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.

**NYC CLAIMS AGAINST E-CIGARETTE SITES DEFEATED**

New York City cannot use a federal racketeering law to accuse Internet retailers of discount cigarettes of evading millions of dollars in sales taxes, the U.S. Supreme Court ruled, 5-3. 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.
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 know 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.

ATTORNEYS GENERAL FIGHTING CYBERCRIME

ALABAMA

Attorney General Troy King presented the State’s sentencing request at a hearing in which Richard Dobbins received life sentences for each of 115 counts of production of child pornography, a class A felony, as well as 10-year sentences for each of 196 counts of possession of child pornography, a class C felony. All sentences are to run concurrently. Dobbins was convicted under Alabama’s child pornography law, which was proposed by Attorney General King. The case was investigated by Attorney General King’s Investigations Division with assistance from the Walker County Sheriff’s and District Attorney’s Offices and the state Department of Revenue. Prosecutors involved in the case were Assistant Attorney General Kelly Hawkins, chief of the Family Protection Unit; Deputy Attorney General Rushing Payne; and Assistant Attorney General Andrew Ar- rington.

CALIFORNIA

Attorney General Edmund Brown, Jr.’s petition to the U.S. Supreme Court to review a case involving a state law prohibiting the sale or rental of violent video games was granted. The 2005 law required violent video games to be labeled with an “18,” prohibited their sale or rental to minors and authorized fines of up to $1,000 for each violation. The Video Software Dealers Association (now part of the Entertainment Merchants Association) sued to block the law, which was invalidated in 2007, a ruling upheld by the Ninth Circuit Court of Appeals in 2009. Attorney General Brown’s petition argues that violent material in video games should be subject to the same legal standard the courts have applied to limitations on sexually explicit material sold to children.

DELAWARE

Attorney General Beau Biden unveiled S.B. 158, a bill that would extend financial liability to producers and possessors of child pornography and set specific damages available to victims. The bill creates a presumption that victims of child pornography are injured, thus relieving them of having to prove specific damages in court. It entitles them to damages of at least $150,000 and extends the statute of limitations from two to three years from notification of the victim by law enforcement of their victimization, the conclusion of a criminal prosecution
against the defendant or the victim reaching the age of 18, whichever comes later. It also allows the court to award attorney’s fees and costs to the victim.

**FLORIDA**

Attorney General Bill McCollum’s CyberCrimes Unit, assisted by the Clay County Sheriff’s Office, arrested Jeffery Hartsell on charges of possession of child pornography after Unit investigators discovered multiple images of child pornography in his possession during a routine investigation. Investigators traced the images to Hartnell’s computer, and a search warrant was executed at his home. Two computers, two external hard drives and other digital media were seized to undergo forensic analysis, but an initial review of the computers revealed multiple images of child pornography. Hartnell faces 13 counts of child pornography, a second-degree felony and enhanced under the CyberCrimes Against Children Act.

**KANSAS**

Attorney General Steve Six’s Tobacco Enforcement Unit announced that its Operation Cyber-Smoke, a program to crack down on illegal and underage sales of cigarettes over the Internet to state consumers, has resulted in 20 web sites refraining from making additional sales in the state. Attorney General Six’s Office also drafted model sales ban legislation and supported research for age verification software.

**KENTUCKY**

Attorney General Jack Conway announced that Ronald Hornback was indicted by a grand jury on four counts of possession of child pornography. Attorney General Conway’s Cybercrimes Unit investigators, with assistance from the State Police, arrested Hornback after executing a search warrant at his home, culminating a five-month investigation by the Unit.

**MARYLAND**

Attorney General Douglas Gansler announced the successful outcome of a cooperative effort between his Office and Google, Inc. to curb the prevalence of false or misleading advertisements touting cures for viral sexually transmitted diseases (STDs) on Google’s search result pages. Due to this effort, Google has improved its mechanisms for screening out these ads in the “Sponsored Links” sections on the right side of the page of search results. Google responded to Attorney General Gansler’s concerns by adding viral STDs to its list of health conditions for which AdWords ads for “miracle cures” are prohibited.

**MASSACHUSETTS**

Attorney General Martha Coakley announced that Raphael Chiu was arraigned on charges of Dissemination or Possession of Obscene Matter, Dissemination of Child Pornography and Possession of Child Pornography. Chiu was arrested at his residence by State Police assigned to Attorney General Coakley’s Office after an online investigation of computer systems offering known child pornography images and movies over file-sharing networks was tracked to Chiu’s home. Police then obtained and executed a search warrant of the home and discovered the images. The case is being prosecuted by Assistant Attorney General Julie Ross of Attorney General Coakley’s Cyber Crime Division.

**MINNESOTA**

Attorney General Lori Swanson filed three separate lawsuits against online payday lenders that made instant short-term loans over the Internet to
state citizens that grossly exceeded interest rates allowed under state law and also failed to comply with state licensing rules and consumer protections. The lenders are Eastside Lenders LLC of Delaware, Global Payday Loan, LLC of Utah and Jelly Roll Financial, LLC of Utah, none of which have a license with the state Department of Commerce allowing them to make small consumer loans to residents. All three companies charged borrowers $30 in interest for a two-week $100 loan, which is a 782 percent annual interest rate.

MISSISSIPPI

Attorney General Jim Hood’s Cyber Crime Unit assisted Jackson County Sheriff’s Office investigators in arresting Jonathan Russell, a student at Jackson County Community College, who is charged with 10 counts of possession of child pornography. Russell was arrested after the Jackson County Criminal Investigation Division executed a search warrant on his home. If convicted, he faces up to 400 years in prison.

NEBRASKA

Attorney General Jon Bruning was named to the Board of the National Center for Missing and Exploited Children (NCMEC). He will be the first representative from the National Association of Attorneys General (NAAG) on the Board.

NEW JERSEY

Attorney General Paula Dow joined Criminal Justice Director Stephen Taylor to announce that Neil Cohen, a former state Assemblyman, pleaded guilty to a charge of distributing child pornography, admitting that he used computer equipment in his legislative district office to view, print and distribute pornographic images. The guilty plea was taken by Deputy Attorneys General Anthony Picione, Deputy Chief of the Corruption Bureau, and Christine Hoffman, Chief of the Corruption Bureau. Under a plea agreement, the State will recommend that Cohen be sentenced to five years in state prison, will be permanently barred from any public employment or elected office and will be required to register as a sex offender. The State Police and the Division of Criminal Justice conducted the investigation, with the Division represented by Sgts. David Salzmann and Warren Monroe, Detectives Michael Behar and Harry Marino and Deputy Attorney General Anthony Picione, all of the Official Corruption Unit, and Deputy Attorney General Kenneth Sharpe of the Computer Analysis and Technology Unit.

NEW MEXICO

Attorney General Gary King announced that a grand jury charged Jordan Madison with 25 counts of possession and five counts of distribution of child pornography, and charged Marco Baca with 19 counts of possession, seven counts of distribution and four counts of manufacturing of child pornography. Attorney General King’s Internet Crimes Against Children (ICAC) Unit and state ICAC Task Force members worked together on both cases. Madison potentially faces 37.5 years in prison, and Baca faces 85.5 years.

NORTH CAROLINA

Attorney General Roy Cooper reached an agreement with Morris Broadband, a telecommunications and cable company serving western parts of the State, whereby the company agreed to pay $60,000 in additional credits to consumers who experienced lengthy service outages last fall due to technical problems. The credits are in addition to the $68,000 worth of credits already issued. According to the company’s estimates, approximately 1,800 telephone and 8,000 Internet subscribers were without service for up to 10 days.
OHIO

Attorney General Richard Cordray won a decision in the Sixth Circuit Court of Appeals which found that a state law prohibiting adults from sending material defined as “harmful to juveniles” directly to minors by electronic means was constitutional. Attorney General Cordray defended the statute in American Booksellers Foundation for Free Enterprise v. Cordray.

OREGON

Attorney General John Kroger announced that Richard Downward was arraigned on 12 counts of possession of child pornography. As a condition of release on bail, he is not allowed to have contact with minors or access the Internet. Senior Assistant Attorney General Michael Slauson is prosecuting the case.

RHODE ISLAND

Attorney General Patrick Lynch announced that a grand jury indicted David Carrillo on one count of accessing a computer to defraud and two counts of obtaining money under false pretenses. Carrillo accessed a computer system for the purpose of defrauding the City of North Providence.

TEXAS

Attorney General Greg Abbott joined U.S. Attorney for the Southern District of Texas Jose Moreno to announce that Barry Davis, aka “Sir Lewis,” was found guilty of sex trafficking of a minor, enticing and coercing an adult and transporting the victims across state lines for the purpose of engaging in prostitution. One of the victims testified that nude photos of her were posted online for prostitution advertisements. Forensic analysis of Davis’ computer conducted by the Greater Houston Regional Computer Forensic Laboratory revealed pictures of the victims. The case was brought as part of Project Safe Childhood and was prosecuted by Special Assistant U.S. Attorney Angela Goodwin of Attorney General Abbott’s Office and by Assistant U.S. Attorney Sherri Zack of the U.S. Attorney’s Office.

VIRGINIA

Attorney General Kenneth Cuccinelli announced that David Ednie was convicted of 18 counts of possession of child pornography and sentenced to nine years in prison with a recommended fine of $1,000. Immigration and Customs Enforcement (ICE) agents learned that Ednie had sought to purchase a subscription to a known child pornography web site and subsequently interviewed Ednie, who consented to a search of his computer. A subsequent forensic examination of the computer revealed the presence of child pornography. The case was prosecuted by Assistant Attorneys General Tommy Johnstone and Chip Muir.

WASHINGTON

Attorney General Rob McKenna’s legislation to protect children from sexual exploitation was signed into law by Governor Chris Gregoire. HB 2424 makes it a felony to intentionally view child pornography on the Internet. Previously, child pornography could be viewed and prosecution avoided if the material was not downloaded or printed.

WISCONSIN

Attorney General J.B. Van Hollen’s Division of Criminal Investigation agents, with assistance from the Chippewa County Sheriff’s Department, served a search warrant at the residence of Joseph Bade. Bade admitted downloading and viewing child pornography via an online software file sharing program. He also admitted that two computer hard
drives at his residence would contain videos of child pornography, which an on-scene analysis by law enforcement revealed. Bade was charged with two counts of possession of child pornography.

IN THE COURTS

SEARCH AND SEIZURE: SCOPE OF WARRANT

U.S. v. Mann, 2010 U.S. App. LEXIS 1264 (7th Cir. January 20, 2010). The Seventh Circuit Court of Appeals affirmed a lower court ruling finding that a search that uncovered child pornography on defendant’s computer did not exceed the scope of a warrant to uncover images of voyeurism. While working as a life guard, Matthew Mann covertly installed a video camera in a locker room to take pictures of women changing their clothes. The camera was discovered and turned over to the police, and a search warrant was executed at Mann’s home for “video tapes, CDs or other digital media, computers and the contents of said computers, tapes or other electronic media, to search for images of women in locker rooms or other private areas.” Police seized computers and an external hard drive. They later ran forensic software on the equipment that revealed child pornography. Mann moved to suppress the images found on his hard drive, but the U.S. District Court for the Northern District of Indiana denied the motion. Mann then pled guilty, but reserved the right to litigate his Fourth Amendment claim on appeal. The Seventh Circuit concluded that the search was lawful because the child pornography was discovered while conducting a systematic search for evidence of voyeurism. The court, however, did acknowledge that the police failure to stop the search and request a new warrant was troubling.

FOURTH AMENDMENT: P2P FILE SHARING

U.S. v. Borowy, 2010 US App. LEXIS 3056 (9th Cir. February 17, 2010). The U.S. Court of Appeals for the 9th Circuit found that an FBI agent did not violate the Fourth Amendment by finding and downloading defendant’s files from a shared folder on a P2P network. Charles Borowy installed file-sharing program Limewire on his computer which, as a feature, made his hard drive available to anyone with Limewire installed. FBI Special Agent Byron Mitchell logged onto Limewire to monitor trafficking in child pornography and searched for the term, “Lolitaguy,” a name frequently associated with child pornography. He got “hits” from Borowy’s computer, so Mitchell used Limewire’s “view-files-on-this-host” feature and saw about 240 files identified as known child pornography. Using that as probable cause, Mitchell downloaded copies of files from Borowy’s computer, confirmed they were child pornography and arrested Borowy. Borowy moved to suppress the evidence, which the U.S. District Court for the District of Nevada denied. Borowy appealed, arguing that the evidence was obtained in violation of the Fourth Amendment. The Ninth Circuit affirmed the district court decision upholding the actions of the FBI and finding that it had not violated Borowy’s Fourth Amendment rights. It found that Borowy had no expectation of privacy on the file-sharing network.

COMPUTER FRAUD AND ABUSE ACT: AUTHORIZATION TO ACCESS

U.S. v. John, 2010 US App. LEXIS 2742 (5th Cir. February 9, 2010). The Fifth Circuit Court of Appeals affirmed the defendant’s conviction to commit access device fraud, finding that “unauthorized access” under the Computer Fraud and Abuse Act (CFAA) could encompass limits placed on the use of the information obtained. Demetriace John, an ac-
count manager at Citigroup, gave her half-brother customer account information which he and his friends used to run up fraudulent charges. She was charged with credit card fraud and conspiracy, as well as with unauthorized access to Citigroup’s computers. The jury convicted on all counts. On appeal, Johns challenged her conviction for unauthorized access because she was authorized as an employee to access the computer. The Fifth Circuit disagreed, finding that limits on access could be placed, especially where Johns knew or reasonably should have known that she was not authorized to access the computer, or information obtainable from the computer, in furtherance of or to perpetrate a crime.

FIRST AMENDMENT: OFF-CAMPUS ONLINE SPEECH

Evans v. Bayer, 2010 WL 521119 (S.D. Fla. February 12, 2010). The U.S. District Court for the Southern District of Florida ruled that a high school student who was suspended for creating offline a Facebook group which criticized a teacher has a valid claim for violation of her free speech rights. Karen Evans created a Facebook page after hours on her home computer, the purpose of which was to voice dislike of a particular teacher. The teacher was unaware of the page, which did not disrupt school activities, although Evans took it down two days later. The principal, Peter Bayer, became aware of the page after it had been taken down and suspended Evans for three days and removed her from advanced placement classes. Evans filed suit against Bayer under § 1983, alleging violation of her First and Fourteenth Amendment rights and seeking an injunction ordering Bayer to revoke the suspension, in addition to nominal damages and attorney’s fees. Bayer moved to dismiss the demand for damages. The district court noted that Evans’ speech was made off-campus, was never accessed on-campus and was no longer accessible when Bayer learned of it. The court also rejected Bayer’s contention that he was justified in regulating Evans’ speech based on a reasonable expectation of disruption because nothing in the pleadings indicated that such expectation was well founded. It concluded that Evans had a constitutional right to engage in the speech at issue and denied Bayer’s motion to dismiss Evans’ demand for nominal damages.

TRESPASS: ONLINE MAPS

Boring v. Google Inc., 2010 WL 318281 (3rd Cir. January 28, 2010). The Third Circuit Court of Appeals reversed a lower court, finding that a real property owner who alleges trespass for being a target of Google’s street view does not have to allege damages. The Google camera car drove down the private driveway belonging to Aaron and Christine Boring, took pictures of their house and published the photos on Google Street View. The Borings sued for trespass, but the U.S. District Court for the Western District of Pennsylvania rejected their claim because they had not adequately alleged damages from the trespass. On appeal, the appeals court reversed the district court, finding that a real property owner does not have to allege damages in order to state a valid trespass claim.

CONVICTED SEX OFFENDERS: LIFE-TIME BAN ON INTERNET

U.S. v. Heckman, 592 F.3d 400 (3rd Cir. January 11, 2010). The Third Circuit Court of Appeals rejected the imposition of a lifetime ban on Internet access imposed by the district court. Arthur Heckman admitted to receiving and then transmitting 18 images of child pornography on the Internet. The U.S. District Court for the Eastern District of Pennsylvania imposed an unconditional lifetime ban on Internet access. On appeal, the Third Circuit Court of Appeals rejected this condition. The court noted that while Heckman had a lengthy history of
child molestation, he had never been convicted of using the Internet to exploit a child, and the court refused to make the assumption that Heckman would progress to using the Internet to harm a child. The court noted that there were alternative, less restrictive means of controlling an offender’s Internet use, including computer monitoring.

**STATE CHILD PORNOGRAPHY STATUTE: OVERBROAD CHALLENGE**

American Booksellers Foundation for Free Expression v. Cordray, 2010 Ohio LEXIS 52 (January 27, 2010). The Ohio Supreme Court agreed, 7-0, with state Attorney General Richard Cordray’s interpretation that a state law banning electronic transmission to minors of pornography or other material “harmful to juveniles” applies only to personally directed communications, such as instant messages and emails. The American Booksellers Foundation for Free Expression sought an injunction barring the state attorney general and county prosecutors from enforcing the provisions of R.C. 2907.31, a statute that makes it a crime to disseminate to a juvenile any material or performance that is “obscene or harmful to juveniles.” The U.S. District Court for the Southern District of Ohio granted the injunction, finding that the statute was unconstitutionally overbroad and violated the strict scrutiny test of the First Amendment. The state appealed, and the Sixth Circuit Court of Appeals asked the Supreme Court of Ohio to review the statute and answer two questions: 1) Is the Attorney General correct in construing R.C. 2907.31(D) to limit the scope of R.C. 2907.31(A), as applied to electronic communications, to personally directed devices such as instant messaging, person-to-person emails and private chat rooms? 2) Is the Attorney General correct in construing R.C. 2907.31(D) to exempt from liability material posted on generally accessible websites and in public chatrooms? The Supreme Court answered both questions in the affirmative., agreeing with the Attorney General’s narrow reading of the statute.

*Ed. Note: The case was handled by Benjamin Mizer, Solicitor General, and Elise Porter, Assistant Solicitor, both with the Office of the Attorney General of Ohio.*

**And see another challenge...**

**“HARMFUL MATERIAL”: INSTANT MESSAGES**

Commonwealth of Massachusetts v. Zubiel, 2010 LEXIS 24 (February 5, 2010). The Massachusetts Supreme Court overturned the conviction of a man accused of sending sexually explicit instant messages to a 13-year-old girl, ruling that such messages were not covered by state law. Matt Zubiel began having sexually explicit conversations via instant messaging 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. Zubiel was convicted in a jury-waived trial and sentenced to one year in prison. On appeal, Zubiel argued that although the law listed more than one dozen examples of the obscene “matter” that adults can’t give to minors, instant messages were not included. The court considered whether instant messages could be included under several examples listed in the statute, but decided they did not fit. The court found that the messages were not a “visual representation” of sexually explicit material, ruling that the category included only photographs and other images, but not text. It also ruled that instant messages were not handwritten material because they were not written with pen or pencil. Finally, the court ruled that they were not printed material because no paper was involved.
Search and Seizure: Scope of Consent

State of Maine v. Bailey, 2010 WL 724808 (ME March 4, 2010). The Supreme Court of Maine concluded that a detective’s search of defendant’s computer had violated his Fourth Amendment rights because it was not consistent with the detective’s stated purpose for the search. The Maine State Police Computer Crimes Unit contacted a detective in the Bangor Police Department regarding the dissemination of child pornography using a peer-to-peer networking program with a Maine IP address. The Unit had already subpoenaed Time Warner RoadRunner for the name and address of the subscriber. The detective obtained and executed a search warrant on the subscriber residence and, while not finding the computer or any child pornography, did find an unsecured wireless router sharing that IP address. The detective canvassed neighboring homes in range of the router and came to the home of Jack Bailey. He identified himself as a police officer and told Bailey there was a problem with people accessing someone else’s computer. He asked Bailey if he could take a quick look at his computer to make sure he didn’t have that problem also, and Bailey agreed. Once given access, the detective ran a general search for video files and found four files that appeared to contain child pornography. The detective questioned Bailey, who then admitted he had a “problem” with child pornography. Bailey orally consented to a search of his residence, and officers found tapes of exposed underage girls filmed by someone off-camera they called “Jack.” Bailey was charged with and convicted of 10 counts of gross sexual assault, one count of gross sexual exploitation of a minor and two counts of unlawful sexual contact. Bailey appealed, arguing that 1) his consent was obtained by deception and thus invalid, and 2) the detective exceeded the scope of consent in violation of the Fourth Amendment. As to the first argument, the court reviewed the conversation between Bailey and the detective and concluded that although the detective’s exchange was somewhat ambiguous, it was not expressly misleading, so the consent was thus voluntary. As to the second argument, the court found that a reasonable person would have concluded from the conversation that Bailey consented to a search to see if his computer was being accessed by someone else, so the detective exceeded that scope when he ran a general search in violation of the Fourth Amendment. The court vacated the conviction and remanded the case for a determination if the unconstitutional search required suppression of other evidence.

Sentencing: Enhancements for Child Pornography

U.S. v. Dodd, 2010 US App. LEXIS 5136 (8th Cir. March 11, 2010). The 8th Circuit Court of Appeals affirmed a lower court’s imposition of sentencing enhancements for receiving and possessing child pornography. A law enforcement officer investigating child pornography distribution conducted a search on LimeWire for “preteen.” He found files containing child pornography. A warrant search of Dodd’s home revealed 17 videos on his computer containing child pornography. Dodd was charged and pled guilty to receiving and possessing child pornography. The presentence investigation report (PSR) recommended that the base offense level be increased by two levels because Dodd distributed the child pornography to another person. Dodd objected, but the district court imposed the enhancements. On appeal, Dodd again objected to the increase, arguing there was no evidence that he was aware his files were available to others. The government countered that LimeWire is set up for the sole purpose of sharing files, and affirmative steps must be taken to make the files available. The court concluded that prior circuit cases establish that the increase is applicable if a file sharing device is set up so files can be shared.
SEXTING: PROSECUTION OF MINORS

Miller v. Mitchell, 2010 US App. LEXIS 5501 (3rd Cir. March 17, 2010). In the first case to challenge the constitutionality of prosecuting teens for sexting, the Third Circuit Court of Appeals upheld an injunction barring the district attorney from bringing child pornography charges against girls who refused to attend an educational class on the dangers of sexting as a remedy for their engaging in such practice. Officials in a Pennsylvania school district discovered photographs of nude and semi-nude teenage girls on students’ cell phones. The District Attorney of Wyoming County, Pennsylvania sent a letter to several students’ parents, threatening to bring charges against students unless they completed an education program of six to nine months and which included writing a report about why they were there. At a public hearing, the District Attorney reiterated that he would bring felony charges against any child who did not submit to probation, pay a $100 program fee and complete the education program. A mother and daughter, using the pseudonyms “Jane Doe” and “Nancy Doe,” sued the District Attorney for violating their constitutional rights. They argued that any prosecution in these circumstances would be unconstitutional retaliation that would punish Jane Doe’s right to direct her child’s upbringing without government interference, as well as Nancy Doe’s free speech right not to write a confessional report. The Third Circuit agreed. First, it found that the education program’s lessons interfered with an essential component of Jane Doe’s right to raise her daughter, and therefore the District Attorney could not coerce attendance by threatening prosecution. Second, the court found that it would violate the First Amendment to force Nancy Doe to explain why her actions were morally wrong as part of the program. Finally, the court held that the District Attorney lacked probable cause to prosecute Nancy Doe because “appearing in a photo provides no evidence as to whether that person possessed or transmitted the photo.”

FOURTH AMENDMENT: DELIVERED E-MAIL

Rehberg v. Paulk, 2010 US App. LEXIS 5198 (11th Cir. March 11, 2010). In a very controversial ruling, the 11th Circuit Court of Appeals held that sending e-mails to third parties constitutes a voluntary relinquishment of the right to privacy in that information. State investigators suspected Charles Rehberg of sending anonymous faxes to the management of a local hospital. They allegedly used a state subpoena to obtain the contents of Rehberg’s e-mail from his Internet service provider. Rehberg was indicted for harassment and other charges, but eventually the charges against him were dismissed. Rehberg turned around and sued the investigators for malicious prosecution in violation of his Fourth and Fourteenth Amendment rights. Rehberg also alleged that defendants violated his privacy by illegally issuing subpoenas to Internet service providers without a pending indictment and as a discovery device for private civilians. The defendants moved to dismiss under Rule 12(b)(6) arguing immunity, but the U.S. District Court for the Middle District of Georgia denied the motion and defendants appealed. The 11th Circuit ruled that defendants would receive qualified immunity because Rehberg’s subpoena violations failed to state a constitutional violation. The court found that the subpoenas covered information that Rehberg had voluntarily provided to third parties and for which Rehberg did not have a legitimate expectation of privacy. Thus, the court reasoned, the subpoenas did not violate Rehberg’s Fourth Amendment right to be free of unreasonable search and seizure.

CONVICTED SEX OFFENDERS: ONLINE IDENTIFIERS

White v. Baker, 2010 WL 1009758 (N.D. Ga. March 3, 2010). The U.S. District Court for the Middle District of Georgia found that the 2008 amend-
ment to Georgia’s sex offender registration law, which requires providing Internet identifiers to law enforcement, is not sufficiently narrow to accomplish the state’s legitimate interest in protecting children. Terrence White was convicted of enticing a child for indecent purposes and served his time. Upon release, he challenged the 2008 amendment to Georgia’s sex offender law, which required him to submit his email addresses, usernames and passwords to law enforcement as a condition of registration. White claimed that the law had a “chilling” effect on his free speech rights because of the possibility that his communications were being monitored by law enforcement and his identifying online information could be disclosed to the public. He also argued that the law was overbroad to the extent it would allow law enforcement to access his online accounts and other information. The state argued that the measure was necessary to protect the public. The district court found that the amendment had a chilling effect on White’s right to anonymous free speech and that it was not sufficiently narrow to accomplish Georgia’s legitimate interest in protecting children. The court granted White’s motion for an injunction preventing enforcement of the statute.

Ed, Note: The state’s case was argued by Paige Boorman and Joseph Brolet, attorneys in the Office of the Attorney General of Georgia

CONVICTED SEX OFFENDER: 30-YEAR COMPUTER BAN

U.S. v. Russell, 2010 U.S. App. LEXIS 6846 (D.D.C. April 2, 2010). The U.S. District Court for the District of Columbia struck down a 30-year ban on computer use by a convicted sex offender as a “substantial burden” on a person’s liberty interest. Mark Russell pleaded guilty to one count of traveling to engage in unlawful sexual activity. He was sentenced to 46 months in prison and 30 years of supervised release during which he was banned from possessing or using a computer for any reason. Russell appealed the duration of his supervised release as well as the restriction on his computer usage as substantively unreasonable. The district court affirmed the length of his supervised release but found that the ban on his computer usage interfered with the goal of rehabilitation, noting that even submitting a job application requires the use of a computer. The court vacated the computer restriction and remanded for resentencing.

LEGISLATIVE NEWS

ELECTRONIC COMMUNICATIONS BY JURORS

CALIFORNIA. On April 14, AB 2217, a bill that would amend civil and criminal contempt statutes to allow punishment of jurors who electronically discuss confidential information concerning the case before them, passed the Assembly. The bill does not modify standard jury instructions, but instead puts the burden on the officer in charge of the jury. The bill was referred to the state Senate for further consideration.

SEXTING

RHODE ISLAND. On March 23, the Rhode Island Senate Judiciary Committee recommended further study on S. 2635, a bill that would make sexting a status offense to be referred to the Intake Unit of Family Court, rather than subject to prosecution under the state child pornography law. The bill was drafted by the Attorney General’s Office.

CYBERSECURITY

PASSED SENATE COMMITTEE. On March 24, S. 773, a bill sponsored by Senator John Rockefeller (D-WV) to address cybersecurity, was reported fa-
vorably out of the Committee on Commerce, Science and Transportation. The bill would 1) provide for the development and implementation of a system to provide cybersecurity and vulnerability status, 2) establish cybersecurity standards for all federal government agencies, 3) require development of a secure domain name addressing system and 4) establish a board to review and approve all software products to be purchased by the federal government.

PEER-TO-PEER SOFTWARE

PASSED HOUSE. On March 24, H.R. 4098, a bill sponsored by Representative Edolphis Towns (D-NY) which would require the Office of Management and Budget to issue guidance prohibiting the personal use of peer-to-peer file sharing software by federal government employees, passed the House. The bill has been referred to the Senate Committee on Homeland Security and Government Affairs.

INTERNATIONAL CYBERCRIME

INTRODUCED. On March 23, Senator Kirsten Gillibrand (D-NY) introduced S. 3155, a bill that would 1) give priority assistance to countries lacking the infrastructure to combat cybercrimes, 2) require the development of an action plan for each country determined to be a cyber concern and 3) take restrictive action against non-compliant countries. The bill has been referred to the Committee on Foreign Relations. A companion bill, H.R. 4962, was introduced in the House by Representative Yvette Clarke (D-NY) and referred to the Committee on Foreign Affairs.

INTERNET GAMBLING

INTRODUCED. On March 25, Representative Jim McDermott (D-WA) introduced H.R. 4976, a bill that would impose a gambling license fee and taxes on Internet gambling operations. The bill also contains a provision that would allow each state and tribal government to be paid six percent of all deposits placed by residents of their jurisdiction with licensed online gambling operations. It would also assign 25 percent of the federal revenue collected to provide assistance to children in foster care. The bill was referred to the Committees on Ways and Means and Education and Labor.

NEWS YOU CAN USE

NYC BAR: LIMIT PERSONAL DATA IN FILINGS

A New York City Bar subcommittee released a report urging courts to adopt a statewide rule that would curtail the inclusion of “sensitive personal information” in civil court filings. Citing the increasing availability of court documents online, the subcommittee on electronic records with the Bar’s Council on Judicial Administration advised that filings omit nine categories of information, including Social Security, taxpayer identification and driver’s license numbers. The rule would also prohibit the names of minor children, dates of birth, bank and financial account numbers, government-issued identification numbers and “other identification numbers which uniquely identify an individual.” Attorneys and other personnel filing documents would be responsible for complying with the rule. However, under the proposal, if there is a good faith belief that the information is “material or necessary to the action” and “compelling reasons” exist for its inclusion, filers could list an abbreviated version of the information, such as the last four digits of a Social Security number or the initials of minor children.
FCC VOTES TO EXPAND E-RATE

The Federal Trade Commission (FCC) voted to expand E-Rate, a program that funds schools’ connectivity to the Internet under the $B billion Universal Service Fund, a U.S. subsidy program enabling low-income families to access telephone service. The five FCC members approved an order that would allow local communities to use their schools’ Internet access after school hours, thus ostensibly providing greater access to broadband for the public at no additional cost to the Fund. The program could now assist adults taking evening digital literacy courses, unemployed individuals looking for jobs posted online and people who need to access online government services.

SURVEY: JOB SEEKERS REJECTED DUE TO ONLINE INFORMATION

Seventy percent of hiring managers say they’ve decided not to hire an applicant because of information they have found online, according to a survey commissioned by Microsoft of 1,200 human relations managers and consumers. While most of those surveyed stated they research candidates online and think they are justified in doing so, only seven percent of consumers believed that recruiters check out potential candidates online when making hiring decisions. Over one-half of managers surveyed agreed that data on lifestyle, inappropriate written text and inappropriate photos were types of information that could result in rejecting a candidate. An overview of the findings from the survey can be accessed at http://www.microsoft.com/privacy/dpd/research.aspx.

STUDY TIES EXCESSIVE INTERNET USE TO DEPRESSION

A direct relationship exists between the amount of time spent surfing the Internet and the signs of depression, according to a study by scientists at Great Britain’s Leeds University. The study analyzed Internet users and depression levels of 1,319 Britons between the ages of 16 and 51. It found that of those surveyed, 1.2 percent were addicted to the Internet which, while seemingly insignificant, is higher than the incidence of gambling in Britain, which is .06 percent. Those individuals found to be addicted spent proportionately more time browsing sexually gratifying websites, online gaming sites and online communities, as well as having higher incidence of moderate to severe depression than normal Internet users. It was, however, unclear whether depressed people are drawn to the Internet or whether the reverse is true. Additional information can be accessed at http://www.medicalnewstoday.com/articles/178042.php.

REPORT: PHISHING ATTACKS ON THE RISE

The Anti-Phishing Working Group (AWPG) issued its Phishing Activity Trends Report for the third quarter of 2009, finding that every statistic involving phishing had increased. Reports of phishing submitted to APWG rose 5.5 percent to 40,621 in August 2009. While the total number of malware infected computers decreased slightly, more than 48 percent of the total sample of scanned computers were infected. According to AWPG, the U.S. leads in phishing sites, with 75.76 percent of sites originating in the U.S. Hong Kong is a distant second with 6.49 percent, and China is third with 3.44 percent of sites. The report may be accessed at http://www.antiphishing.org/reports/
IC3 REPORT: RISE IN ONLINE CRIME COMPLAINTS

The Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center, issued its 2009 annual report, finding that 336,655 complaints of online crime were filed last year, a 22.3 percent increase from 2008. Financial losses associated with online fraud also rose substantially, doubling from $265 million in 2008 to $559.7 last year. The report noted that the District of Columbia, 116 per 100,000 population), Nevada (106.73), Washington (81.33), Montana (68.2), Utah (60.22) and Florida (57.28) had the highest per capita rate of Internet crime perpetrators in the U.S. The majority of reported perpetrators were in the U.S., although many were also from the United Kingdom, Nigeria, Canada, Malaysia and Ghana. The number one offense last year involved advanced fee scams using the FBI’s name (16.6 percent) followed by non-delivery of merchandise and/or payment (11.9 percent). Additional popular scams last year included hitman scams, an email extortion scheme in which the victim receives an email from a member of an organization such as the “Ishmael Ghost Islamic Group” threatening to assassinate the victim and the victim’s family; and astrological reading frauds, in which the victim receives an email offering free astrological readings after providing his/her birth date and location, after which the victim is enticed to purchase a full reading with the promise that something favorable is about to happen, although the victim gets neither the reading nor something favorable. The full report can be accessed at http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

STUDY RANKS RISKIEST PLACES TO BE ONLINE

A joint study by Symantec and research firm Sperling’s Best Places resulted in a list of the 50 riskiest places in the U.S. to be online. The rankings were determined through a combination of data from Symantec Security Response and third party data about online behavior, such as accessing WiFi hotspots and online banking. Each city was scored across several categories, such as the number of malicious attacks per capita, prevalence of Internet use and the number of bot-infected machines per capita. Seattle was the only city in the study to be in the top 10 in each category. Researchers also listed Boston, San Francisco and D.C. high in part due to the large number of WiFi hotspots, although Boston and D.C. both scored high in the area of cybercrimes per capita as well. Raleigh finished high primarily due to the high percentage of residents with Internet access who participate in online activities. The top 10 list also included Atlanta; Minneapolis; Denver; Austin, Texas; and Portland, Oregon. According to the research, Atlanta residents experience the most cyber-attacks and potential infections, while Minneapolis and Portland are included for risky online behavior. Denver and Austin scored high across the board, according to the study. Of the 50 U.S. cities studied, Detroit was the least risky online city, with residents found to be less likely to participate in risky online behavior. Detroit also ranked low in cybercrime, wireless Internet access and Internet access compared with other cities. El Paso, Texas and Memphis were second and third safest cities, respectively. The complete list can be accessed at http://www.symantec.com/about/news/release/article.jsp?prid=20100322_01.
DEFENSE DEPARTMENT OKS SOCIAL MEDIA ACCESS

The U.S. Defense Department issued a memo-
randum which makes it official policy that its non-
classified network will be configured to provide ac-
cess to Internet-based capabilities across all compo-
nents, including combat branches. It thus allows
employees to use social networking services and
other interactive Web 2.0 applications, although
military personnel will still be expected to refrain
from conduct that could compromise military actions
or undercut readiness. The Department stated that
it will continue to prevent malicious activity on mili-
tary information networks, deny access to prohibited
content sites, such as gambling, pornography and
hate crime related sites, and take immediate action
where necessary. A factor in the decision to permit
access is the recognition that social networks are
useful tools for different agencies to interact with
other agencies as well as with the public. The policy
can be accessed at http://www.defense.gov/NEWS/
DTM%2009-026.pdf.

REPORT LISTS SEVEN CLOUD COMPUTING SECURITY RISKS

Seven types of security risks in cloud computing
that can be intensified by its openness and scale of
services have been identified, according to a study
conducted by the Cloud Security Alliance. First is
misuse of cloud computing, where the cloud itself is
used to host attacks. The report noted that clouds
have been infected with malware, and because peo-
ple can access services with only a credit card or
even with a free trial, criminals are able to send
spam and spread malware anonymously. To help
prevent misuse, the study recommends stricter reg-
istration and validation, better credit card fraud de-
tection and data traffic monitoring. Another problem
is unsecured application program interfaces (APIs)
which can contain exploitable loopholes. Here, the
study suggests closer analysis of API security as well
as strong authentication, access controls and en-
cryption. The third risk concerned malicious insiders
which is exacerbated with cloud services because of
lack of control over who the cloud vendor hires. An-
other area of concern is shared technology. The re-
port noted that in an environment where multiple
virtual servers have the same configuration, a mis-
configuration or bug can be replicated across a
cloud infrastructure. The report’s solution was that
companies should ensure that their cloud vendor
follows best practices for network and server con-
figuration and should enforce service level agree-
ments for patch management and vulnerability
remediation. A fifth concern that is magnified in the
cloud is data leakage. Another concern listed was
account or service hijacking, and the study recom-
mended two-factor authentication and proactive
monitoring to detect unauthorized activity. Lastly,
there is the threat of the unknown. The full report
can be accessed at http://
www.cloudsecurityalliance.org/topthreats/
csatreats.v1.0.pdf.

BAN ON TEXTING WHILE DRIVING PROPOSED

The U.S. Transportation Department proposed a
ban on text messaging while driving for interstate
truck and bus drivers. The proposal would make
permanent an interim ban announced in January.
Truck and bus drivers who violate the law could face
civil or criminal penalties of up to $2,750. Federal
Motor Carrier Safety Administration research shows
that drivers who text take their eyes off the road for
an average of 4.6 seconds out of every six seconds
while doing so. At 55 miles per hour, that means
that the driver is traveling the length of a football
field, including the end zones, without looking at the
Drivers who text were shown to be 20 times more likely to get into an accident than non-distracted drivers. Currently, 20 states and the District of Columbia ban texting for all drivers, according to the Governors Highway Safety Association, and another nine states ban texting for novice drivers.

**FTC SEEKS COMMENTS ON COPPA RULES**

The Federal Trade Commission (FTC) is asking for comments on whether changes are needed to the rules imposing requirements on web sites directed at children, including a mandate that they obtain parental consent before collecting personal information from children under 13 years of age. In a Federal Register notice, the FTC stated that the Children’s Online Privacy Act (COPPA), which became effective in 2000, requires a review of the rules every five years. While no changes were made in 2005, the FTC said it now “believes that changes to the online environment over the past five years, including but not limited to children’s increasing use of mobile technology to access the Internet, warrant reexamining the rule at this time.” In addition to parental consent, the current rules under COPPA also require web sites aimed at children under 13 to secure the information they collect from children and bars them from requiring children to provide more information than is “reasonably necessary to participate” in activities provided on the site. Comments are due June 30, and the FTC is asking for specific input on such issues as whether the definition of “Internet” should be expanded to include mobile communications, interactive television and gaming and other activities and whether the definition of “personal information” also should be expanded to include persistent IP addresses, mobile geolocation data or information used to target ads at specific Internet users. The FTC is also seeking comment on whether changes should be made to the requirements that information be kept secure and private; the requirement that allows parents to review or delete personal information about their children; and on the provision barring the linking of participation in activities on a children’s web site to the collection of personal information. The Federal Register notice can be accessed at [http://edocket.access.gpo.gov/2010/2010-7549.htm](http://edocket.access.gpo.gov/2010/2010-7549.htm).

**HELPFUL GUIDES AND WRITINGS**

**Internet Safety**

“Net Cetera: Chatting with Kids About Being Online” is a free guide that provides parents with practical recommendations to help them talk with their children about the hazards of navigating online. The guide was published by the Federal Trade Commission, and includes detailed information designed to reduce online risks. It can be accessed at [http://www.onguardonline.gov/pdf/tec04.pdf](http://www.onguardonline.gov/pdf/tec04.pdf).

**Computer Search and Seizure**

Professor Orin Kerr of George Washington University posted a draft article, Ex Ante Regulation of Computer Search and Seizure, to be published in the Virginia Law Review. He states that the article is a response to “dynamics that have been evolving over the last decade in the lower courts that were turned up to eleven by the Ninth Circuit’s en banc decision in United States v. Comprehensive Drug Testing. The abstract follows:
“In the last decade, magistrate judges around the United States have introduced a new practice of regulating the search and seizure of computers by imposing restrictions on computer warrants. These ex ante restrictions are imposed as conditions of obtaining a warrant: Magistrate judges refuse to sign warrant applications unless the government agrees to the magistrate’s limitation on how the warrant will be executed. These limitations vary from magistrate to magistrate, but they generally target four different stages of how computer warrants are executed: the on-site seizure of computers, the timing of the subsequent off-site search, the method of the off-site search and the return of the seized computers when searches are complete.

This Article contends that ex ante restrictions on the execution of computer warrants are constitutionally unauthorized and unwise. The Fourth Amendment does not permit judges to impose limits on the execution of warrants in the name of reasonableness. When such limits are imposed, they have no legal effect. The imposition of ex ante limits on computer warrants is also harmful: Ex ante assessments of reasonableness in ex parte proceedings are highly error-prone, and they end up prohibiting reasonable practices when paired with ex post review. Although ex ante restrictions may seem necessary in light of the present uncertainty of computer search and seizure law, such restrictions end up having the opposite effect. By transforming litigation of the lawfulness of a warrant’s execution into litigation focusing on compliance with restrictions rather than reasonableness, ex ante restrictions prevent the development of reasonableness standards to be imposed ex post that are needed to regulate the new computer search process. Magistrate judges should refuse to impose such restrictions and should let the law develop via judicial review ex post.”

JOB OPENING: Law Fellow

The National Center for Justice and the Rule of Law at the University of Mississippi School of Law has an opening for the position of Law Fellow. The Center will fill that opening on a temporary basis, as a one or two year fellow.

The successful candidate will be given the opportunity to acquire experience and skills in Cyber Crime and the Fourth Amendment (search and seizure). The primary focus is to conduct legal research, write articles, and prepare materials in those two areas. The Fellow will also assist with planning for conferences, prepare web based, and other technology based instructional and informational materials.

The Center has two initiatives that produce approximately 12 conferences each year. The Center’s Cyber Crime Initiative develops educational programs targeting computer-related crime. The Center’s Fourth Amendment Initiative promotes awareness of search and seizure principles through conferences, judicial and prosecution training, and support for selected publications.

Applicants must have a J.D. degree from an ABA-accredited school. Preferred accomplishments include an interest or experience in Cyber Crime and the Fourth Amendment (search and seizure).

For more information about the Center, please visit our website at www.NCJRL.org. The University of Mississippi is an EEO/AA/Title VI/Title IX/Section 504/ADA/ADEA employer. All applicants must formally apply on line at https://jobs.olemiss.edu/. Applicant must submit a cover letter, resume, and writing sample. The position will remain open until filled.