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, Cyberspace Law Counsel (hlitwin@naag.org, 202-326-6022).

This project is supported by grants provided 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 TAKES 4TH AMENDMENT TEXTING CASE

The U.S. Supreme Court agreed to decide whether a police department violated the constitutional privacy rights of an employee when it inspected personal text messages sent and received on a government pager. The case opens “a new frontier in Fourth Amendment jurisprudence,” according to a three-judge panel of an appeals court that ruled in favor of the employee. The following is a summary of the case written by Dan Schweitzer, Supreme Court Counsel at NAAG.

City of Ontario v. Quon, 08-1332. At issue is whether a city police department violated the Fourth Amendment rights of a police officer when it read the transcripts of text messages the officer sent while on duty on a department-issued text-
messaging pager. The City of Ontario, California had a written policy advising employees that use of City-owned computer-related services for personal purposes was forbidden, that the City reserves the right to monitor “all network activity including e-mail and Internet use, with or without notice,” and that “[u]sers should have no expectation of privacy or confidentiality when using these resources.” When the City Police Department obtained text-messaging pagers for its SWAT team officers, it told the officers that the e-mail policy applied to pager messages. The City, however, had to pay extra when a pager went above its monthly character limit. The officer in charge of the administration of the pagers, Lieutenant Steve Duke, adopted an informal agreement that he would not audit pagers that went above the monthly limit if the officers agreed to pay for any overages. Eventually, Lieutenant Duke became tired of collecting bills. That prompted the Chief of Police to order a review of the pager transcripts for the two officers with the highest overages to determine whether the monthly character limit was insufficient to cover business-related messages. One of those officers was respondent Sergeant Jeff Quon. After initial Department review, the matter was referred to internal affairs to determine whether Sergeant Quon was wasting time with personal matters while on duty. Internal affairs discovered that, during the month under review, Sergeant Quon sent and received 456 personal messages while on duty, some to his wife, some to his mistress, many sexually explicit in nature. Sergeant Quon, his wife, and his mistress (collectively, respondents) filed a §1983 action against the City, the Police Department, and others (the “City”), alleging Fourth Amendment violations. A jury found that the Chief of Police’s purpose in ordering review of the transcripts was to determine the character limit’s efficacy

The district court ruled that that was reasonable under the circumstances, and therefore constitutional under O’Connor v. Ortega, 480 U.S. 709 (1987) (plurality). The Ninth Circuit reversed, holding that respondents were entitled to summary judgment in their favor. 529 F.3d 892.

The Ninth Circuit held as a threshold matter that respondents possessed a reasonable expectation of privacy in their text messages. The court found that the City’s general non-privacy policy was overridden by Lieutenant Duke’s informal policy of not auditing pagers so long as the officers paid any overages. Because Duke was in charge of administering the pagers, and Quon’s messages had never previously been reviewed, Quon had a reasonable expectation of privacy in the text messages. The court next held that the search was not reasonable. The court applied O’Connor, in which the plurality stated that, “[g]iven the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis” that looks to “[t]he operational realities of the workplace.” The court found that the search was not reasonable in scope because the government could have accomplished its objectives through “less intrusive methods” – such as “warning Quon that for the month of September he was forbidden from using his pager for personal communications,” “ask[ing] Quon to count the characters himself,” or “ask[ing] him to redact personal messages and grant permission to the Department to review the redacted transcript.” Seven judges dissented from the denial of rehearing en banc.

The City argues that the Ninth Circuit’s opinion “undermines the ‘operational realities of the workplace’ standard” of O’Connor by “erroneously holding that a police lieutenant’s informal policy creates a reasonable expectation of privacy in text messaging on a police department pager in the face of the Department’s explicit no-privacy policy and potential disclosure of the messages as public records.” The
City further argues that the Ninth Circuit erred in applying a “less intrusive means” test to assess the reasonableness of the search. The City cites Skinner v. Ry. Labor Executives’ Ass’n, 489 U.S. 602, 629 n.9 (1989), as stating that the Court has “repeatedly” rejected the “existence of alternative ‘less intrusive’ means” as a basis for evaluating the reasonableness of government searches and seizures. According to the City, the court should instead have “balance[ed] [the search’s] intrusion on the individual’s Fourth Amendment interests against its promotion of legitimate governmental interests” (citation omitted). Respondents assert that the Ninth Circuit did not, in fact, adopt a “less intrusive means” test, but rather held that the search “was excessively intrusive in light of the noninvestigatory object of the search.” Respondents further contend that O’Connor mandated a “case-by-case” fact-intensive inquiry, which necessarily limits this case to its facts, such as the precise authority of Lieutenant Duke.

ATTORNEYS GENERAL FIGHTING CYBERCRIME

MULTI-STATE

Thirty-two Attorneys General reached a $3 million settlement with Vonage, a large Internet-based phone service provider, which requires the company to make significant changes to its marketing practices, to honor consumer cancellation requests and provide refunds to eligible consumers. Vonage formerly paid incentives to customer service representatives for retaining or “saving” customers wanting to cancel, but the settlement strictly limits this practice and requires recording and verification of retention telephone calls. The settlement also compels Vonage to revise its disclosures regarding the offer of “free” services, money back guarantees and trial periods. It requires restitution to eligible consumers who filed complaints or who file complaints through the end of February 2010. The investigation of the case was led by the Attorneys General of Connecticut, Illinois, Michigan, Oregon, Pennsylvania, Texas and Wisconsin. Attorneys General also participating in the settlement include those of Alabama, Arizona, Arkansas, Florida, Hawaii, Idaho, Indiana, Kansas, Kentucky, Louisiana, Maine, Missouri, Montana, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, South Carolina, South Dakota, Tennessee, Vermont, Washington and West Virginia.

ATTORNEY GENERAL Richard Blumenthal of Connecticut and Attorney General Jack Conway of Kentucky requested information from Topix.com, an interactive message board web site based in California, concerning its policies for removing abusive posts that violate the web site’s terms of service. Consumers have complained that it is virtually impossible to remove false and defamatory posts, including those targeting children, unless consumers pay a $19.99 fee.

ALABAMA

Attorney General Troy King personally appeared in court to accept Richard Dobbins’ plea to 311 counts related to production and possession of child pornography. Dobbins faces a maximum sentence of life imprisonment and fines of up to $60,000 for each count of production of child pornography, and up to 10 years imprisonment and fines of up to $15,000 for each count of possession of child pornography. The case was investigated by Attorney General King’s Investigations Division with assistance from the Walker County Sheriff’s Office and
District Attorney’s Office and the Alabama Department of Revenue. The case was prosecuted by Deputy Attorney General Rushing Payne and Assistant Attorney General Andrew Arrington.

**ARIZONA**

Attorney General Terry Goddard announced the indictment of Angel Montalvo, a former Tucson police officer, on nine counts of computer tampering, one count of trafficking in the identity of another person, one count of aggravated taking the identity of another person and one count of fraudulent schemes and artifices. The charges include nine Class 6 felonies, one Class 3 felony and two Class 2 felonies. According to court documents, Montalvo misused his access to police databases for non-law enforcement purposes. He accessed the ACJIS database which contains sensitive information relating to driver registrations, criminal backgrounds, home addresses and other personal information of state citizens. The case resulted from a joint investigation by the Tucson Police Department and the FBI. The case is being prosecuted by Assistant Attorney General Michael Jette.

**COLORADO**

Attorney General John Suthers joined with the Electronic Software Association and Web Wise Kids to launch “Wired With Wisdom,” an Internet safety program designed to educate parents on how to help keep their children safe online. The program addresses the dangers associated with social networking, email, cell phones, chat rooms, instant messaging and other technology widely used by youth. The program will be available free of charge to state parents and caregivers who register.

**CONNECTICUT**

Attorney General Richard Blumenthal sued Health Net of Connecticut, Inc. for failing to secure private patient medical records and financial information involving 446,000 state enrollees, as well as to promptly notify those endangered by the security breach. Attorney General Blumenthal is also seeking a court order blocking Health Net from continued violations of the Health Insurance Portability and Accountability Act (HIPAA) by requiring that any protected health information contained on a portable electronic device be encrypted. Health Net learned that a portable computer disk drive containing protected health information, social security numbers and bank account numbers had disappeared. The data was not encrypted or otherwise protected from access or viewing by unauthorized persons. It was not until six months after the breach was discovered that Health Net posted a notice on its web site and sent letters to consumers. Attorney General Blumenthal alleges that Health Net failed to effectively supervise and train its workforce on policies and procedures concerning appropriate use and disclosure of information, as well as to promptly notify his office of the breach. Assistant Attorneys General Steve Courtney, Tom Ryan and Matt Fitzsimmons, under the direction of Phil Rosario, Arnold Menchel and Henry Salton, worked on the case.

**FLORIDA**

Attorney General Bill McCollum announced that Samuel Keller was sentenced to 15 years in prison after pleading guilty to 20 counts of possession of child pornography and one count of promotion of child pornography. Keller was arrested after he began chatting with an undercover Boynton Beach police officer and then sent the officer images of child pornography. Investigators with Attorney General McCollum’s CyberCrime Unit, the Boynton Beach and Boca Raton Police Departments and the Florida Department of Law Enforcement confiscated com-
Puters from Keller’s home and office and discovered numerous pornography images. Keller was prosecuted by Unit attorneys. In addition to his prison sentence, Keller must serve 10 years of sex offender probation upon his release and will be required to register with the state as a sex offender.

ILLINOIS

Attorney General Lisa Madigan filed a lawsuit against Peel, Inc., an online marketing firm, for “cramming” consumers’ credit cards with unexpected charges for supposedly “free trial” offers for such products as coffee, posters and jewelry. The complaint alleges that Peel sells products on many web sites, including seattlecoffeedirect.com, metroposters.com, posterpass.com and shopdani.com. It markets its products using “free trial” offers and requires consumers to provide their billing information purportedly to cover shipping and handling fees. However, soon after signing up for a free trial, consumers receive unauthorized charges ranging from $19.99 to $49.99. The suit alleges violations of the state Consumer Fraud and Deceptive Business Practices Act and seeks a permanent injunction barring Peel from doing business in the state, restitution for consumers, civil penalties of $50,000 for each violation of the Act and an additional $30,000 for each violation committed with the intent to defraud. Assistant Attorney General Adam Sokol is handling the case.

KENTUCKY

Attorney General Jack Conway’s Department of Criminal Investigations announced the arrest of Sherman Pike, a convicted sex offender, on four counts of possession of child pornography. Attorney General Conway’s Cybercrimes Unit investigators, with assistance from the Marion County Sheriff’s Department and Lebanon Police Department, arrested Pike after executing a search warrant at his home.

MASSACHUSETTS

Attorney General Martha Coakley joined state House Judiciary Chairman Eugene O’Flaherty and 50 other legislators in filing “An Act Further Defining the Dissemination of Obscene Material,” a bill that would update the law regarding the dissemination of harmful material to minors to include electronic communications. The bill would amend Massachusetts General Laws Chapter 272, Section 3, which provides the definition of what “matter” is harmful to minors.

MICHIGAN

Attorney General Mike Cox announced the arrest of Scott Owen as a result of an undercover Internet child predator sting. Owen, who claimed to be employed by a local manufacturing company and a member of the National Guard, is accused of using the Internet to solicit a minor for sex after making advances towards what he thought was a 14-year-old girl, but was actually one of Attorney General Cox’s investigators and an investigator from the volunteer organization, Perverted Justice. Owen was charged with one count of using the Internet to accost a child for immoral purposes, a 10-year felony, and one count of using a computer to disseminate sexually explicit matter to a minor, a four-year felony.

MISSISSIPPI

Attorney General Jim Hood’s Cyber Crime Unit investigators arrested Roy Ellis, who is charged with three counts of possession of child pornography. The penalty for possession is five to 40 years per count in the custody of the state Department of Corrections, so Ellis faces up to 120 years behind bars if convicted. The Clarke County Sheriff’s Office, part of the state’s Internet Crimes Against Children Task Force, assisted with the arrest.
NEBRASKA

Attorney General Jon Bruning unveiled his 2010 legislative package, which includes the Exploited Children’s Rights Act. This bill would allow victims of child pornography to seek a civil remedy of a minimum of $150,000 against those who created, distributed or actively acquired their images. It also would allow the Attorney General’s Office to pursue these cases on behalf of the victim upon their request.

NEW JERSEY

Acting Attorney General Paula Dow joined Criminal Justice Director Stephen Taylor to announce that Stuart Patterson was sentenced to three years in state prison for distributing child pornography on the Internet. Patterson is barred from using the Internet and from having unsupervised contact with minors for the duration of his sentence and must register under Megan’s Law. He was arrested when the State Police executed a search warrant that revealed multiple images of child pornography on his home computer. The State Police Digital Technology Investigations Unit coordinated the investigation, and Deputy Attorney General Lee Schaer prosecuted the case and represented the Department of Criminal Justice at the sentencing.

NEW MEXICO

Attorney General Gary King reported that Jack Skinner was released on a conditional discharge in district court after pleading guilty to 11 counts of possession of child pornography and will also not be required to register as a sex offender. The state Internet Crimes Against Children Task Force executed a search warrant at Skinner’s home after his actions were discovered while Attorney General King’s Office was investigating two other cases. Attorney General King’s Office had recommended six years of incarceration. Attorney General King’s Office was assisted by the FBI and U.S. Immigration and Customs Enforcement.

NEW YORK

Attorney General Andrew Cuomo announced an investigation of 22 popular online businesses that deceptively link unsuspecting consumers to fee-based membership programs that charge unauthorized fees under the guise of discount offers. Attorney General Cuomo has sent subpoenas to Barnes & Noble, Orbitz.com, Buy.com, Ticketmaster.com, MovieTickets.com, FTD.com, Shutterfly.com, 1-800Flowers.com, Avon.com, Budget, Staples.com, Priceline.com, GMAC Mortgage, Classmates.com, Travelocity, Vistaprint, Intellus, Hotwire.com, Expedia/Hotels.com, Columbia House, Pizza Hut and Gamestop/EB Games, all known to have deals with the three major companies that offer these discount programs: Webloyalty, Affinion/Trilegiant and Vertrue. The investigation is being handled by Assistant Attorney General Amy Schallop, Special Counsel Carolyn Fast, Assistant Attorneys General Jennifer Huber, Brian Montgomery and Harkiranjit Chahal of the Bureau of Consumer Frauds and Protection under the supervision of Bureau Chief Joy Feigenbaum.

OHIO

Attorney General Richard Cordray received a favorable decision by the state Supreme Court in a case involving a state law prohibiting adults from sending material defined as “harmful to juveniles,” such as pornography, directly to minors by electronic means. A group of online publishers had challenged the law as violating their free speech rights under the First Amendment. The court confirmed Attorney General Cordray’s position that the statute covers only “electronic communications that can be personally directed,” such as email, text
messages and instant messages. The case will now return to the Sixth Circuit Court of Appeals, which will use the state Supreme Court’s authoritative interpretation of the law.

OREGON

Attorney General John Kroger’s Internet Crimes Against Children Unit arrested Brian Berry on charges of Encouraging Child Sex Abuse in the First and Second Degrees. The unit investigated the case and served a search warrant on Berry’s house. Berry is on probation for a prior conviction.

PENNSYLVANIA

Attorney General Tom Corbett’s Child Predator Unit agents arrested Jason Krebs, who is accused of using Internet instant message programs to sexually proposition what he believed were 13- and 14-year-old girls, but were actually undercover agents using the profiles of children. Krebs also used his computer webcam to send nude images of himself. Agents executed a search warrant on Krebs’ home, seizing computers and data storage devices which will be analyzed by Attorney General Corbett’s Computer Forensics Unit. Krebs is charged with three counts of unlawful contact with a minor and one count of criminal use of a computer, all third-degree felonies which are each punishable by up to seven years in prison and $15,000 fines. The Swatara Township Police Department assisted with the arrest. Krebs will be prosecuted by Deputy Attorney General Christopher Jones of the Unit.

RHODE ISLAND

Attorney General Patrick Lynch announced that the Statewide Grand Jury handed down an indictment naming David Lopez on two counts of first-degree child molestation and one count of possession of child pornography. West Warwick Police conducted the investigation.

TEXAS

Attorney General Greg Abbott’s Fugitive Unit arrested previously convicted sex offender Ernest Bellotte for using the Internet in violation of his parole terms. Unit investigators discovered that Belotte had established online profiles on several social networking sites, including MySpace.com, Twitter and Facebook.

UTAH

Attorney General Mark Shurtleff announced that 14 suspected child pornographers were arrested by his Internet Crimes Against Children (ICAC) Task Force during a month-long special operation called Operation Frostbite. Operation Kids, a national child protection organization, provided private financing for the operation. Six home search warrants and 10 computer search warrants were served during the operation, and ICAC agents interviewed another 25 persons suspected of child sexual exploitation. The law enforcement blitz included the FBI, ICE, state Departments of Public Safety and Corrections, Summit County and Tooele County Sheriff’s Offices and the Salt Lake City, Layton City, West Valley City and South Jordan Police Departments.
WASHINGTON

Attorney General Rob McKenna announced that one of his public safety bills, H.R. 2424, which would give law enforcement an additional tool to prosecute those who intentionally access child pornography, was heard by the House Public Safety & Emergency Preparedness Committee. A companion bill has been introduced in the state Senate.

WISCONSIN

Attorney General J.B. Van Hollen announced that the Kaukauna Police Department has joined the state Internet Crimes Against Children Task Force. As a member, the department will be eligible for investigative assistance, access to the ICAC email group, recognition, reimbursement to help fund ICAC-related expenses and priority for ICAC training.

IN THE COURTS

FOURTH AMENDMENT: GENERAL SEARCH WARRANT

U.S. v. Cioffi, 2009 U.S. Dist. LEXIS 99409 (E.D.N.Y. October 26, 2009). The U.S. District Court for the Eastern District of New York granted the motion to suppress the evidence because the search warrant was too general to comply with the warrants clause of the Fourth Amendment. Ralph Cioffi and Matthew Tannin, former Bear Stearns fund managers, were charged with conspiracy, securities fraud and wire fraud. Prosecutors obtained a warrant to search Tannin’s personal Gmail account, but the warrant failed to specify what evidence was to be seized or what crimes the evidence related. After some initial difficulty, Google gave a copy of the email account to the government. Tannin moved to suppress the evidence on the ground that it violated the Fourth Amendment. The district court agreed, finding that the warrant was facially overbroad and that the affidavit had not been attached or incorporated into the warrant. The court also held that the warrant did not qualify for the “good faith” exception because it does not apply to facially invalid warrants. The “inevitable discovery” exception also does not apply because the government wrongly focused on what would have happened given, rather than without, the unlawful search.

DATABASE BREACH: ACTUAL INJURY REQUIREMENT

Amburgy v. Express Scripts, Inc., 2009 WL 4067218 (E.D. Mo. November 23, 2009). The U.S. District Court for the Eastern District of Missouri dismissed a class action over a database breach because of plaintiff’s failure to establish an injury-in-fact. John Amburgy filed a putative class action against Express Scripts alleging negligence, breach of contract, violation of data breach notification laws and the state Merchandising Practices Act, arising out of the theft of its customers’ personal information. The suit alleged that the breach placed class members at an increased risk of identity theft and extortion, and they would have to spend considerable time and money to protect themselves. Express Scripts moved to dismiss for lack of standing and failure to state a claim for relief. The district court granted the motion, observing that Supreme Court authority requires the injury to be actual or imminent as required for standing.

INEFFECTIVE ASSISTANCE OF COUNSEL: FAILURE TO SEARCH

State v. Gill, 2009 Mo LEXIS 540 (Mo. December 1, 2009). The Missouri Supreme Court overturned defendant’s death sentence because he had ineffective assistance of counsel for failing to request a copy of the victim’s computer which contained child pornography. Mark Gill was arrested for killing
Ralph Lape, Jr. Before the trial, prosecutors provided Gill’s defense attorneys with a police report listing the file folders and directories found on Lape’s computer, which Gill had used to access Lape’s bank information. The report included a list of instant message accounts with sexually explicit names, but defense attorneys never requested a copy of the computer’ contents. A jury found Gill guilty of first degree murder. During the penalty phase, the state introduced evidence of Lape’s good character, but defense attorneys failed to rebut, and Gill was sentenced to death. He appealed both the guilt and penalty phases of his trial, which the circuit court denied. On appeal, the Supreme Court affirmed the denial of the motion as to the guilt phase of the trial, but reversed the denial of the motion as to the penalty finding that defense attorneys failed to inquire about the computer’s contents or interview the police officer who prepared the report about the computer files. The case was remanded.

SEARCH AND SEIZURE: SCOPE OF WARRANT

U.S. v. Williams, 2010 US App. LEXIS 2584 (January 21, 2010). The Fourth Circuit Court of Appeals affirmed defendant’s conviction for possession of child pornography following a search of his home. The Fairfax Baptist Temple in Virginia began receiving sexually explicit emails from an individual who claimed he was a pedophile and that he previously had sexual encounters with several boys in the choir and wanted to continue. The Fairfax County police investigated and found that at least one of the accounts used to transmit the emails had been repeatedly accessed by Karol Williams, wife of defendant Curtis Williams. A search warrant for the Williams home was issued which commanded the officers to search and seize, among other things, “any and all computer systems and digital storage media.” During the search, an officer opened a DVD that had been seized and found over 1,000 images in “thumbnail view” of minor boys in sexually explicit poses. During trial, Williams moved to suppress the evidence, which the district court denied. The court concluded that the child pornography images were “instrumentalities of criminal activity” and therefore their seizure was authorized by the warrant. Williams appealed, but the 4th Circuit upheld the decision. Alternatively, the court held that even if the officers exceeded the scope of the warrant, the seizure of the child pornography was justified under the plain view exception to the warrant requirement.

FIRST AMENDMENT: ONLINE STUDENT PARODY

Layshock v. Hermitage School District, 2010 U.S. App. LEXIS 2384 (3rd Circ. February 4, 2010). The Third Circuit Court of Appeals upheld a lower court ruling finding that a school’s actions over a student’s posting parodying his principal were unconstitutional because they punished the student for exercising his free speech rights. High school student Justin Layshock created a MySpace profile at his grandmother’s house in which he poked fun at the principal for being a “large” man. In response, the school suspended Justin for 10 days, banning him from extracurricular activities and his graduation ceremony. Justin and his parents, as well as the ACLU, sued the school for violating Justin’s First Amendment rights. In its opinion, the court noted that Justin’s speech took place off campus and did not interrupt school operations; therefore, the school did not have the authority to punish him.

But see, in the same circuit court of appeals, on the same day...

J.S. v. Blue Mountain School District, 2010 U.S. App. LEXIS 2388 (3rd Circ. February 4, 2010). In this case with a similar fact pattern as above, the 3rd Circuit Court of Appeals affirmed the lower court
ruling, finding that school officials had a right to punish the student because her profile created a reasonably foreseeable potential for disruption at the school. Here, J.S., an eighth grade honor student, was suspended for 10 days for creating at her home an online profile featuring her principal which featured comments about his sexuality and inappropriate behavior toward students. J.S. and her parents, as well as the ACLU, sued the school for violation of J.S.’s free speech rights. The real possibility of a school disruption was found to justify the school’s actions.

STATE “HARMFUL TO MINORS” LAW: INSTANT MESSAGES

_Commonwealth v. Zubiel_, 2010 Mass. LEXIS 24 (February 5, 2010). The Massachusetts Supreme Judicial Court overturned defendant’s conviction, finding that M.G.L. § 31 does not include electronically transmitted text, or “online conversations.” Matt Zubiel began having sexually explicit online conversations by instant message with what he believed to be a 13-year-old girl but was actually a deputy sheriff. He was arrested at a pre-arranged meeting place with the “girl.” Zubiel was then convicted under state law of four counts of attempting to disseminate harmful material to a minor. He appealed, arguing that the “harmful material” banned under the law did not include sexually explicit instant messages. Under the law, “matter” is defined as: 1) any handwritten or printed material; 2) any visual representation; 3) any live performance; and 4) any sound recording. The high court found for Zubiel in that §31 did not include instant messages or other electronically transmitted text.

ECPA: OPEN WI-FI HOTSPOTS

_U.S. v. Ahrndt_, 2010 WL 373994 (D. Or. January 28, 2010). The U.S. District Court for the District of Oregon found that a child pornography suspect had no constitutionally protected privacy right in the files found on his personal computer, accessible by a neighbor who was piggybacking on his unsecured wireless network. A woman named JH, using her computer, picked up another wireless network and connected to the Internet. She used her iTunes software which, when configured to “share,” also allows users to browse music and video stored in the iTunes libraries of other computers on the network. She accessed another user’s library and found files with names indicating child pornography. JH then contacted the sheriff’s office and again accessed the library while an officer observed. Officers determined and traced the network’s IP address and searched and seized computers and related equipment at the home of John Ahndt under a search warrant. Ahndt argued that JH violated the ECPA when she connected to his unsecured wireless network and accessed his iTunes library while the officer observed. The court noted that under the ECPA, it is lawful for someone “to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.” Since Ahndt’s iTunes program was configured to automatically share files with anyone on the network, it was accessible to the general public, and his ECPA claim failed. The court also rejected his Fourth Amendment claim, finding Ahndt had no reasonable expectation of privacy in his wirelessly accessible files.

CHILD PORNOGRAPHY CONVICTION: RELEASE CONDITIONS

_U.S. v. Miller_, 2010 US App LEXIS 2496 (3rd Cir. February 5, 2010). The Third Circuit Court of Appeals struck down as substantively unreasonable a supervised release condition which put a lifetime limit on Internet use. Donald Miller was sentenced to 30 months’ imprisonment and a lifetime term of supervised release after being convicted of posses-
sion of child pornography. The U.S. District Court for the Middle District of Pennsylvania imposed eight special conditions of his supervised release, including a lifetime restriction on Internet access, mandatory computer monitoring and a limitation on association with minors. Miller appealed, challenging the lifetime limitation on his Internet use. The Third Circuit agreed, finding that the lifetime restriction was a greater restraint of liberty than was reasonably necessary. The decision was vacated and remanded to the district court for further proceedings.

SUPREME COURT NEWS

NYC CLAIMS AGAINST E-CIGARETTE SITES DEFEATED

New York City cannot use a federal racketeering law to accuse discount Internet retailers of cigarettes of evading millions of dollars in sales taxes, the U.S. Supreme Court ruled, 5-3, on January 25. The case is Hemi Group, LLC, et al v. City of New York, No. 08-969. Petitioner Hemi Group is an online cigarette sales company that sells cigarettes to residents of New York City. The City taxes the sale of cigarettes, but in the case of out-of-state and online purchases, the City must collect the taxes directly from the buyer/taxpayer. The Jenkins Act, 15 U.S.C. §§ 375-378, requires out-of-state sellers to provide New York State with customer information. The State then passes this down to the City to enable it to track down customers who do not pay their taxes. The Hemi Group failed to submit Jenkins reports, which the City claimed was both mail and wire fraud under the Racketeer Influenced and Corrupt Organizations (RICO) Act and considered racketeering under 18 U.S.C. § 1961(1).

The U.S. District Court for the Southern District of New York dismissed the City’s claims. That decision, however, was vacated and remanded by the Second Circuit Court of Appeals, which held that the City’s asserted injury – lost tax revenue – came about by reason of the mail and wire frauds.

As the Supreme Court has previously held, to establish that an injury came about by reason of a RICO violation, a plaintiff must show that a predicate offense not only was a “but for” cause of the injury, but was the proximate cause as well, otherwise known as the direct relationship requirement. In the instant case, the Supreme Court held that the City’s causal theory could not satisfy RICO’s direct relationship requirement. Because there was a third party (the State) and a fourth party (the taxpayers), New York City’s RICO claim was not straightforward enough to meet the direct relationship requirement.

LEGISLATIVE NEWS

INTERNET CENSORSHIP

INTRODUCED. On January 26, Representative Bill Foster (D-IL) introduced H.R. 4504, a bill which would authorize the Federal Communications Commission to issue regulations against the censorship of Internet search results. The bill has been referred to the Committee on Energy and Commerce.

INTRODUCED. On February 4, Representative David Wu (D-OR) introduced H.R. 4595, a bill which would establish the Internet Freedom Foundation to promote Internet freedom through education, advocacy and research. The Foundation would be established by the National Science Foundation. The bill has been referred to the Committee on Science and Technology’s Subcommittee on Research and Science Education.
CYBERSECURITY

PASSED HOUSE. On February 4, H.R. 4061, a bill to advance cybersecurity research and development, passed the full House, 422-5. The bill, sponsored by Representative Dan Lipinski (D-IL) would provide nearly one billion dollars in appropriations for federal cybersecurity efforts, including research and development and adoption of technical standards. The bill also authorizes the National Institute of Standards and Technology to develop a cybersecurity education program to help consumers, businesses and government employees keep their computers secure. The bill has now been referred to the Senate Committee on Commerce, Science and Transportation.

NEWS YOU CAN USE

HARVARD STUDY TOUTS ONLINE GAMBLING REGS

A study conducted by Harvard Professor Malcolm Sparrow determined that combining regulation with effective technology and education is the best way to manage the risks of online gambling in the U.S. The study found that the current climate of prohibition has not prevented millions of Americans from gambling online via unregulated, offshore operations. In fact, the study determined that it has left them exposed to risks such as underage gambling, money laundering, problem gambling and fraud. The study was commissioned by WiredSafety, an Internet safety and education resource. The 103-page study can be accessed at http://www.brattle.com/_documents/UploadLibrary/Upload821.pdf.

FCC ISSUES NATIONAL BROADBAND PROPOSALS

The Federal Communications Commission (FCC) unveiled a list of proposals in order to meet a congressional mandate to give every U.S. home access to high-speed Internet service. One proposal put forth by the FCC’s broadband task force calls for using money from the Universal Service Fund, which subsidizes rural phone service, to pay for adding high-speed Internet capacity to remote and low-income regions of the country. The FCC also recommended allocating some airways from television broadcasters to wireless broadband to support the next generation of iPhones and BlackBerrys. Also discussed was revamping the television set-top box market, which has been slow to change and is dominated by a few companies that work directly with cable and satellite operators to lease the boxes to customers. Nearly every home has a television, and the FCC believes that set-up boxes might be a gateway for Internet services.

And see this survey...

The National Telecommunications and Information Administration released a survey showing that while the U.S. has made progress in the number of households that get broadband Internet service, minorities, seniors, less-educated, unemployed and low-income households still lag behind the rest of the population. The survey, conducted by the Census Bureau among more than 50,000 households, found that 64 percent of U.S. households have broadband access, compared with 51 percent in October 2007. Despite national efforts, there is still an urban divide, with two-thirds of urban households reporting broadband service access at home compared with 54 percent of rural households. These figures did improve since 2007, when 54 percent of
urban households and 39 percent of rural households had broadband. The survey also found income disparities in broadband adoption, with 89 percent of those earning $150,000 or more having broadband service at home, compared with just 19 percent for those making $15,000 or less. The top reasons for not getting broadband service were a perception that the service is unnecessary or too expensive. Rural residents also cited a lack of access to the service. The survey report may be accessed at http://www.ntia.doc.gov/reports/2010/NTIA_internet_use_report_Feb2010.pdf.

TOP ANTI-VIRUS PRODUCTS RATED

The publication PC World.com reported its researchers have reviewed and rated several of the top security programs. Their review first determined the products’ detection rates for malware, both known and new. They also measured scan speed, disinfection performance and rate of false alarms, in addition to looking at those features that are designed to protect the average consumer. The review also examined each application’s user interface and simulated a variety of scanning scenarios to ensure it was user-friendly. Full reviews of the top five paid antivirus products may be accessed at http://www.pcworld.com/articles/182539/advanced_antivirus.html.

REPORT: RISKS AND BENEFITS OF CLOUD COMPUTING

The European Network and Information Security Agency (ENISA) released a report which outlines the benefits and potential pitfalls of cloud computing. The report noted that cloud computing provides several clear benefits; it’s computing “on tap,” available instantly and commitment-free. The number one issue restraining businesses and individuals from embracing cloud computing is security. Although providers promise 24/7 availability, data centers can go down. Additionally, security is taken out of the hands of the consumer, who must trust the service provider and therefore companies potentially could face challenges from regulatory audits. Some cloud providers may not fully and properly delete data even if requested. The report finds that companies must perform risk assessments, compare cloud providers to narrow their choice and then obtain service-level assurances from the selected providers and specify the services and tasks that will be handled by the cloud provider. To assist in this process, the report includes a checklist and detailed questions that consumers can use when selecting a cloud provider. The report may be accessed at http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/.

REPORT: SOCIAL MEDIA, BANKING SCAMS ON RISE

Cisco Systems released a report which indicated that social media and data-theft Trojan attacks are on the rise. The new attacks include the Koobface worm, which spreads via Facebook and Twitter. Koobface asks victims to look at a fake YouTube video, which ultimately leads to a malicious download. According to the report, Cisco estimates that Koobface has infected more than three million computers. Another attack on the rise with cyber criminals is the Zeus password-stealing Trojan. Cisco finds that Zeus variants infected almost four million computers last year. Typically, the Zeus Trojan is used to hack into bank accounts, and when hackers infiltrate the accounts, they use their network of money mules to move the stolen funds overseas. Cisco notes that one “old” crime – spam – is still an active threat, with spam volume expected to rise between 30 and 40 percent next year. The re-
DOJ CHILD EXPLOITATION PREVENTION HEAD NAMED

The Department of Justice appointed Francey Hakes to serve as National Coordinator for Child Exploitation Prevention and Interdiction. The position, which is housed in the Office of the Deputy Attorney General, was created under the Protect Our Children Act of 2008. The coordinator is charged with formulating and implementing a national strategy to combat child exploitation, then submitting that strategy and relevant reports to Congress. Hakes will serve as the department’s liaison with all federal agencies regarding the strategy. Hakes has been an Assistant U.S. Attorney in the Northern District of Georgia since 2002, having served previously as an Assistant District Attorney in Georgia for six years.

POLL: INTERNET USERS AVERAGE 13 HOURS/WEEK

A Harris Poll reported that adult Internet users are spending an average of 13 hours per week online, although there is a wide variance in usage. For example, one in five adult Internet users are online for only two hours or less per week while one in seven are spending 24 or more hours per week online. Additionally, the poll highlighted that users aged 30-39 spend the most time online (18 hours), with users aged 25-29 and 40-49 a close second at 17 hours per week. An interesting finding was that one-half of those surveyed reported that they had made a purchase via Internet shopping within the last month. However, the number of adults online – now 184 million or 80 percent – has not changed significantly since 2008, although the number of adults online at home has increased to 76 percent this year compared with 70 percent in 2006. The poll may be accessed at http://news.harrisinteractive.com/profiles/investor/NewsPDF.asp?b=1963&id=35164&m=rl.

TOOLS YOU CAN USE

“Net Cetera: Chatting With Kids Online”

This free guide from OnGuardOnline.gov covers what parents and teachers need to know in order to talk to kids about issues such as cyberbullying, sexting, mobile phone safety and protecting the family computer. Sections of the guide may be posted on an organization’s web site. The guide may be accessed at http://www.onguardonline.gov/topics/net-cetera.aspx and in Spanish at http://www.alertaenlinea.gov/topics/net-cetera.aspx. Bulk quantities can be ordered at http://bulkorder.ftc.gov.

Acquisition Tool Test Results

This series of special reports, sponsored by the National Institute of Justice (NIJ), presents test assertions, environments and results on several mobile device acquisition tools. It is available at http://www.ojp.usdoj.gov/nij/topics/technology/electronic-crime/cftt.htm.
FREE TRAINING TO AG OFFICES

BASIC CYBER CRIME TRAINING

April 20—22, 2010

University of Mississippi School of Law
University, Mississippi

Registration Deadline: March 22, 2010

(application on back pg 16)

This course will teach prosecutors with little or no experience with digital evidence who would like to get up to speed on computer crimes. Also, the course will focus on search and seizure, digital evidence, Fourth Amendment issues and specific computer crimes, such as possession and dissemination of online child pornography and online child exploitation. Attendees will receive CLE credit, and there is no registration fee for Attorney General Office attendees. Travel scholarships are available.

National Association of Attorneys General/
National Center for Justice and the Rule of Law
NATIONAL ASSOCIATION OF ATTORNEYS GENERAL
BASIC CYBER CRIME TRAINING

April 20-22, 2010
University, MS 38677

NOMINATION FORM - RETURN BY MARCH 22, 2010

**PLEASE NOTE: THIS FORM IS NOT AN AUTOMATIC APPROVAL TO ATTEND THE TRAINING.
APPROVAL NOTICE WILL BE SENT UNDER SEPARATE COVER**

MEETING ID NO. 1004_CYBT

Please use one form per registrant/nominee. Complete all sections.

Please return form to: National Association of Attorneys General, Attn: Marland Holloway, Cyberspace Law Paralegal, 2030 M Street, N.W., 8th Floor, Washington, DC 20036 or Fax to (202) 331-1427.

Name (as it should appear on badge):

_________________________________

Full Mailing Address:

_________________________________

Title: ________________________________  ___________________________________

Phone Number: _______________________  ___________________________________

Fax Number: _________________________

E-mail: ______________________________

Attorney General Office: ______________________________

Travel By (Check one):    Air_____ Rail ______ Car______

State Bar registration number(s)  State _____ Number _______
(For CLE credit)

State _____ Number _______

Dietary Restrictions? If so, describe:  ______________________________

Special Requests  If you require special services or auxiliary aids to assist you while attending the meeting and events during the Basic Cyber Crime Training, such as sign-language interpreters, note-takers, large print materials or Braille materials, please contact Marland Holloway, Cyberspace Paralegal, at 202-326-6262 or by email at mholloway@naag.org. NAAG will make suitable arrangements.