

News Highlights in This Issue:

MySpace Not Liable for User's Assault	7
US Largest Source of Online Attacks	12
Four AGs Attend Cyber hate Program	2
New Jersey Senate OKs Internet Dating Bill	13
Search of Cellular Phone Before Arrest OK	9
ICANN Nixes .xxx Domain	12
Washington Enacts Internet Tax Authorization	14
Spyware/Phishing Training Scheduled for August	15
Multiple Porn Images Equals Only One Count	8
Trading in Spammed Stocks Suspended by SEC	10
Mississippi Conforms Law to Adam Walsh Act	14
Tech Guide for Information Security Released	14
Search Engines Have Right to Reject Ads	7
Eight Programs Certified Safe to Download	10
Florida Enhances Child Pornography Penalties	13
Section 230 Immunity Applies to Web Postings	8
Federal Agencies Must Apply New Security	12
Kentucky Expands Sex Offenders Information	14
Computer Sabotage Statute Constitutional	9
North Dakota Strengthens Sex Offender Law	14

Table of Contents

<u>Features</u>	
NAAG Committee Meets on Cyber Hate	2
Spyware/Phishing Training Set for August	15
<u>AGs Fighting Cyber Crimes</u>	3
AG King Speaks at Training on Sex Offenders	
Colorado AG Releases ID Theft Repair Kit	
AG Blumenthal Announces Social Networking Bill	
Delaware AG Creates Child Predator Unit	
AG McCollum's Unit Arrests Child Predator	
Indiana AG: Refunds Made in Online Fraud Case	
AG Morrison Speaks About Internet Killer	
Kentucky AG: Arrest in Child Predator Sting	
AG Cox's Team Arrests Two Online Predators	
New Hampshire AG Speaks on Internet Safety	
AG Rabner Keynotes Cyber Hate Summit	
New Mexico AG: Maximum Sentence for Predator	
AG Cuomo Settles Data Breach Case	
Ohio AG Sues Search Firm for Online Fraud	
AG Corbett's Agents Arrest Child Predator	
South Carolina AG: Arrest in Internet Sting	
AG Abbott Says 95 Years for Internet Predator	
Utah AG: Task Force Arrest 2 Predators	
AG McKenna Settles Spyware Suit	
West Virginia AG Shuts Down Online Firm	
<u>In the Courts</u>	7
MySpace Not Liable for User's Assault	
Search Engines Have Right to Reject Ads	
Section 230 of CDA Applies to Web Messages	
Multiple Child Porn Images = Only One Count	
Computer Sabotage Statute Constitutional	
OK to Search Cell Phone Contents Before Arrest	
<u>News You Can Use</u>	10
Trading in Spammed Stocks Suspended by SEC	
Eight Programs Certified as Safe to Download	
FCC: Rural Carriers Must Allow Internet Access	
Florida Bar Approves Online Testimonials	
Pilot Program to Post Patent Applications Started	
Royalty Rates Per Song for Webcasts Raised	
Tests on International Domain Names Successful	
ICANN Votes Against .xxx Domain	
Report: Most Online Attacks Come From US	
Federal Agencies Requires to Use New Security	
<u>Legislation Update</u>	13
New Jersey Senate OKs Internet dating bill	
Florida Legislature Enhances Child Porn Penalties	
North Dakota Strengthens Sexual Predator Law	
Mississippi Conforms Law to Adam Walsh Act	
Kentucky Expands Sex Offender Required Data	
Washington Authorizes Internet Sales Tax	
Utah Creates Electronic Registration Mark	
<u>Guide for Information Security Available</u>	14

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

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

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

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

**NAAG CRIMINAL LAW COMMITTEE
MEETS AT UNIVERSITY OF MISSISSIPPI
ON CYBER HATE**

By Hedda Litwin¹

The NAAG Criminal Law Committee, co-chaired by Attorneys General John Suthers of Colorado and Jim Hood of Mississippi, met on April 23 at the National Center for Justice and the Rule of Law to discuss “*Cyber Hate: Survey of the Problem and Attorney General Responses.*” Joined by Attorneys General Paul Morrison of Kansas and Douglas Gansler of Maryland, the Committee heard first from Brian Marcus, Director of Internet Monitoring at the Anti-Defamation League, who illustrated hate speech sites on the Internet and also gave an overview of cyberbullying on the Internet. The Committee then discussed the constitutional and regulatory issues raised by hate speech on the Internet, following a presentation by Susan Brenner, Associate Dean and Professor of Law at the

University of Dayton School of Law. David Barkey, Southern Area Counsel at the Anti-Defamation League, then followed with a discussion with the Attorneys General of appropriate responses from law enforcement and public officials.

The program on cyber hate was followed by the unveiling of a new Cyber Guide by Tom Clancy, Director of the National Center for Justice and the Rule of Law. The Guide, developed by the Center, provides a blueprint for setting up and/or enhancing the capacity to address cyber crimes in an Attorney General office. Copies were distributed to the Attorneys General present at the meeting, and the Guide will be distributed by mail to all Attorneys General during the beginning of May.

¹Hedda Litwin is Cyber Crime Counsel for the National Association of Attorneys General.

AGs FIGHTING CYBER CRIMES

ALABAMA

Attorney General Troy King spoke to 82 law enforcement officers at a training session about sex offenders co-sponsored by his office and the Sylacauga Police Department. The session covered all of the state laws relating to sexual predators, including an “A to Z look at Alabama’s Community Notification Act.” Attorney General King also spoke about his legislative package which includes legislation to further strengthen the Community Notification Act, shield child victims from having to testify in the same room with the offender and clarifying that each consecutive sentence of an offender is counted separately for purposes of parole consideration. Attorney General King is also asking legislators to change the law so that a criminal is guilty of child solicitation, even if the “child” the criminal believes he is soliciting is actually an undercover officer. He also wants legislators to provide life without parole or the death penalty for repeat sex offenders who prey on children.

COLORADO

Attorney General John Suthers released an Identity Theft Repair Kit, a 21-page, full color booklet developed by his office which discusses how to avoid becoming a victim of identity theft and what to do if you become a victim. It also contains a 10-step checklist for victims, as well as credit bureau phone numbers and information about filing a report with the Federal Trade Commission. Attorney General Suthers partnered with FirstBank Holding Company in the initiative, which paid the printing costs of the booklet. The company will also distribute 20,000 of the kits through its 118 branches in the state.

CONNECTICUT

Attorney General Richard Blumenthal, together with bipartisan members of the state General Law Committee, announced legislation requiring social networking sites to verify users’ ages, obtain parental consent to post profiles of minors under 18 years of age and allow parents access to their children’s pages. Under the proposal, sites that violate the legislation would face civil penalties of up to \$5,000 per violation. The legislation would also provide for a private right of action.

DELAWARE

Attorney General Beau Biden announced the creation of his new child predator unit. Originally, Governor Ruth Ann Minner had called for \$164,000, enough for a deputy attorney general and an investigator, to get the unit started in the budget year that begins July 1, 2007, but the legislative Joint Finance Committee and the Governor’s office later agreed to finance the unit three and one half months earlier. Deputy Attorney General Melanie Walters, a Department of Justice veteran of 18 years who heads the felony unit in Sussex County, will lead the unit, with an investigator to be hired as soon as possible. Attorney General Biden said the unit would operate Internet stings to identify and apprehend predators. It will also target manufacturers, distributors and possessors of child pornography and would, with other law enforcement agencies, track down convicted child predators who fail to register as such.

FLORIDA

Attorney General Bill McCollum’s Child Predator CyberCrime Unit arrested Daniel Lenz after discovering that he was attempting to lure a 15-year-old girl that he sexually solicited over the

Internet from New Hampshire to his Florida home. Lenz met the girl through a computer game and used “grooming” techniques to gain her trust. The girl was intercepted in South Carolina and returned to her home in New Hampshire through the coordinated efforts of Attorney General McCollum’s office, the FBI Cybercrime Task Forces in Jacksonville, Florida and New Hampshire, the U.S. Attorney’s Office for the Middle District of Florida, the New Hampshire Police Department, the Clarendon County, South Carolina Sheriff’s Office and U.S. Immigration and Customs Enforcement. A search warrant executed at Lenz’s house led to the seizure of several computers, which will undergo forensic analysis for evidence of the crime. Lenz is charged with one count of computer solicitation and, if convicted, would face up to five years in prison. Attorney General McCollum’s CyberCrime Unit acted as a member of the FBI CyberTask Force in Jacksonville.

INDIANA

Attorney General Steve Carter said that Internet seller Kumara Jayasuriya, aka Jay Smith, issued 10 consumer refunds totaling \$3,649 and is required to comply with state law in all future transactions. A circuit court approved an agreement requiring the refunds after Attorney General Carter investigated complaints that consumers paid for auto parts advertised online and did not receive their items in a timely fashion or received incorrect or defective auto parts. Some of the complaints were resolved through refunds, chargebacks or shipment of the items prior to the court’s order.

KANSAS

Attorney General Paul Morrison was the featured speaker at the 18th Annual Regional Criminal Justice Conference at the University of Nebraska. He discussed the prosecution of a serial killer who murdered at least nine women in the Kansas City area and who lured his victims using the Internet. Both University and high school students attended the conference.

KENTUCKY

Attorney General Greg Stumbo announced the arrest of Matthew Barlow of Ohio, the 12th arrest in his Child Predator Sting. Barlow, who had been communicating online with a decoy, arrived at a restaurant to meet who he thought was a 13-year-old girl, but was instead met by the Chief of the Highland Heights Police Department. He is charged with unlawful transaction with a minor, a class B felony punishable by 10-20 years in prison.

MICHIGAN

Attorney General Mike Cox announced the arrests of Kevin Wolfers, a youth soccer coach, and Lee Vanbeek, a youth wrestling coach, for using the Internet to solicit a minor for sexual acts and to disseminate sexually explicit material to a minor. Wolfers was arrested by the Michigan Internet Crimes Against Children Task Force, operated by the State Police, and arraigned on two counts of using the Internet to solicit or accost a minor for immoral purposes, a 10-year felony. Vanbeek was arrested by Attorney General Cox’s investigators for engaging in graphic sexual conversation with and propositioning someone he thought was a 14-year-old girl that he met in a chat room but was actually an undercover agent.

NEW HAMPSHIRE

Attorney General Kelly Ayotte joined local police at the Rochester Middle school for an educational discussion with parents about the dangers their children face while using the Internet. Much of the discussion centered on social networking sites and predators trying to lure children into face-to-face meetings. Both Attorney General Ayotte and Detective James Bonneau outlined Internet chat rooms, instant messaging and MySpace.com as online activities that put children at risk, not only for online solicitation but also for cyberbullying. Everyone in attendance received a copy of Attorney General Ayotte’s new Internet Safety Guide for Parents and Teens, a 56-page booklet that addresses the dangers of online predators and offers advice to parents on how to

protect their children and to teens on how to protect themselves.

NEW JERSEY

Attorney General Stuart Rabner was the keynote speaker at the first “New Jersey Unites Against Hate” summit, a program co-hosted by his office. The program brought together about 40 groups to discuss and participate in workshops, including “Hate on the Internet” and “Facilitating Community Dialogue.” Other speakers included State Senator Diane Allen; Etzion Neuer, New Jersey Regional Director of the Anti-Defamation League; and Paul Winkler of the New Jersey Holocaust Commission.

NEW MEXICO

Attorney General Gary King said that convicted sex offender Jeramie Dante was sentenced to a maximum penalty of 18 months in prison for one count of fourth degree child solicitation by computer. Dante had been arrested by Attorney General King’s Internet Crimes Against Children (ICAC) Unit. During an online chat using Yahoo! Instant Messaging, an ICAC agent posing as a 12-year-old girl received sexually explicit messages from Dante, who then sent pictures of himself and his body parts. Although Dante never showed for meetings with the “girl,” agents were able to identify him through the pictures he sent.

NEW YORK

Attorney General Andrew Cuomo obtained the first settlement under the state’s Information Security Breach and Notification Law. CS STARS LLC, a Chicago-based claims management company, failed to notify the owner of computerized data and approximately 540,000 state consumers that their personal information was at risk for five weeks. Under New York’s law, any business which maintains private data must notify the owner of the data immediately after discovery of any breach as well as affected consumers. Notification must also be given to the Attorney

General’s office, the Consumer Protection Board and the state office on Cyber Security. Without admitting any violation but cooperating fully with the investigation, CS STARS agreed to comply with the law and implement more extensive security practices. They must also pay Attorney General Cuomo’s office \$60,000 to cover the costs of the investigation. The case was handled by Special Assistant Attorney General Stephen Mendel and Assistant Attorney General Herbert Israel in the Consumer Frauds and Protection Bureau.

OHIO

Attorney General Mark Dann filed suit against Courts Online, an Internet-based company offering unlimited searches of public and private databases, including criminal background checks, for a one-time fee ranging from \$24 to \$36. His office had received more than 50 complaints from consumers across the country, including allegations that the company failed to deliver purchased services, misrepresented services offered in advertising and failed to properly advise consumers about refund policies. The investigation also revealed that Courts Online was not properly registered as a business in the state. Complaints were also lodged with the Better Business Bureau and the Federal Trade Commission. Attorney General Dann is asking the court to prevent Courts Online from entering into any further transactions until they have paid restitution to previous customers, pay a penalty of \$25,000 per violation and allow his office the right to see the company’s business records for five years to ensure they are in compliance with state law.

PENNSYLVANIA

Attorney General Tom Corbett’s Child Predator Unit agents arrested David Wimer, who is accused of using an Internet chat room to sexually proposition and send sexually explicit videos to what he believed to be a 13-year-old girl. Instead, the “girl” was actually an undercover Unit agent. Using a screen name, Wimer told the “girl” that he was a 34-year-old male named Dave and then he began to ask her personal questions, commenting

that they could do “some cool stuff” if they got together. He repeatedly proposed meeting for the purpose of having sex. Wimer is charged with two counts of unlawful contact with a minor and one count of criminal use of a computer, all third degree felonies carrying maximum penalties of seven years in prison and a \$15,000 fine. He will be prosecuted by Deputy Attorney General William Caye of the Unit.

SOUTH CAROLINA

Attorney General Henry McMaster announced that Richard Holbrook of Michigan was arrested in an undercover Internet sting by the City of Charleston Police Department, a member of Attorney General McMaster’s Internet Crimes Against Children (ICAC) Task Force. Holbrook was arrested on one count of Criminal Solicitation of a Minor, a felony punishable by up to 10 years imprisonment. Arrest warrants allege that Holbrook solicited sex on the Internet with an individual he believed to be a 12-year-old girl, but in reality was an undercover police officer. When police learned that Holbrook was on a flight to Boston from Charleston International Airport, they arranged to arrest him upon landing, with the assistance of the Charleston Airport Authority. Holbrook was carrying a laptop computer, which was seized upon his arrest. The case will be prosecuted by Attorney General McMaster’s office.

TEXAS

Attorney General Greg Abbott announced that Joe Cook, a convicted felon arrested by Attorney General Abbott’s Cyber Crimes Unit, was sentenced to 95 years in prison, the longest prison sentence ever handed down to an online predator arrested by the Unit. A jury had returned a guilty verdict on one count of attempted aggravated sexual assault on a child. The sentence was enhanced because of Cook’s two prior felony convictions in Illinois for burglary and home invasion. Unit investigators and Longview Police Department officers arrested Cook after he rode his bicycle to meet someone he believed to be a 13-year-old child he had solicited over the Internet for sex, but was

actually an undercover Unit investigator who had posed as an underage girl. *Note: The Editor thanks Grant Sparks, Assistant Attorney General, Office of the Attorney General of Texas, for information about this case.*

UTAH

Attorney General Mark Shurtleff announced that the Internet Crimes Against Children Task Force, which his office oversees, arrested Henry Howk on five counts of sexual exploitation for possessing child pornography and John Keane for enticement of a minor over the Internet. Howk applied for a job as a law enforcement officer and then admitted to viewing child pornography while being questioned during a routine employee selection process. Realizing his admission would trigger an investigation, he destroyed his computer, but ICAC investigators from Attorney General Shurtleff’s office and Adult Probation and Parole located the computer hard drive with the cooperation of Howk’s wife. Investigators sent the hard drive to the Regional Computer Forensics Lab where it was reconstructed and found to contain child pornography. Keane was arrested after a three month investigation conducted by a Department of Public Safety investigator who is assigned to the Task Force.

WASHINGTON

Attorney General Rob McKenna reached a settlement with three California-based businesses – Digital Enterprises d/b/a Movieland.com, AccessMedia Networks and Innovative Networks, resolving allegations that they installed software that took control of a consumer’s computer by launching persistent pop-ups that demanded payment for a movie download service, in violation of the state’s Computer Spyware and Consumer Protection Acts. According to the complaint, the defendants offered a free three-day trial period for the movie service, then remotely activated billing software on the personal computers of those who accepted the offer. After the trial period, a 40-second video recurred hourly telling consumers they were legally obligated to purchase a subscription.

Under the settlement, the defendants must not offer anonymous free trials in the state for movie downloads. If they use a software-based collection method, they must not try to collect payments from state residents unless they have a valid contract and they must not install any software on the computer of a Washington resident without the express consent or the owner of an authorized user. Defendants must also pay \$50,000 to resolve allegations.

WEST VIRGINIA

Attorney General Darrell McGraw announced that Sataline.com, an Internet business that offered to deliver premium cable television

channels via the Internet for viewing on consumers' personal computers for \$12.95 per month, was shut down for failure to respond to and resolve customer complaints. Although Sataline.com offered a one-month trial subscription, consumers were actually required to sign up for a six-month subscription. In addition, consumers complaining to Attorney General McGraw's Consumer Protection Division claimed that the television channels received from Sataline.com were undesirable and not the channels the company offered on its web site. Some consumers complained that they were not able to access the service at all.

IN THE COURTS

SOCIAL NETWORKING SITES: LIABILITY

Doe v. MySpace Inc., 2007 WL 471156 (W.D. Tex. February 13, 2007). A district court found that the social networking site MySpace.com cannot be held liable for the sexual assault of a teen-aged girl who met her attacker on the site. "Jane Doe," a 14-year-old girl from Texas, met a 19-year-old man on MySpace. They met in person, and the man sexually assaulted her. She reported the incident to police, who subsequently arrested and indicted the man. "Jane Doe" and her mother sued MySpace and its parent company, News Corp., which is based in New York, in a New York court, alleging negligence, fraud and misrepresentation. MySpace removed the case to the U.S. District Court for the Western District of Texas, then filed a motion to dismiss under Section 230 of the Communications Decency Act, which immunizes online service providers from tort claims stemming from information or content

provided by third parties. The "Does" argued that Section 230 was only meant to preempt defamation claims and suits based on the content of materials, and the instant case had nothing to do with the content of messages. The court, however, rejected that narrow interpretation and found MySpace immune because it is merely an intermediary that provides a forum for third-party users to exchange messages. The suit was dismissed.

SEARCH ENGINES: FIRST AMENDMENT

Langdon v. Google, 2007 WL 530156 (D. Del. February 20, 2007). A district court ruled that search engines have a First Amendment right to reject ads as part of their protected right to speak or not. Christopher Langdon, who runs two web sites, www.NCJusticeFraud.com and www.ChinalsEvil.com, sought to buy ads on Google, MSN and Yahoo to air his many gripes. All three search engines declined his ad requests, and

Langdon sued them for violation of his First and Fourteenth Amendment rights, as well as fraud, breach of contract, deceptive business practices and the doctrine of public calling, requesting that they be enjoined to carry his ads. All three companies filed a motion to dismiss all claims, which the U.S. District Court for the District of Delaware granted, finding that Langdon had not shown that he had sustained an injury-in-fact. The court also made the following key rulings: 1) search engines have a First Amendment right to reject ads; 2) search engine decisions to reject ads is protected under 47 U.S.C. §230©(2) as a legitimate decision to filter objectionable content, and 3) search engines are not state actors and thus are not bound by the First Amendment so they cannot deprive potential advertisers of their First Amendment Rights if they reject their advertisements.

**COMMUNICATIONS DECENCY
ACT: WEB-BASED MESSAGE
BOARDS**

Universal Communications Systems, Inc. v. Lycos, Inc., 2007 WL 549111 (1st Cir. February 23, 2007). In a unanimous ruling, the First Circuit Court of Appeals joined other courts in finding that a host's limited influence on the content of the postings on a web-based message board does not impact the applicability of the Section 230 immunity under the Communications Decency Act. Lycos, Inc. hosts a web site, RagingBull.com, which includes a message board that allows viewers to post comments about publicly traded companies. Universal Communications, Inc. ("UCS") sued Lycos, alleging that web postings about the company's financial condition and integrity were false and defamatory.

Lycos moved to dismiss based on Section 230 immunity afforded computer service providers from defamation claims. The U.S. District Court for the District of Massachusetts granted the motion, and UCS appealed. The appeals court agreed, finding no evidence that Lycos actively induced the posted information and therefore was not responsible for the alleged defamatory content. The court also included that Section 230 immunity extends to any claim based on the host as a publisher of information.

**POSSESSION OF CHILD
PORNOGRAPHY: MULTIPLE
COUNTS**

State v. Muhlenbruch, No. 05-2038 (Iowa, February 23, 2007). The Iowa Supreme Court found that a man who had hundreds of child pornography images on his computer can only be charged with one count of possession of child pornography. Randall Muhlenbruch's wife discovered pictures of child pornography on her husband's computer, copied them onto a disc and gave them to police. Muhlenbruch was then charged with 10 counts of sexual exploitation of a minor, with prosecutors claiming that each count was based on downloading different images on different days. Muhlenbruch challenged the 10 charges, arguing that he had only one computer and therefore only one charge was proper. The trial court agreed and dismissed nine of the counts. On appeal, the Iowa Supreme Court upheld the lower court decision, finding that under the statute which Muhlenbruch was charged, Iowa Code 728.12(3), the number of images is not relevant and cannot result in multiple charges.

COMPUTER SABOTAGE: COMMERCE CLAUSE

United States v. Trotter, No. 05-4202 (8th Cir. February 23, 2007). The 8th Circuit Court of Appeals found that a computer sabotage statute was constitutional as applied to an attack on the Salvation Army's computer network. A law enforcement investigation of intrusions into the Salvation Army's computer network led to John Trotter, a former information technology supervisor who was fired by the Salvation Army. Trotter was charged with intentionally causing damage to a protected computer without authorization, in violation of 18 U.S.C. §1030(a)(5)(A)(i). After unsuccessfully trying to dismiss the charges, Trotter pleaded guilty to one count of computer sabotage, reserving the right to challenge the constitutionality of the statute. The U.S. District Court for the Eastern District of Missouri sentenced Trotter to 18 months in prison and ordered him to pay approximately \$19,000 in restitution. On appeal, Trotter contended that the statute was unconstitutional as applied to his conduct because the Salvation Army's network was not a "protected computer" within the meaning of the statute and the statute could not possibly be so broad as to cover the network of a non-profit organization like the Salvation Army. The 8th Circuit disagreed, finding that the Salvation Army's computers were protected by the statute because they were engaged in interstate communication connected to the Internet, and were part of a "system that is inexorably intertwined with interstate commerce" and thus within the realm of Congress' Commerce Clause powers.

SEARCH AND SEIZURE: CELL PHONE CONTENTS

United States v. Finley, 2007 U.S. App. LEXIS 1806 (5th Cir. 2007). The 5th Circuit has ruled that an officer may lawfully examine the stored numbers and text messages of a cellular phone as a search incident prior to arrest. Jacob Finley was arrested after the passenger in his company vehicle delivered methamphetamine to undercover law enforcement agents. A search warrant was executed on his passenger's (and co-defendant's) home, during which agents examined Finley's company cellular phone for telephone numbers to which calls were placed and text messages sent and received. At trial, Finley moved to suppress the evidence gathered from his cell phone, arguing it was the fruit of an unlawful search. The U.S. District Court for the Western District of Texas denied the motion. Finley was convicted and appealed. On appeal, the 5th Circuit found that Finley had an expectation of privacy in the contents of the cell phone and thus did have standing to challenge the search. However, the court reasoned that the scope of a search incident to arrest includes a search for evidence of the crime for the purpose of preservation, as well as for weapons and instruments of escape, and including searching closed containers on the defendant's person and those within his reach. The fact that the search of the cell phone did not occur immediately after the custodial arrest did not affect the validity of the search, the court added. The court held that as long as the search is substantially contemporaneous with the arrest, the exception to the warrant requirement still applies.

NEWS YOU CAN USE

TRADING IN STOCKS LINKED TO SPAM SUSPENDED

The Securities and Exchange Commission (SEC) suspended trading in the stocks of 35 small companies linked to spam e-mail campaigns urging investors to buy shares. The potentially fraudulent spam e-mail promotes small company stock with phrases like “Ready to Explode,” “Ride the Bull” and “Fast Money.” The SEC said that an estimated 100 million of these spam messages are sent every week, triggering dramatic spikes in share price and trading volume before the spamming stops and investors lose their money. The SEC estimates that investor losses related to the 35 companies are in the tens of millions of dollars.

EIGHT PROGRAMS CERTIFIED AS SAFE TO DOWNLOAD

The TRUSTe group, an organization that monitors web site privacy and email practices for businesses, certified eight programs as consumer-friendly and non-invasive. The group’s Trusted Download Program is designed to help companies make decisions about where to advertise and with whom to partner. Independent technicians hired by TRUSTe review software used for advertising or tracking user behavior. To be certified, adware and other software must obtain consent before downloading, be easy to uninstall and be unable to modify computer settings to cause damage. The certified programs are Save 4.0 from WhenU.com, CamFrog Video Chat 3.81 from Camshare LLC, Coupon Bar 5.0

and Coupon Printer 5.0 from Coupons Inc., Crawler Toolbar 4.2 from Crawler LLC, Illumio 1.2.73 from Tacit Software Inc, MostFun 1.0 from NeoEdge and Vomba 1.2.0.0 from Vomba Network Inc. TRUSTe said that all applicants had made changes to their software to receive certification.

FCC ALLOWS INTERNET PHONE ACCESS

Rural telephone companies must allow carriers to use local lines to connect Internet-based calls, according to a ruling by the Federal Communications Commission. The ruling granted a petition filed by Time Warner Cable and supported by AT&T and Verizon. The order overrides rulings by state regulators in Nebraska and South Carolina that barred certain carriers from connecting calls using Voice over Internet Protocol (VoIP) to traditional phone lines. In its decision, the FCC said that the state rulings would have impeded phone competition and hindered the deployment of high speed Internet access.

FLORIDA BAR OKS TESTIMONIALS ON WEB SITES

The Florida Board of Governors tentatively approved a proposed rule on law firm web sites that would let lawyers publish client testimonials and claims about their past successes. Under the proposed rule, the inside pages of law firm web sites (not the home page) could include testimonials, references to past results and statements characterizing the quality of the services, as long as the

statements are truthful, not misleading and come with disclaimers. The disclaimers must say that past results do not guarantee a future success. Currently, Florida Supreme Court rules do not allow law firms to provide such information to potential clients unless the clients specifically request it. That restriction would remain in effect for lawyer advertising in other media. However, unlike other forms of media, web sites would not have to be submitted for the Bar's approval. The proposal still must be passed by the Board of Governors in a second reading and approved by the Supreme Court.

USPTO PILOT TO POST PATENT APPLICATIONS

The U.S. Patent and Trademark Office (USPTO) is starting a pilot project that will post patent applications on the Internet and invite comments. The project would also use a community rating system designed to raise the most respected comments to the top of the file for serious consideration by patent examiners. Currently, patent examiners rarely seek outside opinions, instead relying on scientific writings and archived records of previous patents. The number of patent filings, however, has made the current procedures unwieldy. Last year, USPTO's 4,000 examiners completed a record 332,000 applications. Under the pilot project, some companies submitting patent applications will agree to have them reviewed on the Internet. The list of volunteer reviewers includes IBM, Microsoft, Intel, Hewlett-Packard and Oracle. Ultimately, those registered to participate will vote on all the nominated information, and the top 10 items will be passed on to the examiner, who will serve as the final arbiter on whether to

award a patent. Examiners will award "gold stars" to people who previously submitted the most useful information.

ROYALTY RATES FOR WEBCASTS RAISED

The U.S. Copyright Royalty Board released new royalty rates for webcasters to pay for each song streamed to each user, effective from 2007 to 2010. The 2006 rate is \$.0008 to stream one song to each user, and the rates increase each year as follows: 2007: \$.0011, 2008: \$.0014, 2009: \$.0018 and 2010: \$.0019. The Radio and Internet Newsletter (RAIN) calculates that, assuming the average station plays 16 songs per hour, sites would have to pay about 1.28 cents per listener per hour using the 2006 rate, and would owe this retroactively, in addition to licensing fees going forward. Even small sites would owe the minimum of \$500 per channel per year.

INTERNATIONAL DOMAIN NAMES PASS TESTING

The Internet Corporation of Assigned Names and Numbers (ICANN) announced that it had successfully completed testing of international domain names (IDNs). ICANN had commissioned a laboratory test of IDNs that was designed to establish whether the use of encoded internationalized characters would have any impact on the operations of the root name servers. The results of the testing showed no impact, with all involved systems behaving as expected. However, the test did not include the "end-user perspective" of a live root test. It instead concentrated on replicating the root server environment, suggesting that further testing is required. Details of the test setup and

design are available on ICANN's web site, www.icann.org.

ICANN VOTES AGAINST .XXX DOMAIN

ICANN rejected another proposal by ICM Registry LLC for an .xxx domain for pornographic web sites for the third time. ICANN had revived the proposal in January of this year after ICM agreed to hire independent organizations to monitor pornographic sites' compliance with rules that would be developed by a separate body called the International Foundation for Online Responsibility. Nearly all of the ICANN board members who voted against approving the domain said they were concerned about the possibility that ICANN could find itself in the content regulation business if the domain name was approved. ComScore Media Matrix, a web site measurement firm, finds that four percent of all web traffic and two percent of all time spent web surfing involves adult sites.

REPORT: US MOST PROLIFIC SOURCE OF ONLINE ATTACKS

U.S. networks were responsible for the highest percentage of attacks during the second half of 2006, with China at a distant second, according to the Internet Security Threat Report produced by security firm Symantec. The report said that the U.S. accounted for 31 percent of malicious activity originating from computer networks, while 10 percent came from China and seven percent from Germany. Symantec also found that 51 percent of all known servers used by attackers to buy or sell stolen personal information, such as credit card or bank account numbers, are located in the U.S. U.S.-based credit

cards, with accompanying verification numbers, were reported to be selling for \$1 to \$6 each on these servers. However, other personal identification data, such as a person's birthdate and banking and government-issued identification numbers, was selling for \$14 to \$18. Trojan-horse software, which can load keylogging software onto computers, accounted for 45 percent of the top 50 malicious code samples collected by Symantec, up from 23 percent for the first half of 2006. The report also noted that a daily average of 961 phishing e-mails were sent to people on weekdays, compared with 27 percent fewer phishing messages on weekends.

FEDERAL AGENCIES MUST USE NEW SECURITY STANDARDS

The White House Office of Management and Budget issued a memo requiring all federal agencies using Microsoft Windows software to implement new security standards developed in tandem with the National Security Agency (NSA). The new rules mandate that agencies use preconfigured security settings on all existing PCs. They also require agencies seeking to purchase Windows Vista, the latest version of Microsoft's operating system, to order systems specially configured to meet the government's new security requirements. Agencies must also include tactics such as disabling unneeded software and services that expose systems to cyber attacks, as well as configuring machines to run under user accounts that cannot install new programs or alter existing software. The standards are based on configurations developed by the NSA, U.S. Air Force, the National Institute of Standards and Technology and the Defense Information Systems Agency. They have been

implemented in more than 420,000 Air Force Windows PCs during the past year, and are directly responsible for decreasing the security incidents and the

overall workload of Air Force information technology personnel by 30 percent. Full compliance by federal agencies is required by February 2008.

LEGISLATION UPDATE

INTERNET DATING SERVICES

On March 13, the New Jersey Senate unanimously approved S.1977, a bill that would require Internet dating services doing business in the state to advise whether their users have undergone criminal background checks. If the service does not conduct criminal background screenings, it must so advise its New Jersey members, clearly and conspicuously, in bold, 12-point capital letters. The disclosure must be made by e-mails sent or received by a New Jersey member, on the profile describing a member to a New Jersey member and on the web page used when a New Jersey member signs up. If, however, the service does conduct background screenings, it must disclose prominently whether it has a policy of allowing members identified as having criminal convictions to have access to its service to communicate with a New Jersey member. It must also state that criminal background screenings are not foolproof, that criminals may circumvent even the most sophisticated search technology and that only publicly available convictions are included in the screening. The bill includes a safe harbor for Internet service providers who serve as intermediaries for the transmission of electronic messages among members of an Internet dating service. Violations of the bill would be a violation of the state Consumer Fraud Act, N.J.S.A. 56:8-1 et seq. The bill has been sent to the Assembly for consideration. If enacted, the bill would make New Jersey the fourth state to enact

such legislation; Florida, Michigan and Texas have enacted similar bills.

CYBERCRIMES AGAINST CHILDREN

The Florida Legislature (Senate on March 7, House on March 8) passed S. 1004, a bill which would enhance the penalties for possession of child pornography when the offender possesses 10 or more images and at least one of those images is of a child under five years of age. It also would expand the scope of the investigative and prosecutorial authority of the Attorney General's Office of Statewide Prosecution to include violations of ch. 827, F.S. (concerning abuse of children) when the crime is facilitated by use of the Internet or an electronic data storage or transmission device. The bill would also create a new felony offense of traveling to meet a minor for the purpose of committing unlawful sexual conduct with a child. In addition, it would require sex offenders to register any e-mail address and instant message (IM) names with the Florida Department of Law Enforcement (FDLE) prior to using it, and authorizes FDLE to provide those e-mail addresses and IM names to social networking sites so they can screen for them. The bill expressly states that it does not impose civil liability on the social networking sites.

SEXUAL PREDATORS

North Dakota Governor John Hoeven signed HB 1216 and 1217 and SB 2029 into law on April 3, strengthening the state's

penalties, probation and commitment for sexual predators. HB 1216 imposes a minimum 20-year sentence and lifetime supervised probation, including first-time offenses, for violent sex offenders. The bill also increases the penalty, and allows state attorneys more opportunity to prosecute, individuals who commit sexual offenses against minors. HB 1217 allows for a more flexible determination of a sexual disorder or tendency to commit sexual crimes in civil commitment cases. SB 2029 increases the penalties for violating restrictions set by a court, parole board or law enforcement for Global Positioning System (GPS) monitoring.

SEX OFFENDER REGISTRATION

On March 15, Mississippi Governor Haley Barbour signed HB 1015 into law, a bill that amends the state's sex offender registration law to conform to the Adam Walsh Act. Among its provisions is that it requires the submission of palm prints in addition to fingerprints, in addition to requiring a current photograph on every reregistration. The bill makes kidnapping of a child under 18 years of age a registrable offense. In addition, sex offenders are required to obtain a new driver's license, permit or identification card that identifies the individual as a sex offender.

On March 23, Kentucky Governor Ernie Fletcher signed SB 65 into law, a bill that expands the information a sex offender must provide during registration. The new law requires sex offenders in the state to also register their e-mail addresses and any instant messaging, chat or other Internet communication identities with the State Police Sex Offender Registry.

INTERNET SALES TAX

Washington Governor Christine Gregoire signed S. 5089 into law on March 29, legislation which would authorize the state to join the project with 21 other states advocating having Internet and catalog companies collect and distribute sales taxes. The project was started in 2000 by national tax and government associations, including the National Governors Association and the National Conference of State Legislatures.

TRADEMARKED KEYWORDS

Utah Governor Jon Huntsman, Jr. signed SB 236 into law, a bill which effectively prohibits the competitive use of trademarked terms as keyword advertising triggers. The new law establishes "an electronic registration mark that may not be used to trigger advertising for a competitor and creates a database for us in administering marks."

TOOLS YOU CAN USE

Information Technology Security Guidance

"Law Enforcement Tech Guide for Information Technology Security," provides strategies, best practices, recommendations and ideas for

developing security policies. The COPS publication will help to identify and assess risks and provide ideas for mitigating these risks. It can be accessed at:

<http://www.cops.usdoj.gov/mime/open.pdf?Item=1969>.

HOLD THE DATE

ADVANCED TRAINING ON SPYWARE/PHISHING SET FOR AUGUST

An Advanced Training on “What Prosecutors Need to Know About Spyware and Phishing: Approaches to Prosecution and Pitfalls to Avoid” will be held on August 28-30 at the University of Mississippi School of Law under the partnership between the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL) at the University. The course will be offered at no cost to prosecutors from Attorney General offices.

The training will include sessions on state legislative approaches to spyware and phishing, privacy issues and tools and techniques for investigating these crimes. Attendees will also hear from state prosecutors across the country who have “been there and done that” in handling these crimes.

Registration materials will be available in June. For additional information, please contact Hedda Litwin, Cyber Crime Counsel at NAAG, at hlitwin@naag.org or (202) 326-6022.