



Issue 21

**News Highlights in This Issue:**

34 AGs Settle With Online Marketer	3
No Conviction for Child Pornography in Cache	8
List of World's Top 10 Spammers Released	13
North Carolina Sex Offender Law Effective	15
Guide to Managing Sex Offenders Available	16
CAN-SPAM Act Preempts Oklahoma Spam Law	8
Scammers Targeting Wealthier "Phish"	12
Michigan Legislature Approves Data Breach Law	15
Free Cyber Crime 101 Training Offered in April	16
Third Party Ad Publisher Not Liable Under CDA	9
Investor Alert Issued for E-Mail Stock Scams	12
University E-Mail Restrictions Constitutional	10
ABA, Maryland Bar Say Use of Meta Data Ok	14
Both Parties Must OK Marital Computer Search	7
List of Top 20 Hacking Targets Released	13
Congress Passes Cross Border Safe Web Act	15
CFAA Allows Civil Suits for All Violations	10
Changes to Federal Rules Effective	14
4 <sup>th</sup> Amendment Protects Border Laptop Search	7
Countries With No Internet Freedom Listed	12
Pulitzer Prize to Allow Online Submissions	14

**Table of Contents**

<b><u>Features</u></b>	
NH AG Reports on State Cyber Crime	2
Free Cyber Crime 101 Course Offered	16
<b><u>AGs Fighting Cyber Crimes</u></b>	3
34 AGs Settle With Online Marketer	
AG King Adds ICAC Agents in North	
AG Goddard Sues Bogus Web Site Seller	
Florida AG Settles Problems With AOL	
AG Bennett's Agents Arrest Child Predator	
AG Wasden Issues Net Safety Publications	
AG Madigan's ICAC Unit Arrests Predator	
Kentucky AG's Agents Seize Internet Drugs	
Michigan AG: Internet Predator Arrested	
AG Hood: Child Pornographer Arrested	
AG Ayotte Speaks at Award of Net Grant	
AG Rabner Writes Social Networkers	
Pennsylvania AG: Predator Pleads Guilty	
AG McMaster Announces Predator's Arrest	
Texas AG Says 3 Online Predators Indicted	
AG Shurtleff Says Two Predators Arrested	
Virginia AG Proposes Sex Offender Law	
AG McKenna Settles Spyware Case	
West Virginia AG Sues Internet Lenders	
<b><u>In the Courts</u></b>	7
Marital Computer Search Needs 2 Consents	
Reasonable Suspicion Needed for Border Search	
Merely Looking at Child Pornography Legal	
No Conviction for Child Pornography in Cache	
CAN-SPAM Preempts Oklahoma Spam Law	
Only Original Defamer Can Be Liable Under CDA	
Third Party Publisher Not Liable Under CDA	
Web Site Booking Doesn't Confer Jurisdiction	
University E-mail System Constitutional	
CFAA Authorizes Civil Suits in All Provisions	
<b><u>News You Can Use</u></b>	11
Survey: Corporate Data Loss Prevalent	
NY Committee: Lawyer Blogs Are Ads	
Asia-Pacific Domain Approved	
DC Expands Civil Case E-Filing	
E-Mail Stock Scam Alert Issued	
"Enemies of the Internet" Released	
Survey: Scammers Targeting Richer Phish	
World's Top 10 Spammers Listed	
Study: Most Web Queries Not Explicit	
Top 20 Hacking Targets Identified	
Portland, OR to Get Wireless Network	
ABA, Maryland Bar: Meta Data Use OK	
Pulitzer Prize Allows Online Submission	
Changes to Federal Rules Effective	
<b><u>Legislation Update</u></b>	15
Congress Passes Cross-Border Crime Bill	
North Dakota Sex Offender Law Effective	
Michigan Senate Approves Data Breach Bill	
<b><u>Publications</u></b>	16
Sex Offender Management Guide	

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

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

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

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

---

**ATTORNEY GENERAL REPORTS ON  
CYBER CRIME IN  
NEW HAMPSHIRE**

By Tom Ralph<sup>1</sup>

Attorney General Kelly Ayotte has reported on the results of a survey commissioned by her office to determine the impact of cyber crime on law enforcement in New Hampshire. The survey, conducted by Justiceworks at the University of New Hampshire, was a continuation of an effort by Attorney General Ayotte and the New Hampshire Cyber Crime Initiative (NHCCI) to determine the nature and extent of cyber crime in the state and is a direct result of the strategic plan to address cyber crime that was adopted by the NHCCI in 2004.

An analysis of the data received indicated that, as in pervious years, theft and fraud

constitute more than 65 percent of the cyber offenses most often faced by New Hampshire law enforcement. Stalking and criminal threatening constituted another 20 percent of reported offenses, and enticement and child pornography accounted for approximately five percent. In nearly all categories, the number of reports of cyber crime offenses increased significantly in 2005 as compared with previous years. Attorney General Ayotte reports that these increases are being addressed in the Strategic Plan by a combination of advanced and in service training for law enforcement, practical training for prosecutors, and a distributed forensic analysis project that is projected to reduce turnaround time from months to days for a trained investigator.

<sup>1</sup>Tom Ralph is an Assistant Attorney General in the Office of the Attorney General of New Hampshire.

# AGs FIGHTING CYBER CRIMES

---

## MULTI-STATE

**Attorneys General of 34 states** reached a \$2 million settlement with YP Corporation to resolve claims that the company deceived consumers by automatically signing them up for its online yellow pages. The company, also doing business as YP.com and Telco Billing, Inc., mailed checks for a small amount, usually \$3.50, to businesses, churches and government agencies. Any organization that deposited the check was automatically signed up for the online yellow pages service and billed \$27.70 to \$39.95 a month on their phone bill. In some cases, YP withdrew the monthly fee directly from their checking accounts. The settlement agreement orders YP.com to cease sending checks to market its services. YP must also pay \$2 million to the states to be used for consumer refunds, as well as send letters to all current customers giving them the opportunity to cancel the service and receive a refund for the past two months' worth of charges. Participating states in the settlements were: Alaska, Arizona, Arkansas, California, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Kansas, Kentucky, Louisiana, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, North Dakota, Oregon, Pennsylvania, South Carolina, Tennessee, Texas, Washington, West Virginia and Wyoming.

## ALABAMA

**Attorney General Troy King** announced that his office will increase the Internet Crimes Against Children (ICAC) Task Force in North Alabama by having an agent in that area who will work out of the Madison County Sheriff's Office, as well as two of his other agents in Montgomery who are assigned to the ICAC program. Attorney General King was joined by Major Ken Hallford, Alabama Bureau of Investigation Chief, and Blake

Dorning, Madison County Sheriff, in making the announcement.

## ARIZONA

**Attorney General Terry Goddard** filed suit against Guaranteed Prescriptions Pharmaceutical Wealth Network which allegedly sold bogus pharmaceutical web sites to consumers. Named in the lawsuit were Brent Emerson, Louisa Gore, Anthony and Lisa White and Gary Murdie. The company, which also did business as National Pharmaceutical Network, Executive Marketing Group, Premier Marketing Group and VIP Marketing, used the Internet, direct mailers and telemarketing to solicit consumers. They claimed that an at-home business selling discounted prescription drugs online could be purchased for under \$1,000 and would earn thousands of dollars. Defendants then used high pressure sales tactics to persuade purchasers to buy additional advertising for thousands of dollars. Few purchasers made money from the sites. The suit alleges violations of the state Consumer Fraud Act and racketeering statutes. A temporary restraining order suspending the company's operations was issued. The suit asks the court to prohibit defendants from selling web sites, require them to return any money or property acquired by deceptive practices, impose a penalty of up to \$10,000 for each violation of the Consumer Fraud Act, prohibit defendants from liquidating or selling assets and order forfeiture of assets to pay restitution, and require defendants to pay investigation costs.

## FLORIDA

**Attorney General Charlie Crist** reached a settlement with America Online (AOL), which will provide restitution for state consumers who have experienced billing and membership problems with the Internet service provider. Attorney General Crist began investigating the company after getting

more than 1,000 complaints about erroneous charges, cancellation requests that were ignored and accounts that were reactivated without permission. AOL did assist in the investigation by identifying consumers who were harmed. Approximately \$330,000 in restitution is available.

## **HAWAII**

**Attorney General Mark Bennett** announced that law enforcement agents from the Hawaii Internet Crimes Against Children Task Force (HICACTF) arrested Brian Uejo for Electronic Enticement of a Child in the First Degree. Uejo asked the person he met online that he thought was a 15-year-old girl to meet him for sex. He was arrested after he arrived at the meeting place. As a result of Act 80, Session Laws of Hawaii 2006, the crime carries a mandatory jail term of one year.

## **IDAHO**

**Attorney General Lawrence Wasden** released two Internet safety publications. The Parent's Guide to Social Networking describes the nature and content of social networking web sites and the risks of unsupervised use of the sites by young people. The booklet also discusses how parents can determine if their children are using those sites, how they can discuss the issue with their children and how to delete a social networking account. The 36-page Internet Lingo Dictionary lists more than 500 common Internet acronyms and their meanings. Both publications are available in English and Spanish on Attorney General Wasden's web site.

## **ILLINOIS**

**Attorney General Lisa Madigan's** Internet Crimes Against Children (ICAC) Task Force assisted the Winfield Police Department in arresting Jorge Paniagua when he attempted to meet and have sex with what he believed to be a child, but was actually an undercover police detective that he met in an Internet chat room. Paniagua was charged

with one count of Indecent Solicitation of a Child, a Class 3 felony, punishable by a maximum of five years in the Illinois Department of Corrections. Following the arrest, a search warrant was issued for Paniagua's computers, and a forensic search of the computers will be conducted by Attorney General Madigan's office.

## **KENTUCKY**

**Attorney General Greg Stumbo** announced that Kentucky Bureau of Investigation (KBI) agents seized shipments of illegal Internet drugs at shipping hubs in central and eastern Kentucky. An ongoing investigation revealed that AVEE, a licensed out-of-state pharmacy, was illegally shipping drugs to state residents. The KBI confiscated 10,656 pills, including 7,865 Hydrocodone tablets, with a street value of nearly \$89,000. This seizure puts the KBI over the \$1,000,000 mark in contraband confiscation.

## **MICHIGAN**

**Attorney General Mike Cox** announced the arrest of Fred Damron on charges of soliciting a minor over the Internet and distributing lewd material to a minor. The arrest was made by investigators from the U.S. Secret Service assigned to the Michigan Internet Crimes Against Children (ICAC) Task Force. Damron allegedly engaged in graphic sexual conversation and solicited sexual activity in an online chat room with an undercover Secret Service agent posing as a 13-year-old girl. On one occasion, he sent the agent lewd digital images of adult pornography. Damron was arraigned on three counts of Using a Computer to Arrest and Solicit a Minor, a 10-year felony, and one count of Using a Computer to Disseminate Sexually Explicit Matter to a Minor, a four-year felony.

## **MISSISSIPPI**

**Attorney General Jim Hood** confirmed that Walter Woodland was arrested on 10 counts of possession of child pornography on the Internet, in violation of Mississippi Code Ann. 1972, as

amended, § 97-5-33(5). He was arrested by the Lauderdale County Sheriff's Office following an indictment by the Lauderdale Grand Jury. Based on a Cybertip from the National Center for Missing and Exploited Children, Attorney General Hood's Cyber Crime Unit conducted the investigation and will prosecute the case.

## MISSOURI

**Attorney General Jay Nixon** filed suit against Jennifer Lutke, the owner of Doxy Lingerie, an Internet lingerie business, for accepting payment for online orders of lingerie, but failing to deliver the goods for weeks or months. Customers were told that their orders would be shipped within two weeks and were given an order number to track the merchandise. However, although consumers' credit cards were charged immediately, consumers waited weeks or months for their orders, and many orders never arrived at all. Consumers were also unable to track their orders online. Attorney General Nixon's office and the St. Louis Better Business Bureau received approximately 90 complaints about Doxy from consumers all across the country. Attorney General Nixon is asking the court to grant a temporary restraining order and preliminary and permanent injunctions prohibiting Lutke from advertising and operating a business in the state. The suit also asks the court to order Lutke to pay restitution to consumers suffering a loss, to pay an amount equal to 10 percent of the total restitution into the Missouri Merchandising Practices Revolving Fund, to pay civil penalties of up to \$1,000 per violation of state consumer laws, and to pay the costs of investigating and prosecuting the case.

## NEW HAMPSHIRE

**Attorney General Kelly Ayotte** was a featured speaker at a special town meeting in which Verizon announced a \$150,000 award to support the work of the University of New Hampshire's Crimes Against Children Research Center. The grant will support the Center's work on Internet security issues and best practices in protecting children online.

## NEW JERSEY

**Attorney General Stuart Rabner** sent a letter to the chief executive officers of 10 social networking sites, asking them to work cooperatively to adopt technology that would make their services safer for children. He encouraged companies to place a readily identifiable icon on each page of their respective web sites that would allow users to quickly report inappropriate or suspicious activity such as sexual or predatory content. Those reports would alert both the site and law enforcement of potential criminal behavior. Attorney General Rabner's letter was sent to executives of MySpace.com; Facebook, Inc.; Friendster; Xanga.com; LiveJournal.com; Bebo, Inc.; Tagged, Inc.; BlackPlanet.com; MyYearbook.com; and TagWorld.

## PENNSYLVANIA

**Attorney General Tom Corbett** announced that Melvin Miller had pled guilty to five counts of attempted criminal unlawful contact with a minor and one count of criminal use of a communication facility. Miller was arrested after he accessed an online chat room and instant message program to contact what he believed was a 13-year-old girl but was actually an undercover agent in Attorney General Corbett's office. In exchange for the plea, prosecutors dismissed a count of criminal solicitation of unlawful contact with a minor. Miller faces three to 14 months in prison for each of the six counts.

## SOUTH CAROLINA

**Attorney General Henry McMaster** announced the arrest of William Bishop in an undercover Internet sting conducted by the Spartanburg County Sheriff's Office, a partner in Attorney General McMaster's Internet Crimes Against Children (ICAC) Task Force. Bishop was arrested on one count of Criminal Solicitation of a Minor, a felony punishable by up to 10 years imprisonment, and one count of Attempted Criminal Sexual Conduct With a Minor, a felony punishable by up to 20 years imprisonment. Bishop

chatted online with what he thought was a 13-year-old boy, but was actually an undercover agent, and offered the “boy” money to put him in contact with a girl of the same age. He then solicited sex online from the “girl,” another undercover agent. The case will be prosecuted by Attorney General McMaster’s office.

## TEXAS

**Attorney General Greg Abbott** announced that three men were indicted on attempted sexual assault charges after being arrested for allegedly soliciting sex from teenagers on the Internet. Guadalupe “Wally” DeLaGarza III, Robert Ramirez and William Shrum had been arrested in a joint investigation by Attorney General Abbott’s Cyber Crimes Unit and the Shenandoah Police Department. The men used chat rooms and web sites, including MySpace, to arrange meetings with what they thought were young girls but were actually undercover agents.

## UTAH

**Attorney General Mark Shurtleff** announced that the Utah Internet Crimes Against Children (ICAC) Task Force, which his office oversees, arrested Raymond Janes and Michael Rogers for using computers to exploit children. Janes, who was arrested after ICAC investigators found child pornography on his home computer, is being held on 18 counts of sexual exploitation of a minor. He may face additional charges pending a forensic examination of his computer. Rogers is accused of arranging on the Internet to have sex with an underage person and then traveling to meet the intended victim.

## VIRGINIA

**Attorney General Bob McDonnell** will propose legislation to require convicted sex offenders in the state to register their e-mail addresses and Instant Messaging (IM) identities with the state’s Sex Offender Registry. It is anticipated that such a database would enable social

networking sites to delete and/or block registered addresses from accessing their sites. State Senator Ryan McDougle, a member of Attorney General McDonnell’s Youth Internet Safety Task Force, is the expected patron of the legislation.

## WASHINGTON

**Attorney General Rob McKenna** reached a \$1,000,000 settlement with New York-based Secure Computer that resolves the state’s first lawsuit under its computer spyware law. Attorney General McKenna accused the company of marketing Spyware Cleaner software to consumers by falsely claiming that their computers were infected with spyware. Under the consent decree, Secure Computer will pay \$200,000 in civil penalties, \$75,000 in restitution for consumers and \$725,000 in attorney’s fees and costs. An estimated 1,145 state residents will be eligible for refunds.

## WEST VIRGINIA

**Attorney General Darrell McGraw** filed suit to enforce investigative subpoenas against 14 Internet payday lenders and to enjoin their lending activities in the state. The lenders allegedly made usurious “payday” loans to consumers via interactive web sites. Such loans are short term loans or cash advances, typically for 14 days, secured by a postdated check or by an agreement authorizing an electronic debt in the full loan amount plus interest from the customer’s account. The companies sued deposited the loans electronically into consumers’ accounts and required payment of interest ranging from 600 to 800 Annual Percent Rates (APR), more than 44 times the maximum allowable rate of 18 APR in the state. Attorney General McGraw’s office also reached formal settlement agreements with 18 other Internet payday lenders in which they promised to permanently discontinue their payday loans and refund all unlawful fees and charges collected.

# IN THE COURTS

---

## **SEARCH AND SEIZURE: MARITAL COMPUTER**

*U.S. v. Hudspeth*, 459 F.3d 992 (8<sup>th</sup> Cir. August 25, 2006). The 8<sup>th</sup> Circuit Court of Appeals found that the warrantless seizure of a marital computer, where the husband refused to give permission but the wife consented, was illegal. As part of a prescription drug investigation, the Missouri State Highway Patrol searched the offices of Handi-Rak Services. They found some hand-labeled CDs in CEO Roy Hudspeth's office that appeared to contain child pornography. An officer asked for permission to search Hudspeth's home computer, but Hudspeth refused. Officers then went to his home, identified themselves to his wife and asked to search their computer. They did not tell her that her husband had refused permission. After an unsuccessful attempt to reach their lawyer, and threats by the officers that they would stay until a search warrant could be obtained, the wife eventually granted permission to seize the computer. The U.S. District Court for the Western District of Missouri nevertheless ruled that the wife's consent was voluntary and not coerced, and Hudspeth was convicted. On appeal, the 8<sup>th</sup> Circuit agreed the wife voluntarily gave consent, but found that the police must get a warrant if one co-occupant denies consent to search. They concluded that the wife's consent did not overrule her husband's denial. The case was remanded for further proceedings.

## **SEARCH AND SEIZURE: BORDER SEARCHES OF LAPTOPS**

*U.S. v. Arnold*, 2006 Dist. LEXIS 73311 (C.D. Cal. October 2, 2006). In a case of first impression in Ninth Circuit courts, the U.S. District Court for the Central District of California ruled that the Fourth Amendment requires law enforcement to have reasonable suspicion to search a laptop at U.S. borders. When Michael Arnold arrived at Los Angeles International Airport from overseas, Customs and Border Patrol offices searched his laptop, hard drive, CDs and memory stick. Arnold was indicted for transportation of child pornography and possession of a computer hard drive and CDs containing images of child pornography. He moved to suppress the evidence, and the government argued that a border search of a computer is not subject to Fourth Amendment protection. The district court disagreed, finding that the search of one's private information stored on a computer is no less deserving of Fourth Amendment scrutiny than a strip body search. The court concluded that the government did not have the requisite reasonable suspicion that Arnold's computer contained evidence of a crime. Arnold's motion was granted.

*Ed. Note:* In our September-October issue, we reported on the case of *U.S. v. Romm*, 2006 U.S. App. LEXIS 18474 (9<sup>th</sup> Cir. July 24, 2006) where the court reached the opposite result. In that case, a unanimous three-judge panel of the 9th Circuit Court of Appeals ruled that U.S. customs agents may conduct random warrantless searches of travelers' laptops regardless of

*reasonable suspicion or probable cause. The case is distinguishable in that Customs agents had probable cause to believe the computer contained child pornography because Canadian officials had conducted a search and denied Romm entry.*

### **CHILD PORNOGRAPHY: KNOWING POSSESSION**

*Commonwealth v. Diodoro*, No. 1889 (Pa. Super. Ct. November 2, 2006). In a case of first impression, a three-judge panel of the Pennsylvania Superior Court concluded that merely looking at child pornography on the Internet, without intentionally saving or downloading the images, does not constitute “knowing possession” of child pornography as prohibited by Section 6312(d) of the state’s Crimes and Offenses Code. Anthony Diodoro admitted to intentionally visiting specific web sites where he viewed several hundred photographs of child pornography. The trial court imposed a sentence of nine to 23 months in jail following his conviction on 30 counts of possession of child pornography. On appeal, the Superior Court noted that the prosecution was never able to show evidence that he intentionally downloaded or saved the images, or that he was aware the images were automatically added to his Internet browser’s cache. The court, after reviewing applicable state and federal law, found no case holding that mere viewing of child pornography is illegal. The decision was reversed and Diodoro was released.

### **CHILD PORNOGRAPHY: INTERNET CACHE FILES**

*United States v. Kuchinski*, No. 05-30607 (9<sup>th</sup> Cir. November 27, 2006). The Ninth Circuit Court of Appeals decided that a defendant cannot be convicted on child pornography charges based on possession of images found in his computer’s Internet cache files unless there is knowledge that the computer automatically saved the images from web site the defendant visited. John Kuchinski was convicted for receipt and possession of child pornography in the U.S. District Court for the District of Montana. His sentence included significant enhancements based on the numbers of images involved, which included images found in his cache files as well as images Kuchinski admitted he intentionally saved on his computer. On appeal, Kuchinski argued that only the images he intentionally saved on his computer should be used in sentencing, because there was no evidence that he tried to access the cache files or even knew they existed. The Ninth Circuit agreed, stating it was not proper to charge Kuchinski with possession and control of images in the cache files without an indication of his control over the images. The court upheld his conviction, but sent the case back to the district court for resentencing.

### **CAN-SPAM ACT: PREEMPTION**

*Omega World Travel, Inc. v. Mummagraphics, Inc.*, 2006 U.S. App. LEXIS 28517 (4<sup>th</sup> Cir. November 17, 2006). The Fourth Circuit has ruled that the CAN-SPAM Act preempts Oklahoma’s anti-spam law. Mark Mumma, owner of Mummagraphics, an Oklahoma-based provider of online

services and operator of anti-spam web sites, complained to Virginia-based Omega World Travel and its owners after receiving 11 e-mails from them for cruise vacations, although he did not avail himself of the opt-out e-mail address contained in the e-mails. When he failed to receive satisfaction, Mumma posted derogatory pictures of Omega's owners on his anti-spam web sites. Omega sued for defamation, and Mumma counterclaimed under both the federal CAN-SPAM Act and the Oklahoma anti-spam statute. The U.S. District Court for the Eastern District of Virginia ruled that the CAN-SPAM Act preempted Oklahoma's law and that there was no violation of the CAN-SPAM Act because the alleged inaccuracies in the Omega e-mails were not material and did not rise to the level of being "materially" false or misleading as required by the Act. On appeal, the Fourth Circuit upheld the district court's decision.

**COMMUNICATIONS DECENCY  
ACT: BLOGGER LIABILITY**

*Barrett v. Rosenthal*, No. S122953 (Cal. November 20, 2008). The California Supreme Court overturned a lower court ruling by interpreting Section 230 of the Communications Decency Act (CDA) to apply to "distributors" of online content so that only the originator of a defamatory statement published on the Internet can be held liable. Stephen Barrett and others, physicians against the use of alternative healthcare practices, brought libel claims against Ilena Rosenthal, Director of the Humantics Foundation for Women, as a result of postings she made to several Internet newsgroups denouncing Barrett's actions. Rosenthal moved to dismiss under the state's Anti-SLAPP statute,

which upholds the right to speak on a public issue, and the trial court agreed. On appeal, the Court of Appeals upheld the dismissal, but held Rosenthal liable for one potentially libelous statement she had posted regarding Barrett's alleged "stalking" of an opponent. Rosenthal petitioned the Supreme Court which found that none of Rosenthal's postings were defamatory.

**COMMUNICATIONS DECENCY  
ACT: THIRD PARTIES**

*Chicago Lawyers' Committee for Civil Rights Under the Law, Inc. v. Craigslist, Inc.*, No. 06C-0657 (N.D. Ill. November 14, 2006). Craigslist, the popular web site that publishes classified advertisements authored by third parties, was held to be immune from liability under the Communications Decency Act for publishing housing advertisements that allegedly violate the Fair Housing Act (FHA). The Chicago Lawyers' Committee for Civil Rights Under the Law Inc. (CLC), a consortium of law firms that seek to eliminate discriminatory housing practices, filed suit against Craigslist for violation of Section 3604© of the FHA which makes it unlawful to publish a discriminatory housing sale or rental. Craigslist moved to dismiss the complaint on the ground that Section 230© of the CDA, which provides that "...no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." In opposing the motion, the CLC argued that the CDA only immunizes an Internet service provider (ISP) for acts it voluntarily takes to restrict access to objectionable materials. The U.S. District Court for the Northern District of Illinois found that the CDA

immunized Craigslist from the FHA claims at issue because they sought to treat Craigslist as a publisher of the third party advertisements, which is expressly prohibited by the CDA.

### **CONFLICT OF LAW: WEB SITE TRANSACTIONS**

*Carris v. Marriott International, Inc.*, No. 06-1506 (7<sup>th</sup> Cir. October 15, 2006). The circuit court ruled that Bahamian law governs an Illinois resident's personal injury suit against a Bahamian resort, notwithstanding the fact that the reservation was booked on the resort's web site. Ted Carris of Illinois was injured in a jet skiing accident at the Nassau Marriott Resort. Carris had booked his reservation from the Marriott International web site. He sought to hold Marriott International responsible for negligence, but since it did not own the Nassau Marriott, he could not proceed on the theory of respondent superior. He instead argued in his suit that under Illinois law, liability could be imposed on a theory of apparent authority. Marriott moved to dismiss for failure to state a claim. The U.S. District Court for the Northern District of Illinois granted the motion, holding that Bahamian law, which did not recognize the apparent authority theory, governed the case. On appeal, the 7<sup>th</sup> Circuit affirmed, finding that under Illinois conflict of law principles, a dispute is governed by the law of the jurisdiction that has the most significant relationship to the events from which the suit arose. The fact that Carris booked his trip from a computer in Illinois did not alter the result.

### **FIRST AMENDMENT: FACULTY E-MAIL SYSTEM**

*Faculty Rights Coalition v. Shahrokhi*, No. 05-21098 (5<sup>th</sup> Cir. November 2, 2006). The Fifth Circuit Court of Appeals affirmed a district court's dismissal of a civil rights suit brought to test the free speech rights of college faculty on a state university's e-mail system. Adjunct professors at the University of Houston sued the University's director of information technology to challenge certain restrictions on their e-mail system including 1) disabling the send function upon exhaustion of account storage capacity, 2) the policy of disabling adjunct professors' access to e-mail accounts during the summer and 3) interception of non-commercial e-messages by the University's spam filter. The U.S. District Court for the Southern District of Texas granted summary judgment for the University, holding that 1) the University's e-mail system is not a public forum, 2) the e-mail storage capacity limits are necessary to protect system resources, 3) denial of access to part-time professors during the summer does not violate their equal protection rights and 4) interception of noncommercial e-mail by the University's spam filter does not violate the First Amendment because the University took corrective action to designate the originating address as legitimate. On appeal, the Fifth Circuit affirmed.

### **COMPUTER FRAUD AND ABUSE ACT: PRIVATE RIGHT OF ACTION**

*Fiber Systems International v. Roehrs*, 2006 WL 3378403 (5<sup>th</sup> Cir. November 22, 2006). The Fifth Circuit Court of

Appeals overturned a lower court ruling and found that the Computer Fraud and Abuse Act (CFAA) authorizes civil suits to enforce all of its provisions, not just the subsections specifically mentioned in its civil remedies subsection, 18 USC §1030(g). Fiber Systems alleged that former employees copied confidential information from its database in order to start a competitive business. It sought damages and injunctive relief under §1030(a)(4), (a)(5) and (g). Daniel Roehrs, the principal defendant, countersued for defamation. A jury granted Fiber Systems \$36,000 for the proven violations of the CFAA and \$100,000 apiece in compensatories and

\$1,000,000 apiece in punitives to the counter-claimants on their defamation claims. The trial judge in the U.S. District Court for the Eastern District of Texas entered a take-nothing judgment for Fiber Systems, holding that the CFAA does not create a civil cause of action for violations of subsection (a)(4). On appeal, the Fifth Circuit reversed, reasoning that §1030(g) extends the ability to bring a civil action to any person suffering damage or loss under “this section,” which refers to §1030 as a whole.

## NEWS YOU CAN USE

---

### **REPORT: CORPORATE DATA LOSS PREVALENT**

The Ponemon Institute released a report based on a survey of 850 corporate security practitioners in the United States that focused on how they deal with detection and prevention of data breaches. Although a majority of those surveyed said they could detect data breaches, 63 percent said they can't prevent the attacks. Many practitioners said that are affected by high false-positive rates of up to 35 percent, an operational flaw that negatively influences their detection capability. Additionally, 41 percent of the surveyed companies do not believe they are effective in enforcing their data security policies. The most cited reasons for failed enforcement is lack of resources and management's unwillingness to devote significant funds to security.

### **N.Y. PROPOSAL: LAWYER BLOGS ARE ADVERTISING**

“Computer-accessed communications,” such as blogs, should be included in New York's definition of legal advertising and therefore require state scrutiny, according to a proposal by a committee created by the state's Administrative Board of Courts. The proposal also recommends that the state code of professional responsibility extend court jurisdiction to out-of-state legal advertising that is seen in the state. Attorney discipline is a responsibility of the Board, which is composed of the chief justice of the Court of Appeals and the presiding judges of the four appellate divisions. After a public comment period, the Board will act on the proposal.

## **ASIA-PACIFIC DOMAIN APPROVED**

A “.asia” domain for Internet addresses, designed to unify businesses and other users in the Asia-Pacific region, has been approved by the Internet Corporation for Assigned Names and Numbers (ICANN). The new domain will be operated by the DotAsia Organization Ltd, an organization composed of groups that run domain names for China, Japan and other Asian countries. DotAsia said it will explore allowing suffixes in other languages and will restrict registrations to those in the region. The contract between ICANN and DotAsia has not yet been finalized, and registrations for English language names are not expected for another six to nine months. Prices will vary, with trademark holders getting priority.

## **DC EXPANDS E-FILING TO CIVIL II CASES**

Pursuant to Administrative Order 06-17 issued in May 2005, the Superior Court of the District of Columbia has begun phasing in electronic filing of Civil II cases. Although e-filing is currently voluntary, it will become mandatory for all parties represented by counsel as of February 5, 2007. Each party to a case that is represented by counsel must agree to file and serve all documents electronically; register with service provider CaseFileXpress; and e-file a Consent Notice of eFiled Case. If a case includes a pro se party, attorneys may still e-file to the court and e-serve one another, but service to the pro se party must be by hand or mail. A copy of the Order is available at <http://www.dccourts.gov/efiling>.

## **E-MAIL STOCK SCAM ALERT ISSUED TO INVESTORS**

The National Association of Security Dealers (NASD), the brokerage industry’s self-policing organization, issued an alert regarding the “I hope this is your e-mail” scam. The scam is the latest variant of a “pump and dump” scheme in which perpetrators tout small, thinly traded stocks to push up prices so they can sell their shares in those stocks at a profit. NASD said the e-mails are made to appear as though they were sent to the recipient in error and are often poorly worded. The alert included tips on how to investigate a stock before investing. NASD also urged recipients to forward stock spam e-mails to them at [spam@nasd.com](mailto:spam@nasd.com) for review and possible investigation.

## **ANNUAL LIST OF “ENEMIES OF THE INTERNET” RELEASED**

The annual list of 13 “enemies of the Internet” was released by human rights group Reporters Without Borders (RSB). The list consists of countries that RSB believes are suppressing freedom of expression on the Internet. This year Egypt was added to the list, while Nepal, Libya and the Maldives were removed. RSB also organized an online protest accompanying the list this year. The countries on this year’s list are, in alphabetical order: Belarus, Burma, China, Cuba, Egypt, Iran, North Korea, Saudi Arabia, Syria, Tunisia, Turkmenistan, Uzbekistan and Vietnam.

## **SURVEY: SCAMS TARGETING RICHER PHISH**

The size of the average phishing “take” has increased five-fold, from \$257 per victim last year to \$1,244 in

2006, according to a survey by analysts from technology research and consulting firm Gartner. Gartner analysts say that scammers are identifying higher income targets, often by obtaining credit card numbers in online chat rooms and identifying cards with higher spending limits by the first six digits on the card. According to Gartner, approximately 109 million U.S. adults have received phishing e-mail scams, up from 57 million in 2004. Total losses from phishing attacks have risen to \$2.8 billion in 2006, twice the amount lost in 2004. Gartner's survey found that adults earning more than \$100,000 per year received an average of 112 phishing e-mails each in 2006, compared to 74 e-mails per consumer across all other income brackets. On average, the high-income adults lost \$4,362 each, almost four times as much as other victims.

### **WORLD'S TOP 10 SPAMMERS LISTED**

A revised list of the world's 10 most prolific spammers has been published by anti-spam organization Spamhaus. Four of the spammers in Spamhaus' Register of Known Spam Operations (ROKSO) database are from Russia; two are from the United States; and Canada, Hong Kong, Israel and the Ukraine each house one top spammer. Public spam enemy number one is a Ukrainian known as Alex or Alexei, a prolific user of botnets (networks of PCs compromised with malware), who works in association with Pavka/Artofit, a Russian spam gang. The complete list can be accessed at <http://www.spamhaus.org/rokso/index.la.sso>.

### **STUDY: NOT AS MUCH ADULT CONTENT ON WEB AS THOUGHT**

A confidential analysis of Internet search engines commissioned by the U.S. Department of Justice found that only about one percent of web pages contain sexually explicit materials. The study, which also included a random sample of web pages taken from Google and Microsoft's Internet indexes, was part of an effort by the Justice Department to prove that criminal penalties are necessary to protect minors from exposure to sexually explicit information on the Internet. The analysis was performed by Philip Stark, a professor of statistics at the University of California Berkeley. It found that only six percent of all queries returned a sexually explicit web site, despite the consistent popularity of queries related to sex. It also found that the filters that were most effective at blocking sexually explicit content also inadvertently blocked a substantial amount of content that was not explicit.

### **TOP 20 HACKING TARGETS IN 2006 NAMED**

The Sans Institute, a provider of information security training and certification, named its 20 most vulnerable computer applications for 2006. Included on the list are Microsoft Internet Explorer, Microsoft Office, Windows Libraries and Services and Apple Computer's Mac OS X. The list is written by SANS Institute members as well as security experts from the technology industry and government agencies. It seeks to identify network features that could leave a company vulnerable to attack. The complete list can be accessed at <http://www.sans.org/top20/?ref=1487>.

## **PORTLAND, OREGON TO GET WI-FI NETWORK**

Microsoft and Mountain View's MetroFi are teaming up to build a citywide Wi-Fi network in Portland, Oregon that will provide free wireless to residents using an ad-supported model. Under the deal, Microsoft will create a home page for wireless users that features local news and content and will also help to procure advertisers for the network using its online ad service. The network will span 134 square miles, serving 95 percent of the city's 540,000 residents. Users will get download speeds of one megabit per second. MetroFi users will be able to sign on to the network using a Wi-Fi enabled laptop or Internet device. A one-inch ad bar will appear at the top of their screen when they browse, but Microsoft will offer an ad-free service with full customer support for \$20 a month.

## **ABA, MARYLAND BAR: LAWYERS CAN USE META DATA**

Lawyers have no ethical duty to refrain from reviewing and using meta data embedded in e-mail and other electronic documents received from opposing counsel or adverse parties, according to the American Bar Association (ABA) Standing Committee on Ethics and Professional Responsibility Formal Opinion No. 06-442. The committee advised that attorneys who are worried about the possibility of hidden meta data being revealed in a document can take steps to reduce that risk. Essentially the same conclusion was reached by the Maryland Bar Association, Inc. Committee on Ethics in its opinion docketed as No. 2007-09 entitled "Ethics of Viewing

and/or Using Metadata." Both opinions can be accessed at <http://ddee.pf.com>.

## **PULITZER PRIZE TO ALLOW ONLINE MATERIAL SUBMISSION**

Entries for the 2007 Pulitzer Prizes may contain online material such as video, blogs, databases and interactive graphics for all print categories. The Pulitzer Prize Board allowed online material as part of all entries for this year's awards, but limited it to written stories or still images in 13 of the 14 categories. The only exception was the Public Service category, which has allowed material such as streaming video and databases since 1999. The new rules apply to work done during 2006 for prizes awarded in 2007. The deadline for entries is February 1, 2007, and prizes will be announced on April 16, 2007.

## **CHANGES TO FEDERAL RULES EFFECTIVE**

The long-awaited changes to the Federal Rules of Civil Procedure to address issues arising from the discovery of electronically stored information (ESI) are now effective. Among the notable changes are:

Rule 26(b)(2): A party must provide discovery of relevant reasonably accessible ESI without a court order. A party may file a motion to obtain a court order to gain access to electronic information that is not reasonably accessible to the responding party, and a court may order the responding party to provide the information, but only on a showing of good cause. The rule also establishes a procedure applicable when a responding party asserts that it has inadvertently produced privileged

information without intending to waive the privilege. Finally, the rule allows for a post-production assertion of privilege and requires the return, sequestration or destruction of the material in question pending resolution of the privilege claim.

Rule 33: An answer to an interrogatory involving review of business records should involve a search of ESI and allow the responding party to respond by giving access to that information.

Rule 34: Parties must frame discovery requests to specify whether they are seeking discovery documents, ESI or both.

Rule 37: Provides a narrow safe harbor to protect a party from discovery sanctions for failing to provide ESI lost because of the routine, “good faith” operation of the party’s computer system that causes automatic recycling, overwriting or other.

## LEGISLATION UPDATE

---

### **CROSS-BORDER SPAM, SPYWARE AND FRAUD**

On December 9, 2006, the U.S. House of Representative’s passed S. 1608, known as the SAFE WEB Act of 2005. The legislation, aimed at enhancing the Federal Trade Commission’s (FTC’s) enforcement of cross-border spam, spyware and fraud, had already passed the U.S. Senate. The bill authorizes the FTC, upon request of a foreign law enforcement agency, to provide investigative assistance and to disclose certain privileged or confidential information about an investigation. It also authorizes the FTC to designate its attorneys to assist the U.S. Attorney General with litigation in foreign courts.

### **INTERNET PREDATORS**

On December 1, 2006, North Carolina’s new sex offender law went into effect requiring sex offenders to register for a minimum of ten years and to remain on the Sex Offender Registry for life unless they are removed by the court. Sex offenders are also

barred from living within 1,000 feet of a school or child care center and from working or volunteering where children are present. In addition, offenders must now register with sheriffs every six months in person, rather than once a year by mail as the previous law required. They must give advance notice if they plan to move to another state. The new law makes it a felony for someone to assist a sex offender in avoiding registration, and it directs the Department of Correction to track the worst offenders using global positioning satellite information. Attorney General Roy Cooper was instrumental in urging the enactment of the legislation.

### **SECURITY BREACHES**

On December 14, 2006 the Michigan Senate approved SB 309, a bill that requires notification of a security breach of a database that contains personal information. The bill amends the state’s Identity Theft Protection Act to make individual notification of serious breaches mandatory and subject to steep penalties if violated.

# PUBLICATIONS

---

## **LAW ENFORCEMENT GUIDE TO MANAGING SEX OFFENDERS RELEASED**

“Managing Sex Offenders: Citizens Supporting Law Enforcement,” a resource guide for law enforcement on sex offender management, has been released by the U.S. Department of Justice’s Bureau of Justice Assistance. It highlights relevant sex offender legislation impacting law enforcement,

identifies emerging operational challenges and offers examples of how law enforcement agencies are using citizens to enhance and support their sex offender management and enforcement efforts. Law enforcement initiatives on sex offender database management and on protecting children on the Internet are included. The guide can be accessed at: [http://www.ojp.usdoj.gov/BJA/pdf/CISOM\\_Resource\\_Guide.pdf](http://www.ojp.usdoj.gov/BJA/pdf/CISOM_Resource_Guide.pdf).

# ANNOUNCEMENTS

---

## **BACK BY POPULAR DEMAND!!!! FREE CYBER CRIME 101 TRAINING OFFERED IN APRIL**

Cyber Crime 101, a basic cyber crime course for attorneys who want to get up to speed on computer crimes and electronic evidence, will once again be offered at no charge to Attorneys General offices on April 24-26, 2007 at the University of Mississippi. Airfare to attend the training will be reimbursed, and most meals will be provided. The course, sponsored by the partnership between the National Association of Attorneys General and the National Center for Justice and the Rule of Law at the University of Mississippi School of Law, is ideal for new Attorneys General and Chief Deputies, as well as prosecutors who will be joining a cyber crime unit or who need more experience with digital evidence.

The course will include sessions on the search and seizure of electronic evidence, prosecution issues in computer crime cases, the impact of the Electronic Communications Privacy Act (ECPA) and discussions about the computer crimes encountered by Attorney General Offices, such as online predators, Internet auction fraud, hacking and phishing.

Please watch your e-mails, as well as future issues of this Cyber Crime E-Newsletter, for registration information for the course.