News Highlights in This Issue:

ICAC Funds Awarded to Five AGs
Ohio Pornography Statute Struck Down in Part
Cert Denied in Defective Floppy Disk
Internet Access Tax Ban Extended to 2014
Rise in E-Mails Linking to Malicious Sites
Publication on Investigators’ Tools Available
Utah Court: Jury Instruction in Porn Case OK
New Jersey: Offender Net Access Restricted
Odds of Landing on Typosquatting Site: 1 in 14
Save the Date for Cybercrime Training
Search Engine Not Liable for Query Results
High Court Declines Remote Access Case
House Passes Internet Safety Education Bill
Survey: 8.3 Americans Are ID Theft Victims
Pay-Per-Click Ads Convey Jurisdiction
House Bill Requires 911 Access by VoIP Providers
Foreign Government Increase Blogger Attacks
Web Site Terms of Use Enforceable if Known
Senate Passes Bill to Help ID Theft Victims
Online Database of Threats to Speech Available

Table of Contents

Features
Five AGs Awarded ICAC Grant
Cybercrime Training Announced

AGs Fighting Cyber Crimes
AG Blumenthal Sues Database Developer
FL AG: Pornographer Gets 15 Years
AG Bennett Says Offender Pled Guilty
Illinois AG Offers Cyberbullying Training
AG Gansler Gets Cyber Awards
Massachusetts AG Host Cyber Training
AG Cox’s Office Arrests Online Predator
Mississippi AG Says Offender Sentenced
AG Ayotte Delivers Net Safety Guide
New Mexico AG Arrests Pornographer
AG Dann Awarded Internet Safety Funds
Oklahoma AG Charges eBay Seller Fraud
AG Corbett’s Unit Arrests Predator
South Carolina AG: Sting Gets Predator
AG Abbott Sues Web Sites for Children
Washington AG Sues Web Marketer

In the Courts
Ohio Pornography Law Struck Down
Anti-Child Obscenity Law is Overbroad
Jury Instruction in Child Porn Case OK
Search Engine Not Liable for Query Results
Web Site Terms of Use Enforceable
Two Opinions on Attorney-Client E-Mails
Responder Bears Costs of E-Discovery
Personal Liability for Deceptive E-Mails

In the Supreme Court
Cert Denied in Defective Floppy Disk Case
No Review of Remote Computer Access Case
Adult E-Magazine Piracy Appeal Fails

Legislation Update
Internet Tax Ban Extended to 2014
House Bill Would Set Up National ICAC
Expanded Online Child Crimes Bill Passed
House Passes Child Pornography Bill
Bill Would Require ISPs to Report Porn
House Passes Net Safety Education Bill
New Jersey Curbs Offender Net Access
House OKs Offender Monitor Training
Sex Offender Registration Bill Passes
Grants to Aid Registration Bill Introduced
Broadband Inventory Bill Passes House
Bill Would Require 911 of VoIP Providers
Senate Passes Bill for ID Theft Victims
Online Freedom of Speech Bill Moves

News You Can Use
Database of Threats to Net Speech Posted
E-Mails With Malicious Link Increase
Plan Issued for Fair Use of Filtering
ICANN Committee OKs Database Studies
Blogger Repression Rising Overseas
Typosquatting Report Online Risks
Board Advises Expanding Rural Wireless
Study: Internet Use May Exceed Capacity
More Than 8 Million Are ID Theft Victims
Online Library Has 1.5 Million Books

Tools You Can Use
Tools for Investigators Resource Available
Child Exploitation Research Downloadable
FIVE ATTORNEYS GENERAL RECEIVE ICAC FUNDS

The U.S. Department of Justice announced that five Attorney General offices are among the 13 new state and local law enforcement agencies to receive more than $3 million in funding to form Internet Crimes Against Children (ICAC) task forces in their regions. Those Attorney General offices are: Delaware, Idaho, Mississippi, North Dakota and South Dakota. Each office received an initial $250,000, enabling them to play a critical role in stopping Internet criminal activity targeting children. With the new grants, there will be a total of 59 ICAC task forces nationwide.

AGs FIGHTING CYBER CRIMES

CONNECTICUT

Attorney General Richard Blumenthal sued Maximus Inc., a Virginia company, for failure to provide a timely and complete upgrade of a major law enforcement database in accordance with their contract with the state. In 2003, the state signed a $8.3 million contract with the company to make Connecticut Online Law Enforcement Communications Teleprocessing (COLLECT) comply with federal standards, as well as make it more user-friendly. State officials have found more than 800 defects and inferior performance in the system, and the suit seeks to recoup the $6 million in payments made to Maximus to date and return the funds to the Department of Public Safety.
FLORIDA

Attorney General Bill McCollum announced that Joseph Bass was sentenced to 15 years in prison after pleading guilty to multiple charges of possession of child pornography. Bass was arrested after Attorney General McCollum’s CyberCrime Unit investigators, who were conducting an Internet investigation, discovered his collection of pornographic videos. He was prosecuted by Attorney General McCollum’s Office of Statewide Prosecution. Bass must also serve five years of sex offender probation after his prison term and must register as a sex offender.

HAWAII

Attorney General Mark Bennett announced that Marc Fossorier pled guilty to one count of electronic enticement of a child in the first degree. Fossorier asked a special agent from Attorney General Bennett’s office, who he thought was a 15-year-old girl, to meet him for sex. He was arrested when he showed up at the meeting place by law enforcement agents from the Hawaii Crimes Against Children Task Force, including Attorney General Bennett’s Office, the Honolulu Police Department, the Federal Bureau of Investigation, the U.S. Immigration and Customs Enforcement and the Naval Criminal Investigative Service. Fossorier faces a maximum sentence of 10 years in prison with a minimum sentence of five years probation with a one-year prison term as a condition of probation. He must also register as a sex offender.

ILLINOIS

Attorney General Lisa Madigan’s office will offer a cyberbullying training program for junior high and high school personnel beginning in January 2008. The 90-minute program will cover what cyberbullying is, how it happens and how educators can recognize the signs and take action to thwart the practice. The announcement of the program was made at the annual Internet Crimes Against Children (ICAC) task force meeting, which Attorney General Madigan attended.

MARYLAND

Attorney General Douglas Gansler received the University of Maryland’s CyberEthics, CyberSafety and CyberSecurity (C3) Award in recognition of his Internet safety efforts. Under his Community Leadership in Cyber Knowledge and Safety (C.L.I.C.K.S) initiative, Attorney General Gansler partnered with the NetSmartz Workshop to conduct regional Train the Trainer sessions to create a network of community leaders able to talk to children and parents about Internet safety. He also partnered with experts in law enforcement, education and Internet safety to extend the reach of the C.L.I.C.K.S. initiative.

Note: The Editor thanks Raquel Guillory, Director of Communications in the Maryland Attorney General’s Office, for this information.

MASSACHUSETTS

Attorney General Martha Coakley, in collaboration with the Microsoft Corporation, hosted a one-day cybercrime training session for state law enforcement. “Cybercrime 101” was attended by more than 300 law enforcement officers from the State Police and other police departments, including college and university police departments. During the training, Microsoft staff presented sessions designed to help law enforcement officers transfer traditional investigative techniques to the technological sphere. The training is a part of Attorney General Coakley’s Cybercrime Initiative.

MICHIGAN

Attorney General Mike Cox joined the Michigan State Police to announce the arrest of Matthew Beaujean, a former Michigan resident now living in Alaska, for using the Internet to solicit a minor for sexual acts and sending a minor pornographic images. The complaint alleges that Beaujean, before moving to Alaska, had been communicating with an undercover agent from the Michigan Internet Crimes Against Children Task Force posing as a 13-year-old girl. Beaujean was arrested by Alaska State Police on a fugitive
warrant, which was based on a Michigan felony warrant. Since Beaujean refused to waive extradition, Attorney General Cox will begin extradition proceedings.

**MISSISSIPPI**

Attorney General Jim Hood announced the sentencing of John Argo IV on charges that stemmed from a child pornography investigation conducted by Attorney General Hood’s Cyber Crime Unit. Argo, who was convicted on 14 counts of Exploitation of a Child, received 20 years on each count, with five suspended, 15 to serve and all to run concurrently. He also must pay $1,000 to the Crime Victims Compensation Fund. Argo will then have a five-year supervised probation period and must register as a sex offender. Under the terms of his probation, he cannot use the Internet except for work purposes, and his usage will be monitored by Attorney General Hood’s Office. The investigation, forensic analysis and prosecution were all handled by Attorney General Hood’s Public Integrity Division.

**NEW HAMPSHIRE**

Attorney General Kelly Ayotte joined Governor John Lynch and Commissioner of Education Lyonel Tracy to announce the delivery of more than 105,000 copies of the “Internet Safety Guide” for teens in grades six through 10 in public middle and high schools and their parents across the state. The guide provides information on the risks involved in posting personal information online, as well as resources for parents to keep their kids safe. The guide can also be downloaded from Attorney General Ayotte’s cybercrime prevention web site, connectwithyourkids.org.

**NEW MEXICO**

Attorney General Gary King’s Internet Crimes Against Children (ICAC) Unit, in cooperation with the State Police, arrested Patrick O’Hara and his son, Timothy O’Hara, on multiple charges of possession and distribution of child pornography. The elder O’Hara is charged with 50 counts of child pornography distribution, a third degree felony, and 20 counts of possession of child pornography, a fourth degree felony, and could receive as must as 180 years in prison. His son is charged with 20 counts of possession of child pornography and could receive 60 years in prison. The investigation was the result of a tip from the National Center for Missing and Exploited Children.

**OHIO**

Attorney General Marc Dann announced that the Verizon Foundation awarded a $30,000 grant to the partnership between his office and i-SAFE Inc, a non-profit Internet safety organization, to contribute to their Internet safety initiatives. Those initiatives include the Assembly Experience, a multi-media presentation that encourages kids to spread the word about Internet safety, and the “Safer Surfer City Tour,” a campaign to educate and empower parents and law enforcement against Internet predators.

**OKLAHOMA**

Attorney General Drew Edmondson filed charges against Chelsey Davis for allegedly defrauding consumers in five states using eBay. Davis collected more than $10,000 for silver bars and coins he advertised on eBay, but he never sent the merchandise to buyers. He faces eight felony charges and one misdemeanor count for violating the state Consumer Protection Act. In addition to the Oklahoma victims, five of the victims are from California and the rest are from Arizona, Georgia, New York and Texas.

**PENNSYLVANIA**

Attorney General Tom Corbett’s Child Predator Unit agents, assisted by Schuykill Haven police, arrested Michael Deane, the operator of a music DJ and karaoke business, on allegations of using Internet chat rooms to sexually proposition what he believed to be a 14-year-old girl, but was actually a Unit undercover agent, as well as sending sexually explicit photos and web cam images to the
“girl.” Unit agents also executed a search of Deane’s home, seizing six computers, a web cam and several data storage devices to be analyzed by Attorney General Corbett’s Computer Forensics Unit. Deane is charged with four counts of unlawful contact with a minor and one count of criminal use of a computer, all third degree felonies that are each punishable by up to seven years in prison and $15,000 fines. Deane will be prosecuted by Deputy Attorney General Michael Sprow of the Unit.

SOUTH CAROLINA

Attorney General Henry McMaster announced the arrest of Santos Azaredo during an undercover Internet sting conducted by the Spartanburg County Sheriff’s Office, a member of Attorney General McMaster’s Internet Crimes Against Children Task Force, with the assistance of the Horry County Sheriff’s Office. Arrest warrants allege that Azaredo solicited sex on the Internet from what he believed to be a 13-year-old girl, but was actually a sheriff’s deputy. He was arrested on two counts of Criminal Solicitation of a Minor, a felony punishable by up to ten years imprisonment on each count. Azaredo’s mother consented to the seizure of a laptop computer from his residence. Azaredo will be prosecuted by Attorney General McMaster’s Office.

TENNESSEE

Attorney General Greg Abbott filed suit against TheDollPalace.com and Gamesradar.com, two web sites that cater to children but allegedly fail to adequately protect their privacy and safety. The suit makes Texas the first state to file an action under the Children’s Online Privacy Protection Act (COPPA), a federal law prohibiting web sites from unnecessarily collecting personal information from children under age 13. According to Attorney General Abbott’s investigators, both sites fail to include required disclosures and fail to obtain parental consent before collecting personal information from children. The sites also allow children to access potentially inappropriate content in chat rooms and interactive forums.

Ed. Note: The Editor thanks Paul Singer, Assistant Attorney General, Office of the Attorney General of Texas, for the above information.

WASHINGTON

Attorney General Rob McKenna sued Internet Advancement, a search engine marketing services company, for allegedly misrepresenting its services, failing to honor its guarantees on refunds and making unauthorized charges to customers’ credit cards. The company, which also does business as 4GreatBuys.com, claims that it can make a company’s web site appear in the top 25 results of search engines’ queries, but the suit claims it does not make good on its claim. The company charges between $999 to $3,000 as a set-up fee, as well as $149 in monthly charges. The state had previously settled similar charges with the company in 2004, but had received 60 complaints about them in the past three years.

IN THE COURTS

FIRST AMENDMENT: CHILD PORNOGRAPHY STATUTE

American Booksellers Foundation for Free Expression v. Strickland, 2007 WL 2783678 (S.D. Ohio September 24, 2007). The U.S. District Court for the Southern District of Ohio ruled that parts of an Ohio statute banning the Internet exchange of explicit material were overbroad in violation of the First Amendment. The Media Coalition, a trade association that includes the National Association of Recording Merchandisers, the American
Booksellers Foundation for Free Expression and the Association of American Publishers, asked the court to permanently enjoin the enforcement of Ohio Revised Code § 2709.31(D)(1) and § 2709.01(E), as amended by House Bill 490, on the grounds they were unconstitutionally vague and overbroad in violation of the First and Fourteenth Amendments. The laws generally mandate that no person shall disseminate or offer to disseminate to a juvenile any material that is “harmful to juveniles.” The amended § 2709.01(E) defines “harmful to juveniles” as any material that describes or represents nudity, sexual contact, sexual excitement or sadomasochistic abuse that either appeals to the interest of a juvenile, would be offensive to prevailing standards of what is suitable for juveniles or has no literary or artistic value. The amended §2709(D) states that a person electronically disseminates material under this provision if he or she has reason to believe that the person receiving the information is a juvenile. The court found that while the definition of “harmful to juveniles” did not by itself violate the First Amendment, applying it to the Internet on a “reason to believe” standard was overly broad. As an example, sexually explicit conversations in adult-only chat rooms could be prosecuted if a minor was secretly present. Consequently, the court found that § 2709.31(D)(1) was unconstitutionally broad and violated the First Amendment and issued an injunction, but § 2709.01(E) did not violate the Constitution.

FIRST AMENDMENT: CHILD PROTECTION AND OBSCENITY ENFORCEMENT ACT

Connection Distributing Co. v. Keisler, 2007 WL 3070970 (6th Cir. October 23, 2007). The Sixth Circuit held that the recordkeeping requirements of the Child Protection and Obscenity Enforcement Act, 18 U.S.C. §2257, are overbroad in violation of the First Amendment. The statute’s intent is to combat child pornography by imposing recordkeeping requirements on “producers” of “actual sexually explicit conduct.” “Producers” broadly included anyone who creates, or uses such images to publish, reproduce or reissue them for commercial purposes or anyone who uploads them to a web site. Some of the recordkeeping requirements mandated by the statute were: making a copy of a government-issued picture id and recording the name and date of birth of everyone depicted in an image; making a copy of the image and recording where it is published and when it was produced; recording where the records relating to the image are published and making the records available for inspection by the U.S. government. Connection Distributing Co., publisher of several “swingers” magazines, filed a declaratory action, asking for an injunction against enforcement of the recordkeeping requirements. The U.S. District Court for the Northern District of Ohio granted summary judgment for the government. On appeal, the Sixth Circuit reversed, finding that the statute was overbroad and significantly affected protected speech, including images of adults kept in one’s home. It also found that the recordkeeping requirements were burdensome and led to a significant chilling effect. The court remanded the case to the district court with instructions to enter summary judgment for Connection Distributing.
ONLINE CHILD PORNOGRAPHY: JURY INSTRUCTIONS

State of Utah v. Alinas, No. 20051000 (Utah October 26, 2007). The Utah Supreme Court ruled that a jury instruction defining child pornography as “any visual depiction” of a minor engaging in sexually explicit conduct, including “computer-generated” depictions, does not violate Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002). Lexis Alinas was seen looking at a web site called “Little Girls Extreme” by a librarian at the University of Utah library. University police spoke with Alinas and confirmed that she had been viewing child pornography. She was arrested and searched, resulting in a finding of two floppy disks containing images of nude children in her coat pocket. Alinas was charged with seven counts of sexual exploitation of a minor, and a jury convicted her on all counts. On appeal, Alinas argued that the single jury instruction which required the jury, in order to convict, to find that Alinas knowingly possessed child pornography, as defined above, was invalid because a jury could conceivably convict a person for possession of “virtual child pornography,” which Ashcroft bans. The court disagreed with this argument, finding that the jury instruction clearly required that the jury find the images to be actual conduct. The decision was affirmed.

Ed. Note: The case for the state was argued by Kenneth Bronston, Assistant Attorney General, Office of the Attorney General of Utah.

COMMUNICATIONS DECENCY ACT: LIABILITY

Murawski v. Pataki, 2007 U.S. Dist. LEXIS 72749 (S.D.N.Y. September 26, 2007). The U.S. District Court for the Southern District of New York refused to hold an Internet search engine liable for material it produced in response to a user’s query when only the spacing differed from the original source of the material. William Murowski, a political candidate, brought an action against Yahoo! Inc. for refusing to post his e-mails to their message boards, and against IAC/Interactive Corp., the owner of Ask.com, to remove from their directory a web site that made it appear in their search results that he was a member of the Communist party. The court granted summary judgment for both defendants. It found that Yahoo! was a private entity with no obligation to uphold First Amendment freedom of speech rights. It also found that IAC was protected by the Communications Decency Act, which immunizes “interactive computer services,” including search engines such as Ask.com, from liability arising from third party content.

WEB SITE TERMS OF USE: KNOWLEDGE

Southwest Airlines Co. v. BoardFirst, LLC, No. 06-0891 (N.D. Tex. September 12, 2007). The U.S. District Court for the Northern District of Texas ruled that web site terms of use are enforceable against a user with notice of them. BoardFirst went into business to help Southwest passengers obtain the coveted “A” boarding passes, which are given to the first 45 passengers to check in and therefore board first. A customer authorizes BoardFirst to act as the customer’s agent, and when boarding passes become available, BoardFirst logs onto southwest.com and tries to obtain an “A” boarding pass for the customer. If BoardFirst is successful, it collects a $5 fee from the customer. Southwest sent cease and desist letters to BoardFirst
without result, so it sued the company for breach of contract, violation of the Computer Fraud and Abuse Act and violation of a Texas statute prohibiting harmful access to a computer. The court found that BoardFirst had breached the parties’ “browsewrap agreement,” which is an agreement between a web site owner and a user when the user accesses the site after receiving actual or constructive knowledge that access constitutes acceptance of the site’s terms and conditions. One of the terms and conditions on Southwest.com’s home page was that site use was only allowed for “personal, non-commercial purposes,” and BoardFirst had actual knowledge of this condition from the cease and desist letters. The court added that BoardFirst’s authorization to act for its customers did not make its actions any less of a violation.

*Ed. Note: This opinion is significant because many courts have declined to enforce web site terms and conditions.*

### E-DISCOVERY: PRIVILEGED E-MAILS

*Sims v. Lakeside School*, 2007 WL 2745367 (W.D. Wash. September 20, 2007). The U.S. District Court for the Western District of Washington has found that web-based e-mails between attorney and client are privileged, notwithstanding an employer’s right to inspect an office laptop’s contents. In an employment discrimination case, Lakeside Schools sought an order allowing the review of a hard drive image of a laptop computer furnished to plaintiff Chance Sims while he was employed at Lakeside. Sims objected to the imaging because the hard drive also contained communications with his attorney. The court granted the motion in part and denied it in part. The court found that Sims had no reasonable expectation of privacy in the contents of the laptop because Lakeside’s employee manual was unequivocally clear that user accounts were the property of Lakeside School. However, the court also ruled that web-based e-mails generated by Sims, and any materials he created to communicate with his attorney, were protected under the attorney-client privilege. Accordingly, the court ruled that Lakeside was entitled to review the contents of Sims’ hard drive, but was not allowed to review any e-mails or material used to communicate with his attorney. The court ordered an expert to review and separate the contents accordingly.

But see a different result on similar facts…

*Scott v. Beth Israel Medical Center, Inc.*, 2007 WL 3053351 (N.Y. Sup. October 18, 2007). In this case, Dr. Norman Scott sued his former employer, Beth Israel Medical Center, for breach of contract. While an employee, Scott had communicated with his attorneys regarding the suit using the Center’s e-mail system. Learning that the Center had obtained copies of these e-mails, Scott moved for a protective order seeking their return, arguing that he had an expectation of privacy in the e-mails and that they were protected under the attorney-client privilege. The Center argued that the attorney-client privilege never attached, since Scott knew or should have known their policy which clearly stated that there was no expectation of privacy for e-mails sent or received using their system. The New York Supreme Court, County of New York, relying heavily on the Center’s e-mail policy, ruled in favor of the Center and denied Scott’s request for protection.
E-DISCOVERY: COSTS

PSEG Power New York, Inc. v. Alberici Constructors, Inc., 2007 WL 2687670 (N.D.N.Y. September 7, 2007). The U.S. District Court for the Northern District of New York ordered a party to reproduce documents at its own cost when its original production of documents was unusable. In a breach of contract case, defendant Alberici Constructors asked for production of all electronically stored e-mails with their attachments. In response, plaintiff PSEG Power produced a disc of the e-mails, but due to a technical glitch, the attachments were separate from the e-mails. Efforts to put the e-mails and their proper attachments together failed, and Alberici moved for a second production at PSEG Power’s expense. PSEG argued that a second production would be overly costly and burdensome, but agreed to produce it at Alberici’s expense. The court, relying on Fed. R. Civ. P. 34(b), found that the original production was unusable and ordered PSEG Power to reproduce a second. It also ordered PSEG Power to bear the cost since the responding party presumptively bears the cost of production.

JURISDICTION: PAY-PER-CLICK ADS

Chicago Architectural Foundation v. Domain Magic, LLC, 2007 WL 3046124 (N.D. Ill. October 12, 2007). The U.S. District Court for the Northern District of Illinois held that pay-per-click advertisements on a web site make the site sufficiently interactive to convey jurisdiction. Chicago Architecture Foundation (CAF), founded in 1966, sold tours and books about Chicago’s architecture on the Internet at www.architecture.org. In February 2006, Domain Magic, LLC, a Florida company, registered the domain name www.chicagoarchitecturefoundation.org on which it provided links to businesses that offered tours of Chicago, in direct competition with CAF. CAF sued in Illinois for trademark infringement, and Domain Magic filed a motion to dismiss for lack of personal jurisdiction on the basis that they had not conducted business in the court’s jurisdiction. Although Domain Magic’s web site was primarily informational, the court noted that the company received payments based on the number of clicks on each link, thus often profiting from the “hits” it receives from people looking for information about CAF. Applying the standard set forth in Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F.Supp. 1119 (W.D. Pa. 1997), the court ruled that Domain Magic’s actions satisfied the Illinois Long-Arm statute because it had profited from clicks on its hyperlinks, and the company knew or should have known that CAF would suffer injury in Illinois. The motion to dismiss was denied.

Ed. Note: If this decision were more widely followed, the result would be a major move toward universal jurisdiction of online businesses for courts.

DECEPTIVE E-MAILS: PIERCING THE CORPORATE VEIL

John W. Ferron v. Search Cactus, LLC, 2007 U.S. Dist. LEXIS 44472 (S.D. Ohio June 19, 2007). The U.S. District Court for the Southern District of Ohio held that individual corporate officers can be held personally liable for violations of the Ohio Consumer Sales Practices Act (OCSPA) arising out of the transmission of allegedly misleading and deceptive promotional e-mails. John Ferron, an Ohio lawyer, sued Search
Cactus alleging that the company sent him misleading and deceptive e-mails offering “free products” without adequately disclosing the conditions attached to claiming the products, in violation of O.R.C. § 1.345.02(A). The suit also named two corporate officers of Search Cactus who Ferron alleged had approved all of Search Cactus’ e-mail advertisements. The corporate officers moved to dismiss, arguing that they could not be held liable for Search Cactus’ acts unless Ferron could pierce the corporate veil and prove that Search Cactus was their “alter ego.” The district court rejected this argument, holding that a corporate officer could be personally liable for OCSPA violations if the officer took part, directed, participated or cooperated in the act, such as was alleged in the complaint. The motion to dismiss was denied.

IN THE SUPREME COURT

Since the last issue of this e-newsletter, the U.S. Supreme Court has denied review of several computer-related cases. Below is a summary of those cases.

**Compaq Computer Corp v. Grider, No. 07-95.** The Supreme Court refused to intervene in a class action lawsuit against Compaq Computer, now part of Hewlett-Packard, over allegedly defective floppy disk drives. The company’s appeal challenged the Oklahoma Supreme Court’s acceptance of a 1.7 million nationwide member class of Compaq computer purchasers, arguing that the Oklahoma court wrongly certified a nationwide class. Compaq also argued that a similar lawsuit was brought in Texas in 2000, and the Texas Supreme Court refused to certify a class action, ruling that Texas law shouldn’t apply to out-of-state class members. The case now goes back to the Oklahoma Supreme Court for additional proceedings.

**Heckenkamp v. United States, No. 07-496.** On November 13, the Court declined review of a Ninth Circuit Court of Appeals ruling affirming the federal hacking conviction of a state university student whose personal computer in his dorm room was remotely accessed by university officials without a warrant. The issue in the case was whether a remote search of computer files on a hard drive by a network administrator was justified under the “special needs” exception to the Fourth Amendment. Jerome Heckenkamp, a student at the University of Wisconsin (UW) at Madison, who had been terminated from work at the computer department because of his unauthorized computer activity, tried to hack into Qualcomm, a California corporation. At Qualcomm’s request, the UW systems administrator traced the intrusion to Heckenkamp’s dorm room and disconnected the network cord from the computer. Heckenkamp authorized the administrator to make a copy of his hard drive. A search warrant was issued the
next day, under which his computer was seized. Heckenkamp moved to suppress the evidence gathered from the remote search of his computer, as well as from the image of his hard drive and the seizure of his computer. The Ninth Circuit found that while students have a constitutionally protected reasonable expectation of privacy in their dorm room computers, university officials can search those computers without a warrant for school security purposes under the “special needs” exception.

**Perfect10 Inc. v. CCBill LLC, No. 07-266.** The court refused to consider an appeal by Perfect10 Inc., an online publisher of an adult magazine, claiming that credit card companies were enabling the piracy of its pictures of nude models. The company had sued two credit card intermediary companies, CCBill LLC and CWIE, accusing them of enabling copyright infringement and violating California trademark law by providing online credit card billing and web site hosting services to the pirate sites. The Ninth Circuit Court of Appeals ruled that both companies were shielded from liability under the Digital millennium Copyright Act and the Communications Decency Act.

---

**LEGISLATION UPDATE**

**Internet Taxes**

**ENACTED.** H.R. 3678, legislation extending the ban on state and local taxes on Internet access or commerce until November 1, 2014 has been signed into law. This is the third time the ban has been extended since it was first enacted in 1998.

**Internet Crimes Against Children**

**PASSED HOUSE.** On November 14, the U.S. House of Representatives (House), by a vote of 415-2, passed H.R. 3845, a bill establishing a Special Counsel for Child Exploitation Prevention and Interdiction within the Office of the Deputy Attorney General. The bill, sponsored by Representative Debbie Wasserman Schultz (D-FL), also establishes, with the Department of Justice, a National Internet Crimes Against Children (ICAC) Task Force consisting of state and local task forces. The bill establishes a National ICAC Data Network Center to assist task forces with the investigation and prosecution of child exploitation. The bill authorizes appropriations for these programs from 2009-2016, as well as authorizes the Office of Justice Programs to provide grants to state and local ICAC task forces. Finally, it authorizes additional computer forensic capacity to address the current backlog for computer forensics. The bill has been sent to the U.S. Senate (Senate) where it has been referred to the Judiciary Committee.

**PASSED HOUSE.** That same day, the House unanimously passed H.R. 4120, a bill introduced by Representative
Nancy Boyds (D-KS), which would expand the definitions of child sexual exploitation and child pornography to include those committed in interstate and foreign commerce. The measure has been referred to the Senate Judiciary Committee.

**PASSED HOUSE.** On November 15, the House also unanimously passed H.R. 4136, a bill sponsored by Representative Christopher Carney (D-PA), which would expand the federal definition of “possess” with respect to child sexual exploitation and child pornography to include accessing visual depictions of child pornography with intent to view. It has been referred to the Senate Judiciary Committee.

**PASSED HOUSE.** On December 5, the fourth bill related to Internet crimes against children, H.R. 3791, sponsored by Representative Nick Lampson (D-TX), was passed by the House by a vote of 409-2. The bill requires Internet service providers (ISPs) to report detailed information on a suspected sex offender to the National Center for Missing and Exploited Children (NCMEC), which in turn must report the information to law enforcement authorities. ISPs would also have to preserve the images of child pornography for evidence. NCMEC would be authorized to provide images reported via its CyberTipline to ISPs to stop further transmission.

**Internet Safety**

**PASSED HOUSE.** On November 13, the House also passed, 398-6, H.R. 3461, a bill sponsored by Representative Melissa Bean (D-IL), requiring the Federal Trade Commission (FTC) to develop and carry out a nationwide program to increase public awareness and education on Internet safety. The bill has been referred to the Senate Committee on Commerce, Science and Transportation.

**Sex Offender Registration**

**NEW JERSEY.** On December 27, acting Governor Richard Cooley, who is filling in for vacationing Governor Jon Corzine, signed S. 1979 into law, a bill that allows state courts to restrict Internet access for convicted sex offenders. The law, which takes effect in 90 days, would also allow the court to impose other restrictions, including requiring the offender to submit to periodic unannounced examinations of his or her computer and/or requiring the installation of monitoring devices on the offender’s computer at the offender’s expense. The restrictions are mandatory if a computer was used in the commission of the offense. A sex offender who fails to comply is guilty of a fourth degree crime. The new law also directs the state Attorney General to approve training programs for those who will enforce it.

**PASSED HOUSE.** On November 14, the House unanimously passed H.R. 719, a bill that authorizes appropriations for 2009-2013 to purchase and train personnel on Internet filtering and monitoring programs and devices to supervise sex offenders. Sponsored by Representative Earl Pomeroy (D-ND), the bill also amends federal code to include restricted Internet access and computer monitoring as discretionary conditions of probation for sex offenders. It also imposes a fine and/or prison term of up to 20 years for participating in a financial transaction for access to or possession of child
pornography. The bill was referred to the Senate Judiciary Committee.

**PASSED SENATE COMMITTEE.** On December 3, the Senate Judiciary Committee favorably reported out S. 431, a bill sponsored by Senator Charles Schumer (D-NY) that would require sex offenders to register their e-mail and instant messaging addresses, as well as other Internet identifiers, and keep them current. Failure to register this information would result in a fine and/or prison term of up to 20 years. The bill would require the Department of Justice to maintain a system to allow social networking sites to compare their databases with the National Sex Offender Registry.

**INTRODUCED.** On November 9, Representative Peter King (R-NY) introduced H.R. 4147, which would provide grants to Parents for Megan’s Law Inc. to provide sex offender registration information to law enforcement agencies and identify sex offenders who fail to register. The bill was referred to the Judiciary Committee.

**Broadband and VoIP**

**PASSED BY HOUSE.** On November 13, the House by voice vote passed H.R. 3919, a bill sponsored by Representative Edward Markey (D-MA) that directs the Department of Commerce to develop and maintain an inventory of where broadband service is available in order to identify gaps. The bill has been referred to the Senate Committee on Commerce, Science and Transportation.

**PASSED BY HOUSE.** That same day the House also passed, 406-1, H.R. 3403, a bill that requires VoIP providers to provide 911 service to its customers. The bill, sponsored by Representative Bart Gordon (D-TN), also requires the E-911 Implementation Coordination Office to develop a national plan for migration to an IP-enabled emergency network. The bill has been referred to the Senate Committee on Commerce, Science and Transportation.

**Online Identity Theft**

**PASSED SENATE.** On November 15, the Senate unanimously passed S. 2168, sponsored by Senator Patrick Leahy (D-VT), which would allow victims of online identity theft to seek restitution from criminals for the time they spend fixing the problem or actual costs. It would also allow prosecutors to charge someone who threatens to take or release computer-based information with cyberextortion, as well as with conspiracy to commit a cybercrime. Current federal law only allows for prosecution of criminals who seek to extort companies or government agencies by explicitly threatening to shut down or damage a computer. The bill would also make it a felony to use spyware or keystroke loggers to damage 10 or more computers, even if the total damage is less than $5,000. Currently, damages of less than $5,000 are a misdemeanor. The bill has been referred to the House Judiciary Committee.

**Online Freedom of Speech**

**PASSED BY HOUSE COMMITTEE.** On December 10, the House Committee on Foreign Affairs reported out H.R. 275, sponsored by Representative Christopher Smith (R-NJ), which would declare it is U.S.
policy to promote the free flow of information via any media and to deter U.S. businesses from cooperating to effect online censorship with countries that restrict the Internet. The bill has been referred to the Committee on Energy and Commerce.

NEWS YOU CAN USE

DATABASE OF LEGAL THREATS TO ONLINE SPEECH POSTED

The Citizen Media Law Project unveiled its Legal Threats Database, a compendium of lawsuits, cease and desist letters and other legal challenges to online speech. The database is updated daily and currently contains hundreds of documents from 35 states and nine countries, with threats ranging from copyright infringement suits against bloggers to demand letters sent to social networking users. Users may input threats, comment on posted threats or search the database. The Project is jointly affiliated with the Berkman Center for Internet & Society at Harvard Law School and the Center for Citizen Media. The Legal Threats Database, which is funded by the John S. and James L. Knight Foundation, may be accessed at http://www.citmedialaw.org/database.

INCREASE IN E-MAILS WITH MALICIOUS LINKS REPORTED

The percentage of e-mails with links to malicious sites has increased tenfold since the first quarter of the year, according to a report by Messagelabs, a provider of messaging and web security products. The company said that 35 percent of the e-mail threats it now detects use embedded links to infect computers instead of the more traditional file attachments. The links take unsuspecting users directly to malware downloads or sites containing malicious java script code. In the first quarter of 2007, the percentage of such e-mails was 3.3 percent, but in the second quarter, the percentage rose to 20.2 percent. The report is available at http://www.messagelabs.com/mlireport/MLI_Report_September_03_2007.pdf.

PLAN FOR FAIR USE IN FILTERING ISSUED

A group of public interest organizations issued a six-point plan for the filtering of copyrighted content from user-generated sites. The plan calls for filters that provide a “wide berth” for “transformative, creative uses” of copyrighted content; strict procedures for protecting fair use, including review of content “matches” detected by automated filters before a post is removed from a site; procedures for disclosing all “takedown notices” issued by copyright owners under the Digital Millennium Copyright Act, including users’ right to issue counter-notices in the event of a dispute; and an “informal dolphin hotline” maintained by content owners to allow targets of takedown notices to “easily and informally request reconsideration.” The organizations
signing on to the plan are the Electronic Frontier Foundation, American University’s Center for Social Media and the Program on Information Justice and Intellectual Property, Public Knowledge, the Berkman Center for Internet and Society at Harvard Law School and the ACLU of Northern California.

ICANN COMMITTEE APPROVES DATABASE STUDIES

The Generic Names Supporting Organization Council, a committee of the International Corporation for Assigned Names and Numbers (ICANN) which oversees Internet addresses, voted to conduct further studies on the databases containing names, phone numbers and other private information on domain name owners. It set a deadline of February 15, 2008 to identify the types of studies needed. The committee also rejected, 17-7, a proposal to give Internet users the ability to list third party contacts rather than their own private data in the open, searchable Whois databases. A third proposal of a “sunset” option that would have eliminated the requirement for domain name registration companies to make the data available through Whois was rejected, 13-10, because it would have resulted in large gaps between registration records.

FOREIGN GOVERNMENT CRACKDOWNS ON BLOGGERS RISING

Reporters Without Borders released its 2007 Worldwide Press Freedom Index that reveals that government repression in many countries has shifted from journalists to bloggers. For example, the report notes that while countries such as Egypt and Jordan are no longer sentencing journalists to prison terms, they have been doing so to bloggers. Egypt is ranked 146th, and Jordan 122nd, in press freedom out of the 169 countries for which data was available. Major industrialized countries, except Russia, made progress and moved up the list. Iceland was first in press freedom in the report, with Eritrea ranked last, followed by North Korea and Turkmenistan ranked second and third from the bottom, respectively. The United States moved up to 48th place from last year’s ranking of 53rd. The report is available at http://www.rsf.org/IMG/pdf/index_2007_en.pdf.

TYPO-SQUATTING: WHAT ARE THE ODDS?

Internet users have a 1-in-14 chance of landing on a typo-squatting site, due to mistyping the URL of their intended web site, according to a report by security firm McAfee. The report, entitled “What’s in a Name: The State of Typo-Squatting 2007,” says that landing on a typo-squatting site could result in getting more spam, as one’s e-mail address is harvested from the site. However, the report finds that, in a majority of the cases, typo-squatters are seeking to generate income through pay-per-click ads on their domains. McAfee, which examined 1.9 million variations of 2,771 popular domain names, found that game sites had the greatest likelihood of being typo-squatted at 14 percent, followed by airline sites at 11.4 percent, mainstream media sites at 10.8 percent and dating sites at 10.2 percent. The report may be accessed at http://www.mcafee.com/typosquatting.
BOARD ADVISES CAPPING RURAL PHONES, EXPANDING WIRELESS

A joint federal-state advisory board recommended that federal subsidies for companies providing telephone service in rural areas should be capped at $4.5 billion, and $1 billion should be set aside for wireless phone service and $300 million for broadband Internet service to be provided in underserved areas. The current program is overseen by the Federal Communications Commission (FCC), which makes direct payments to the telecommunications companies providing rural service. It is financed through surcharges on phone bills. Those surcharges go into the Universal Service Fund, which was created by Congress in 1996 to ensure that consumers in rural areas had access to phone service at similar rates charged in urban areas. The Fund has collected $44 billion over its 10-year lifetime. The FCC is not bound by the Board’s recommendation, and has one year to act.

STUDY SUGGESTS INTERNET SOON AT CAPACITY

Internet usage could outstrip network capacity in less than three years, a finding suggested in a research study conducted by Nemertes Research, a research firm specializing in the business impact of technology, and distributed by the Internet Innovation Alliance, a non-profit coalition of business and non-profit organizations promoting universal broadband access. The study, however, makes clear that while the Internet could face a crisis in access capacity around 2010, it will never “break” because of its redundant and self-protecting architecture. A more likely scenario is that users might experience erratic performance, particularly when downloading files over a saturated broadband link. According to Nemertes, the financial investment required to bridge the gap between demand and capacity is between $42 billion and $55 billion in the U.S. and about $137 billion worldwide, both primarily to be spent on broadband access capacity. The study can be accessed at http://www.nemertes.com.

8.3 MILLION AMERICANS ARE ID THEFT VICTIMS

Nearly four percent of American adults were victims of identity theft in 2005, but one-half of them did not incur any out-of-pocket expenses, according to a survey by the Federal Trade Commission (FTC). However, 10 percent of the victims reported expenses of $1,200 or more. The survey found that identity information was stolen from 8.3 million adults, and was most often used to access or open accounts for credit cards, bank checking, telephone service, e-mail and medical insurance. The survey also studied the value of goods or services obtained by thieves using the victims’ personal information. In one-half of the incidents, thieves obtained items or services worth $500 or less, while in 10 percent of the cases, thieves obtained $6,000 or more in goods and services. The FTC survey found that 37 percent of victims reported problems beyond out-of-pocket expenses, including harassment by debt collectors, cut off utilities, denial of new credit or loans, inability to use existing credit cards and difficulty in obtaining or accessing bank accounts. The survey was based on 4,917 telephone interviews.
1.5 MILLION BOOKS AVAILABLE IN ONLINE LIBRARY

The Universal Digital Library (UDL), a book scanning project supported by several major national and international libraries, such as the Bibliotheca Alexandrina in Egypt, completed the digitization of 1.5 million books and made them publicly available for free. The library offers full text downloads of works that are in the public domain or for which the copyright holder has given permission to make available. The works still in copyright, while digitized and indexed, are offered only as abstracts. The project was founded and is currently directed by Raj Reddy, a computer science and robotics professor at Carnegie Mellon. It is partially funded by the National Science Foundation and partners with eight Chinese and nine Indian universities. Unlike other book scanning projects, books from the UDL are available in several open formats, such as HTML, TIFF and DiVi (an alternative to PDF).

TOOLS YOU CAN USE

Investigators’ Tools

“Investigative Uses of Technology: Devices, Tools and Techniques” discusses techniques and resources for investigating technology-related crime. It describes the technology-related tools and devices that an investigator may encounter or that may assist during an investigation, as well as explains legal issues affecting the use of technology. It may be accessed at http://www.ojp.usdoj.gov/nij/pubs-sum/213030.htm.

Sexual Exploitation of Children

“Commercial Sexual Exploitation of Children: What Do We Know and What Do We Do About It?” explores research into the organization of the commercial sexual exploitation of children, its effects on victims and what measures are being taken and can be taken in the future to prevent its occurrence. It can be accessed at http://www.ncjrs.org/pdffiles1/nij/215733.pdf.
HOLD THE DATE

FOR THE FIRST CYBERCRIME TRAINING IN 2008

CYBERCRIME AND JUVENILES: AS VICTIMS AND OFFENDERS
APRIL 1-3, 2008

Mark your calendar for April 1-3, 2008 for this new training course, developed under the partnership between the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL). The course will address how the juvenile justice system deals with cyber crime – juveniles as both victims and offenders. Included in the discussion of juveniles as victims will be presentations on cyberbullying, social networking and virtual communities. The course will also address how state and federal law enforcement systems deal with juvenile offenders.

There will be no fee for prosecutors and civil enforcement attorneys from Attorneys General offices who attend this course, and the NAAG-NCJRL partnership will also pay transportation costs of all attendees. For additional information, please contact Hedda Litwin, Cybercrime Counsel, at hlitwin@naag.org or 202-326-6022. Registration forms will be available shortly.