and uttering and publishing for trying to steal the identity of John Stapp, a baby who died in 1972, so he could move to Oregon without registering as a sex offender. Storti had requested Stapp's birth certificate from the state vital records office and included copies of a fraudulent Oregon driver's license, two credit cards and a Social Security card, all in Stapp's name. However, a vital records office employee discovered that Stapp had died. Storti was sentenced to three years and 10 months in prison in 1999 after he pleaded guilty to interstate shipment of child pornography by computer. If convicted on the current charges, he could face up to 14 years in prison.

## MISSOURI

**Attorney General Jay Nixon** obtained a permanent injunction against **Completeskipractice.com**, a Utah-based web site, and **Rob Schroader**, its owner, which prohibits the company from obtaining or selling cell phone records of Missourians. That prohibition applies to obtaining the information from a third party, as well as using the name or identity of any employee of a cellular or telephone service provider in order to obtain the phone records. Attorney General Nixon had sued the company for violation of consumer protection laws.

## NEBRASKA

**Attorney General Jon Bruning** hosted a Websafe Internet safety conference attended by approximately 200 law enforcement officers, county prosecutors, victim advocates and education professionals. Presenters included representatives from the Nebraska State Patrol and Attorney General Bruning's office. The keynote speaker was Supervisory Special Agent Zachary Lowe, who oversees the cyber crime and computer intrusion squad in the St. Louis, Missouri division of the FBI. Websafe is financed by settlement funds from a 2005 agreement between Nebraska and Yahoo! Inc. following an investigation by Attorney General Bruning's office which barred the posting of 70,000 user-created chat rooms promoting sexual activity between adults and children.

## NEW MEXICO

**Attorney General Patricia Madrid's** Internet Crimes Against Children (ICAC) Unit performed the initial investigation that led to the arrest in Delaware of **Jeff Campbell**, a suspected sex offender. Campbell, using the screen name "hippee1010," had solicited sex and child pornography from an ICAC agent posing as a 12-year-old girl. The agent contacted a detective in the Virginia Computer Crimes Unit who also began communicating undercover with Campbell. When it appeared that Campbell was not willing to travel to New Mexico or Virginia to meet either "girl," the two agencies forwarded the case to a detective from the Delaware State Police High Technology Crimes Unit. A search warrant was executed on Campbell's residence in Delaware, where abundant child pornography was uncovered on his computer. Campbell was arrested and later confessed to soliciting sex from up to 20 underage children as well as to recording webcam video they had sent him. He is initially charged with seven counts of Child Solicitation by Computer.

## NORTH CAROLINA

**Attorney General Roy Cooper** met with police officers and crime victims in Wilmington to discuss the need to strengthen laws against sex offenders and improve the state sex offender registry. He also spoke about how local law enforcement is using the registry to keep track of predators.

## NORTH DAKOTA

**Attorney General Wayne Stenehjem** announced the formation of the multijurisdictional Internet Luring Unit, which will coordinate statewide efforts to identify, apprehend and prosecute sexual predators. The Unit will be headed by the Bureau of Criminal Investigation (BCI), a member of the Internet Crimes Against Children (ICAC) program, which received a \$50,000 grant from ICAC to purchase specialized equipment for enforcement efforts and computer forensic training. The BCI will conduct undercover operations targeting online predators, as well as assist local agencies with forensic investigations. Two BCI agents will complete specialized forensics training in a few weeks, after which the Unit will be fully operational.

## PENNSYLVANIA

**Attorney General Tom Corbett** appeared live via Internet and satellite to officially kick off Operation Safe Surf, his Internet safety program. The broadcast was viewed in schools across the state with one school in each region serving as an official host site. The presentation included portions of a DVD created for middle and high school students by Attorney General Corbett's office that shows an actual victim's story, a portrait of a predator and online safety tips. Through a special partnership with the state bar association, more than 300 lawyers were trained to serve as advocates of the program. Those lawyers, along with agents from Attorney General Corbett's Child Predator Unit and representatives of the Pennsylvania Coalition Against Rape, will make presentations to school and parent groups. In

addition to the DVD and curriculum materials from the Internet Keep Safe Coalition, Attorney General Corbett's web site features Internet safety resources.

## SOUTH CAROLINA

**Attorney General Henry McMaster** announced the arrest of Patrick Sims by the Charleston Police Department, a partner in Attorney General McMaster's Internet Crimes Against Children (ICAC) Task Force. According to arrest warrants, Sims solicited sex while at work from a person he believed to be a 13-year-old girl but was actually an undercover investigator from the police department's Computer Crimes Unit. Sims is charged with two counts of Criminal Solicitation of a Minor, a felony offense punishable by up to 10 years imprisonment. The South Carolina Public Service Authority assisted investigators with confirmation of Sims' identity.

## TEXAS

**Attorney General Greg Abbott** announced that Calvin Hannah, Jr., an alleged Internet predator who was arrested by Attorney General Abbott's Cyber Crimes Unit, was indicted by a grand jury. Hannah allegedly used an Internet chat room to target and arrange a meeting with a 14-year-old girl for sex, but the "girl" was actually an undercover Unit investigator. Hannah then traveled 480 miles from his home in Oklahoma to Houston for the encounter. In doing so, he traveled further than any suspect since the Unit's inception. Hannah was indicted on one count each of online solicitation of a minor, aggravated sexual performance of a child and attempted sexual assault, all third-degree felonies. He faces two to 10 years in prison and up to a \$10,000 fine on each charge, if convicted. Shenandoah Police Chief John Chancellor and District Attorney Michael McDougal participated in the case.

## VIRGINIA

**Attorney General Bob McDonnell** announced that David Tetterton of Boston was found guilty of 127 counts of possession of child

pornography and 26 felony counts of reproduction of child pornography after he pled guilty to all charges. South Boston police had arrested Tetterton after Wal-Mart employees detected him developing explicit photographs. He was arrested on 26 counts of reproduction of child pornography and 27 counts of possession of child pornography, but a grand jury indicted him on an additional 100 counts of possession of child pornography based on material discovered on his computer. The U.S. Postal Inspection Service and the National Center for Missing and Exploited Children assisted in the analysis of the materials. The case is being prosecuted by Assistant Attorney General Gene Fishel of Attorney General McDonnell's Computer Crimes Unit and Halifax County Commonwealth's Attorney Kim White.

## WASHINGTON

**Attorney General Rob McKenna** announced a new multi-agency partnership with the National Center for Missing and Exploited Children (NCMEC) to implement the Netsmartz program for Internet safety education. Nearly 300 educators and law enforcement officers attended workshops sponsored to learn how to teach Internet safety to students, parents and other teachers and enforcement officers. The workshops were sponsored by Attorney General McKenna's office, the U.S. Attorney's Offices for the Eastern and Western Districts of Washington, the Internet Crimes Against Children Task Force, Educational Service District 101, the FBI, the Department of Homeland Security, NCMEC and Netsmartz. They were partly funded by Attorney General McKenna's office using consumer protection recoveries and restitution for education and by the U.S. Department of Justice's Project Safe Childhood initiative.

# IN THE COURTS

---

## FOURTH AMENDMENT: WARRANTLESS BORDER SEARCH

*U.S. v. Romm*, 2006 U.S. App. LEXIS 18474 (9<sup>th</sup> Cir. July 24, 2006). A unanimous three-judge panel of the 9<sup>th</sup> Circuit Court of Appeals ruled that U.S. customs agents may conduct random warrantless searches of travelers' laptops regardless of reasonable suspicion or probable cause. The ruling came in response to an appeal by Stuart Romm, a business traveler who was denied entry into Canada when border agents at a British Columbia airport discovered he was on probation after being convicted on child pornography charges in Florida. An agent searched Romm's laptop where he found child pornography sites in the Internet history list. Romm was sent back to Seattle-Tacoma airport,

where customs officials used EnCase software to uncover 42 child pornographic images that Romm had viewed but not saved. Romm was charged with receiving and possessing child pornography, and the 42 images obtained in the warrantless search were ruled admissible as evidence. Romm was convicted and sentenced to two concurrent prison terms of 10 and 15 years. He appealed, arguing that the evidence against him was obtained without a warrant in violation of the Fourth Amendment's protection against unreasonable search and seizure. The 9<sup>th</sup> Circuit panel found the search of Romm's laptop without a warrant or probable cause "permissible" under a border search doctrine that finds "searches made at the border ... are reasonable simply by virtue of the fact that they occur at the border." *U.S. v.*

*Flores-Montano*, 541 U.S. 149, 152-53 (2004) (quoting *U.S. v. Ramsey*, 431 U.S. 606, 616 (1977)).

*Ed. note: Only one other circuit has addressed this issue and it reached the same conclusion. See U.S. v. Tucker II*, 305 F.3d 1199 (10<sup>th</sup> Cir. 2002).

#### **FOURTH AMENDMENT: SEARCH OF OFFICE COMPUTER**

*U.S. v. Ziegler*, 2006 WL 2255688 (9<sup>th</sup> Cir. August 8, 2006). The 9<sup>th</sup> Circuit affirmed a lower court decision that an employee had no reasonable expectation of privacy in the contents of a company computer which, according to company policy, was subject to routine monitoring. A computer firewall that monitored employee Internet connections at the Frontline Company showed that employee Jeffrey Ziegler was accessing child pornography sites. Frontline notified the FBI and, at the request of an FBI agent, company representatives entered Ziegler's office at night, made a copy of his computer hard drive and gave it to the agent. A forensic examination of the drive revealed several images of child pornography. Ziegler was indicted for possession of child pornography. Ziegler moved to suppress the computer files obtained without a warrant, but the U.S. District Court for the District of Montana denied the motion, finding that Ziegler had no expectation of privacy in the computer files he accessed. Ziegler subsequently entered into a plea agreement whereby the government agreed to drop the child pornography charges and Ziegler would plead guilty to receipt of obscene material. The agreement was also contingent on Ziegler's ability to appeal the suppression ruling. On appeal, Ziegler

argued that he had a reasonable expectation of privacy in the computer files and thus had standing to challenge the search. The government disagreed, citing the fact that Frontline had notified its employees of its monitoring activities. The 9<sup>th</sup> Circuit agreed with the government, finding that Ziegler could not have reasonably expected his computer files were private. The court also responded to the issue of whether the FBI-directed entry into Ziegler's office was a "search" of the office by finding that the entry was "an operational reality of Ziegler's workplace that diminished his legitimate privacy expectations." Ziegler's conviction was affirmed.

#### **PERSONAL JURISDICTION: ONLINE AUCTION TRANSACTIONS**

*Boschetto v. Hansing*, No. C-06-1390 (N.D. Cal. July 13, 2006). The U.S. District Court for the Northern District of California ruled that a Wisconsin resident's sale of an automobile on eBay to a California resident did not give rise to personal jurisdiction in California. In so doing, the court agreed with several other jurisdictions that a single transaction on an Internet auction site does not constitute the requisite "purposeful availment" with the forum required for personal jurisdiction. Paul Boschetto, a California resident, submitted the winning bid for an automobile offered for sale on eBay by Jeffrey Hansing, a Wisconsin resident. Boschetto subsequently filed suit against Hansing and his dealership in the district court in California, alleging that the car he received was defective and not as advertised. Defendants moved to dismiss for lack of personal jurisdiction. The court concluded that Boschetto had

not satisfied his burden of establishing jurisdiction because the negotiations took place entirely over the Internet and not in California and that there was only one transaction involved. The court also noted the considerable harm to e-commerce if there were a more lax standard for personal jurisdiction. The court added that requiring a buyer who purposely made a purchase from a seller in another state to travel to that state to pursue his claim still comported with due process.

But see...

*Dedvukaj v. Maloney*, 2006 WL 2520347 (E.D. Mich. August 31, 2006). The U.S. District Court for the Eastern District of Michigan held that it can exercise personal jurisdiction over an out-of-state eBay seller accused of breach of contract, fraud and misrepresentation. Maloney, a Michigan resident, won two eBay auctions for original paintings from Dedvukaj, a seller in New York. Although Dedvukaj verified the authenticity of the paintings by phone and e-mail, Dedvukaj never shipped the paintings and offered a refund, but Maloney demanded either the original paintings or their fair market value. Maloney sued, and Dedvukaj moved to dismiss for lack of personal jurisdiction or, alternatively, to transfer venue to a New York court. Dedvukaj argued that because he did not target or specifically market his auctions to Michigan residents, his contacts were too attenuated to support personal jurisdiction. The U.S. District Court for the Eastern District of Michigan found that by communicating with Maloney by phone and e-mail, accepting the winning bid and confirming shipping costs, Dedvukaj transacted business in Michigan, satisfying the requirements of

Michigan's long arm statute. The court denied the motion to dismiss or transfer.

### **LONG ARM STATUTE: ONLINE DEFAMATION**

*Whitney Information Network, Inc. v. Xcentric Ventures, LLC*, (slip. op.) 2006 WL 2243041 (11<sup>th</sup> Cir. August 1, 2006). In an online defamation case, the 11<sup>th</sup> Circuit overturned the lower court, finding that defendants had not successfully rebutted allegations of personal jurisdiction under the Florida long arm statute, Fla. Stat. §48.193. Whitney Information Network sued Xcentric Ventures, owners of Ripoffreport.com and other sites, over negative online postings about Whitney. The U.S. District Court for the Middle District of Florida dismissed the complaint, ruling that Xcentric was immune from defamation liability under the Communications Decency Act, 47 U.S.C. §230, which states that a provider of an interactive computer service shall be treated as the publisher of any information provided by another information content provider. Whitney filed an amended complaint, skirting the §230 problem by alleging that Xcentric played an active role in the defamation by adding derogatory words to the postings. Xcentric moved to dismiss for lack of personal jurisdiction, arguing that Whitney failed to satisfy Florida's long arm statute that provides for jurisdiction over an out-of-state defendant that commits a tortious act within the state. Xcentric submitted affidavits in support of their 230 immunization status. The district court dismissed, holding that the affidavits put the burden back on Whitney to prove exercise of jurisdiction. On appeal, the 11<sup>th</sup> Circuit reversed, holding that Xcentric's affidavits were insufficient to shift the

burden and remanded the case for further proceedings on the exercise of personal jurisdiction.

### **ANTI-SPAM LEGISLATION: CONSTITUTIONALITY**

*Jaynes v. Commonwealth of Virginia*, 2006 WL 2527678 (Va. App. September 8, 2006). The Virginia Court of Appeals affirmed the felony conviction of Jeremy Jaynes on three counts of violating the unsolicited bulk electronic mail provisions of the Virginia Computer Crimes Act (VCAA), Virginia Code § 18:2-152.3:1. At trial, it was shown that Jaynes had used computers in his North Carolina home to send more than 10,000 unsolicited e-mails to AOL subscribers. On appeal, Jaynes first argument was that the trial court lacked subject matter jurisdiction because the e-mails were sent from his North Carolina home, but the court disagreed, noting that the e-mails had to pass through AOL's e-mail servers, which were located in Virginia. Next, Jaynes argued that the VCAA prohibits anonymous speech of a non-commercial nature in violation of the First Amendment, but the court found the VCAA does not proscribe protected speech. Jaynes' third argument was that the VCAA violates the Dormant Commerce Clause because it places an impermissible burden on interstate commerce, but the court stated that the only burden was to present truthful transmission. Lastly, Jaynes argued that the VCAA was unconstitutionally vague in that many words were undefined, but the court found that it gave a person of ordinary intelligence the opportunity to know what conduct was prohibited.

### **INTERNET ACCESSIBILITY: DISABILITY RIGHTS**

*National Federation of the Blind v Target*, No. C 06-01803 (N.D. Cal. September 5, 2006). The U.S. District Court for the Northern District of California ruled that a suit against a retailer for violation of the Americans with Disabilities Act (ADA) because its web site is inaccessible to the blind can proceed. The National Federation of the Blind (NFB) sued Target Corp., alleging that their web site is inaccessible to the blind and therefore violates the ADA, the California Unruh Civil Rights Act and the California Disabled Persons Act. Specifically, the NFB argued that target.com fails to meet minimum standards of web accessibility because (1) it has no compliant alt text, an invisible code that allows detection and vocalization of an image to a blind person; (2) it contains inaccessible image maps and graphics, preventing blind persons from navigating and using all functions; and (3) it requires the use of a mouse to complete a transaction, preventing blind people from making purchases. Target filed a motion to dismiss, arguing that only its physical store locations were subject to the ADA. The district court disagreed and denied, in part, the motion to dismiss, allowing the AFB to proceed, but only with claims that dealt with the sections of the web site where inaccessibility would "impede the full and equal enjoyment of goods and services offered in Target stores." However, the court did note that it might in the future allow broader claims if it were shown that the web site and the stores were components of an integrated merchandising effort.

## **FORENSIC TESTIMONY: ADMISSIBILITY**

*The People v. Rutter*, No. B186072 (Cal. App. 4<sup>th</sup> October 16, 2006). A California appeals court found that the late release to the defendant of a computer expert's report on his examination of a laptop was within the bounds of the state penal code. The State of California charged photographer John Rutter with attempted grand theft, forgery and perjury for threatening actress Cameron Diaz with the release of topless pictures taken of her 11 years ago unless she paid him \$3.5 million. Rutter claimed that Diaz had signed a release, but Diaz claimed that the signature on the release was forged. Police obtained a warrant to search Rutter's apartment, where they seized two computers, an external hard drive and a stack of CD-ROMs containing numerous copies of the release. Five days before trial, the State's expert turned over a 113-page summary of the evidence found on the computers to the State, which turned it over to Rutter the next day. Rutter moved to suppress the expert's testimony because of late disclosure. After Rutter refused a continuance, the trial court denied his motion, saying that he had the same access to the evidence as the State and could have conducted his own testing. The expert testified at trial that the signature was forged, and Rutter was convicted and sentenced to three years and eight months in prison. On appeal, his conviction was affirmed. The appeals court cited Penal Code Sec. 1054.7, which requires that discovery be furnished 30 days before trial, or immediately upon the prosecution becoming aware of the material, whichever is later. The State had immediately turned over the report, and nothing in the record indicated that they

learned of the expert's opinion prior to receiving the report.

*Ed. Note: Deputy Attorney Generals Mary Sanchez and Theresa Patterson of the California Attorney General's Office handled the case for the State.*

## **DATA BREACH: LIABILITY**

*Bell v. Acxiom Corp.*, No. 4:06CV00485 (E.D. Ark. October 3, 2006). The U.S. District Court for the Eastern District of Arkansas found that the alleged increase in risks resulting from a data breach were not sufficiently concrete to satisfy the "case or controversy" pleading standard. Acxiom, a data broker/data miner, suffered a major security breach when a hacker extracted personal data and resold it to marketers. April Bell brought a putative class action suit against Acxiom, alleging increased risk of identity theft and of receiving junk mail. Acxiom moved to dismiss for failure to state a claim upon which relief can be granted. Noting that Bell had not alleged that she actually experienced these increased risks, the court granted Acxiom's motion.

*Ed. Note: See also Key v. DSW, Inc.*, 2006 WL 2794930 (S.D. Ohio September 27, 2006), where the U.S. District Court for the Southern District of Ohio reached a similar result.

## **DEFAMATION: WEB SITE POSTING**

*Benz v. Washington Newspaper Publishing Co.*, 2006 U.S. Dist. LEXIS 71827 (D.D.C. September 29, 2006). The U.S. District Court for the District of Columbia allowed a defamation suit by a CNN producer based on web site postings and e-mails to proceed.

Kathleen Benz and John Bisney were colleagues at CNN and, although Bisney wanted a romantic relationship, Benz did not. In retaliation, Bisney, without Benz' knowledge or permission, obtained access to and read her e-mails, and he also established web sites in her name. Bisney posted Benz' personal information on the sites, and also wrote a "fake" article naming numerous men she had dated which he sent to her. Benz filed for a temporary restraining order, and subsequently both parties entered into a settlement agreement providing that they would not intentionally communicate. Soon thereafter, Bisney posted more articles on the web sites. He also used Benz' name to respond to personal Internet ads seeking sexual relations, and Benz received numerous e-mails and phone calls as a result. In addition, the Washington Examiner newspaper published an article in a gossip column based on the Internet postings and which also implied that Benz used her position as a CNN producer to meet men. Benz filed suit against the parent Washington Newspaper Publishing Co. and Bisney, alleging defamation, invasion of privacy and intentional infliction of emotional distress. The newspaper and Bisney moved to dismiss on the basis that the articles didn't constitute defamation, but the district court disagreed, finding that the articles were capable of defamatory meaning. The motions were denied.

#### **SEARCH AND SEIZURE:** **PROBABLY CAUSE**

*United States v. Flanders*, 10785 (5<sup>th</sup> Cir. October 20, 2006). The 5<sup>th</sup> Circuit affirmed a district court's denial of a motion to suppress pornography because the police warrant was based on the good faith exception. Michael Flanders appealed the district court's denial of his motion to suppress child pornography on his computer. He argued that the search warrant was defective because police did not have probable cause to search his computer. The search warrant was for photos, files and other material containing images of minors engaged in sexual activity. The warrant affidavit stated that Flanders had been accused of child molestation, had described alleged sex acts with children in a chat room and had been known to view adult pornography sites. Although there was no direct evidence that Flanders viewed or possessed child pornography, the warrant affidavit concluded that in officers' experience, men who molest children and view pornography online often download child pornography on their computer. The court held that the officers' reliance on the warrant was objectively reasonable, thus triggering the good-faith exception to the warrant requirement.

# NEWS YOU CAN USE

---

## **STUDY: MORE TEENS BOMBARDED WITH ONLINE PORN**

Children aged 10 to 17 are increasingly being inundated with online pornography, according to a report just released by the University of New Hampshire's Crimes Against Children Research Center. It is based on a survey of 1,500 children last year that was compared with findings from a similar group five years ago. Nine percent of children surveyed reported being "very upset" by seeing pornography, up from six percent in the previous study. The study also found that, despite the rise of social networking sites, about 13 percent said they had received an unwanted request to engage in sexual activity or conversations in 2005, compared with 19 percent five years ago. Of those solicitations, 43 percent were from others under age 18. Researchers also found that children are being increasingly harassed and bullied more, often by their peers. The full report can be accessed at <http://www.unh.edu/ccrc/pdf/CV138.pdf>.

## **SPYWARE, VIRUSES COST USERS ALMOST \$8 BILLION**

Consumers paid \$7.8 billion over two years to repair or replace computers that became infected with viruses and spyware, according to a survey of 2,000 households by Consumer Reports magazine. The magazine found that spam is the biggest computer security problem, but viruses are the most expensive. Spyware infections, while declining slightly in the past six months,

still caused almost one million households to replace their computers. Losses from phishing scams, however, increased five fold from 2005, with people telling the magazine that those scams cost them \$630 million in the past two years, an average loss of \$850 per incident. The survey also found that 20 percent of respondents did not have antivirus software, and that 35 percent did not use spyware-blocking software.

## **SEARCH ENGINES JOIN FORCES AGAINST CLICK FRAUD**

Google Inc., Yahoo Inc. and Microsoft Corp. have teamed up with the Interactive Advertising Bureau, an advertising trade group, to find a better way to identify and measure "click fraud." Two smaller search engines, Ask.com and LookSmart Ltd., as well as the non-profit Media Rating Council, also joined the effort. Currently search engines and their partners collect a commission for every click on short advertising links, typically displayed at the top or side of web pages, even if the click doesn't result in a sale. Commissions range from a few cents to more than \$20 per click. Click fraud results in merchants being billed for useless traffic generated by someone who repeatedly clicks on an advertiser's link with no intention to buy. Recent class actions and industry studies claim that advertisers have been collectively overcharged by more than one billion dollars during the past four years due to click fraud. Google has challenged that claim in a report, "How Fictitious Clicks Occur in Third-Party Click Fraud Audit Reports," which can be accessed at

[www.google.com/adwords/ReportonThird-PartyClickFraudAuditing.pdf](http://www.google.com/adwords/ReportonThird-PartyClickFraudAuditing.pdf)

### **SPAM TOUTING STOCKS CAN AFFECT MARKET**

About 15 percent of spam messages tout penny stocks that spammers hope to convince recipients to buy and thereby raise their price, according to a study recently published on the Social Science Network. Users who respond to the “pump and dump” scam can lose eight percent of their investment, while spammers typically see a return of almost five percent. The study, by Professor Laura Frieder of Purdue University and Professor Jonathan Zittrain of Oxford University’s Internet Institute, analyzed more than 75,000 unsolicited e-mails touting stocks. The researchers then compared the estimated size of an e-mail campaign with trading activity and share prices immediately before and after the first spam message. The research team found that on average a victim loses \$52.50 for every \$1000 invested in such schemes. The draft study may be accessed at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=920553](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=920553).

### **TEXAS BAR: ATTORNEYS CAN JOIN ONLINE MATCHING SERVICE**

The Professional Ethics Committee of the State Bar of Texas determined that Texas lawyers can pay a fee to participate in an online service that matches subscribing lawyers with potential clients, as long as the service exercises no discretion in those matchups. Opinion 573, which reverses a bar decision of one year ago, was issued after a Federal Trade Commission letter advised that such services have the

potential to lower consumer costs for obtaining information about the price and quality of legal services. The bar committee does specify that the service must utilize a wholly automated computerized process to identify matches, must include a disclaimer that the service only lists lawyers who have paid a fee and cannot make any assertions about the quality of the lawyers. Rhode Island, North Carolina, South Carolina and Utah also have formal opinions authorizing attorneys to participate in such services.

### **MICROSOFT PARENTAL CONTROL SOFTWARE TESTED**

Microsoft released a beta version of its Windows Live OneCare Family Safety tool designed to help keep web content that parents deem inappropriate from viewing by their children. The test software updates the earlier preview version made available to 3,000 users in March 2006. Before the final release, Microsoft plans to add “contact management” features that will let parents approve contacts within the WindowsLive Mail and Messenger programs, as well as give them control over who can access their children’s blogs on Microsoft’s MSN Spaces service. The beta version currently is only available in the United States, but Microsoft plans to release it in 34 additional markets in 16 languages.

### **FCC ISSUES MORE BROADBAND OVER POWER LINES RULES**

The Federal Communications Commission (FCC) unanimously adopted an order that reaffirms and builds on its first set of rules on broadband over power lines (BPL) technology. The original guidelines

focused on preventing BPL from causing interference with radio signals such as those used in aviation. The new order denies requests by the amateur radio community, TV broadcasters and the aeronautical industry to exclude or prohibit BPL at certain frequencies because the FCC did not have enough evidence of interference by BPL. The order also reaffirms limits on emissions by BPL equipment, requires certification of BPL equipment and requires BPL providers to enter information about their offerings in a public database at least 30 days before making them available. A summary of the order may be accessed at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-266773A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-266773A1.pdf).

### **TECH CONSORTIUM TO BUILD WIRELESS NETWORK**

Metro Connect, a tech consortium that includes IBM Corp. and Cisco Systems Inc., secured the winning bid on a proposal to provide affordable wireless access to the Internet for 2.4 million residents over about 1,500 square miles of Silicon Valley. The selection was made by the Wireless Silicon Valley Task Force, a group comprised of local government officials and representatives from utility companies, although individual municipalities must still give their approval. The privately owned and operated network would be financed through sponsorships, giving residents free access to basic Wi-Fi service. Additional features, such as Internet-based phone calls or steaming video, would require fees.

### **PHISHERS TARGET MORE BRANDS**

A record 154 brands were exploited by online phishing scams, as compared with 71 brands targeted one year ago, according to a study by the Anti-Phishing Working Group (APWG). The study showed that the number of brands under attack from phishing rose by 20 percent from June 2006 and by 12 percent from the previous record in May 2006. While the top 80 percent of scams were still concentrated on 15 brands, the number of brands targeted in the remaining 20 percent is a sign that phishers are exploiting more than the best-known brands. Phishers also became more focused on targeting financial services, which comprised 93.5 percent of all targets in the study. The report also showed a drop in the number of unique reported phishing campaigns, but an 18 percent higher increase in the number of reported phishing sites. The U.S. was the leading country hosting phishing sites with 29.9 percent, followed by Korea (13.3 percent), China (12 percent), France (5.9 percent) and Australia (4.6 percent). Websense, one of the APWG's more than 1,500 members, conducted the study, which is available on the group's web site at <http://www.antiphishing.org>.

### **DHS RELEASES CYBER STORM REPORT**

The U.S. Department of Homeland Security (DHS) released the Cyber Storm Exercise Report detailing key findings from the Cyber Storm exercise held to examine response, coordination and recovery to a simulated cyber attack campaign. More than 110 public, private and international entities were involved in its planning and

implementation. The report noted that the cyber community was effective in addressing individual threats and attacks, but faced challenges in cross-sector situational awareness. It also found that ongoing information sharing fortified relationships between response partners. It can be accessed at [www.dhs.gov/interweb/assetlibrary/prepare\\_cyberstormreport\\_sep06.pdf](http://www.dhs.gov/interweb/assetlibrary/prepare_cyberstormreport_sep06.pdf).

### **REDIRECT FUNCTION PROPOSED FOR .TRAVEL DOMAIN**

Tralliance Corp., operators of the .travel domain, proposed a new search service that would redirect users who mistype .travel web addresses or seek nonexistent .travel addresses, reviving a debate over the amount of control domain operators should have in directing Internet traffic. Under the proposal, such users would instead get a web page or search box inviting them to register for the name, provided it was in one of the eligible travel industry sectors, such as hotels. Tralliance would earn revenue for each new registration. The Internet Corporation for Assigned Names and Numbers (ICANN), the organization that oversees domain name policies, has expressed concern about new services at the domain level because any problems could potentially affect millions of users. It referred the proposal to its Security and Stability Advisory Committee, which found that the service was not intended for large scale use and recommended against it. ICANN opened the issue up for public comment and will make a final determination in November.

### **THREAT REPORT: BROWSER BUGS SURGED IN 2006**

Hackers found 47 bugs in Mozilla's open-source browsers and 38 bugs in Internet Explorer (IE) during the first six months of 2006, according to security firm Symantec's bi-annual Internet Security Threat Report, up significantly from the 17 Mozilla and 25 IE bugs found in the previous six months. Even the number of bugs in Apple's Safari browser doubled from six to 12. Opera was the only browser tracked by Symantic where the number of vulnerabilities slightly declined from nine to seven. While IE remained the main choice of hackers, 31 percent of attacks involved more than one browser, and 20 percent attacked Mozilla's Firefox. Home users are the victims in about 86 percent of all attacks. About 37 percent of online attacks originate in the U.S., making the U.S. the biggest source of hackers. The full report can be accessed at [www.symantec.com/enterprise/threatreport/index.jsp](http://www.symantec.com/enterprise/threatreport/index.jsp).

### **IBM TO POST PATENT FILINGS ONLINE**

IBM, the largest patent holder in the U.S. with 2,974 patents issued last year, will publish its patent filings on the Internet for public review. The move is part of its new policy that includes such standards as clearly identifying the corporate ownership of patents to avoid filings that mask authorship. It does carry some business risk because patents typically take three or four years after filing to be approved by the U.S. Patent and Trademark Office, and companies often try to keep the associated technology hidden during that period. IBM used Internet collaboration to

develop its new policy. More than 50 patent and policy experts from the U.S., Europe, Japan and China exchanged views for two months on a wiki, an online site that can be added to and edited collectively. The resulting document can be accessed at <http://www.ibm.com/gio/ip>.

### **SOCIAL NETWORKING USER PATTERNS CHANGING**

Half of the users on MySpace.com are aged 35 or older, with only 30 percent of users aged 25 and younger, according to an analysis of U.S. Internet traffic measurements by comScore Media Matrix. One year ago, teens under 18 years of age comprised 25 percent of the site's users, but that is now down to 12 percent. By contrast, the 35-54 age group grew from 32 percent to 41 percent. ComScore also reported that MySpace had 56 unique U.S. visitors in August 2006, significantly less than the more than 100 million users worldwide, although it should be noted that many people have multiple profiles that were not counted separately by ComScore. Facebook had 15 million unique users, Xanga had eight million and Friendster had one million, according to ComScore. Of the social networking sites studied, Xanga skewed youngest, with 20 percent of its users in the under 18 years of age category

(although Facebook and MySpace both had more users under 18 years of age due to their larger size). Facebook had the biggest share of users in the 18-24 years of age range, although these figures do not reflect Facebook's recent eligibility change from being part of a high school or college network to just needing a valid e-mail address.

### **SENATE RATIFIES CYBERCRIME TREATY**

The U.S. Senate voted to ratify the Council of Europe's Convention on Cybercrime, making the U.S. the 16<sup>th</sup> country to ratify the treaty out of 43 countries that agreed to support the treaty. The treaty calls for signatory nations to cooperate on cyber crime investigations, although the U.S. could choose to deny cooperation requests if they violate free speech or other rights. It does not require that an action be illegal in both countries before one nation's law enforcement can demand cooperation from another country. The treaty also calls for signatory nations to pass similar cyber crime laws that address issues such as computer intrusion, computer-facilitated fraud, child pornography and copyright infringement. A copy of the treaty can be accessed at <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>.

## **LEGISLATION UPDATE**

---

### **WI-FI SECURITY**

On September 30, California Governor Arnold Schwarzenegger signed AB 2415, the Wi-Fi User Protection Bill, into law, requiring manufacturers of Internet

access equipment to put warning labels on Wi-Fi network equipment warning consumers of the risks of using unsecured wireless connections. There are four ways manufacturers can comply by: (1) placing stickers on the boxes, (2) including them in

the setup software, (3) taking specific action when setting up the router or (4) through another process that automatically secures the connection without consumer effort. Only equipment sold after October 2007 will have to comply with the bill, now Chapter 860.

### **INTERNET GAMBLING**

On October 13, the Unlawful Internet Gambling Enforcement Act was signed into law as an attachment to H.R. 4954, a port security bill. The bill, sponsored by Representative Robert Goodlatte (R-VA), prohibits online gamblers from using credit cards, checks and electronic funds transfers to place and settle wagers. The legislation, encoded as Public Law 109-447, requires financial institutions to block all affected transactions. The bill assigns regulatory enforcement to federal financial regulators and the Federal Trade Commission.

### **SOCIAL NETWORKING SITES**

The U.S. House of Representatives passed H.R. 5319 by a vote of 410-15, which seeks to amend the Communications Act of 1934 by requiring schools and libraries that receive universal service support to enforce a policy to protect minors from social networking sites and chat rooms. Such institutions would be required to prohibit access to a social networking site or chat room that (1) might present them with obscene or indecent material, (2) might subject them to unlawful sexual advances and/or repeated sexual comments or (3) might give them access to other material that is harmful to minors. The bill, sponsored by Representative Michael Fitzpatrick (R-PA), would direct the Federal Communications Commission (FCC) to publish an annual list of sites and chat rooms that foster contact between sexual predators and children. The bill was referred to the Senate Commerce, Science and Transportation Committee, where no action has been taken to date.

### **AGENDA SET FOR CYBER CRIMES AGAINST CHILDREN TRAINING**

The agenda for the training conference on **Prosecution of and Innovative Approaches to Cyber Crimes Against Children**, developed and sponsored by 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 has been finalized. The conference will be held on November 14-16, 2006 at the University of Mississippi School of Law, and air or automobile travel will be reimbursed for all prosecutors from Attorney General offices.

Topics to be addressed include: Legal Issues in Child Pornography Investigations, How Jurisdictions Address Child Pornography, Prosecuting a Case With an Unknown Victim, Psychology of the Online Predator, Interviewing the Online Predator, State Legislative Initiatives, ISP Record Retention, Case Law Update, Social Networking Sites, the Adam Walsh Child Protection and Safety Act and Its Effect on State Prosecutors, Developing an Effective Undercover Operation and Cyber Bullying. In addition, there will be a live chat room demonstration as well as an online child pornography case study. For additional information or questions, please contact Hedda Litwin, Cyber Crime Counsel, at 202-326-6022 or [hlitwin@naag.org](mailto:hlitwin@naag.org)