

News Highlights in This Issue:

Fifty AGs Enter Agreement with MySpace	3
South Dakota Online Sales Tax Bill Endorsed	7
Pointing Cell Phone Camera is Intimidation	10
Missouri Internet Stalking Bill Advances	8
High Court Hears Patent Royalty Case	13
Report: 47 Percent of Adults Self-Googleing	14
Managing Backlogged Crime Lab Report Available	20
Florida Spyware Legislation Pre-File	7
ISP Cannot Reveal Anonymous Blogger's Identity	10
Two Studies: Increase in Online Financial Crime	14
Georgia House Passes Security Freeze Bill	7
Enhanced Sentence for Net Pharmacist Upheld	10
California Task Force: More Broadband Access	17
ID Theft/Phishing Bill Introduced in Kentucky	7
Suspect's Encrypted File Password Protected	11
Colorado House Passes Anti-Spam bill	9
FCC Begins Investigation of P2P Complaints	18
Delaware Enhanced Sex Offender Law Effective	8
Report: More Sophisticated Online Fraud Seen	18
Sex Offender Bill Introduced in New York	8

Table of Contents

Features

Why Attorneys Need to Understand E-Discovery	2
E-Discovery Training Nomination Form	21

AGs Fighting Cyber Crimes

50 AGs Announce Settlement With MySpace	
AG Goddard Speaks on Internet Safety	
Florida AG Settles With Internet Marketer	
AG Wasden Announces ICAC Task Force	
Illinois AG's Task Force Arrests Pornographer	
AG Conway Participates in Net Safety Forum	
Louisiana AG's Unit Arrests Net Predator	
AG Coakley Plans High Tech Forensic Lab	
Mississippi AG Say Pornographer Sentenced	
AG Nixon Sues Web Seller of Private Data	
New Mexico AG's Task Force Arrests Predator	
AG Cuomo Subpoenas Cable Provider	
New Jersey AG Speaks at Net Safety Training	
AG Edmondson Says Internet Fraud Top Crime	
Oregon AG Settles With Online Yellow Pages	
AG Corbett's Agents Arrest Online Predator	
South Carolina AG Says Predator Arrested	
AG Abbott's Unit Arrests Internet Predator	
Virginia AG Speaks About Net Safety Games	

Legislation Update

South Dakota Online Sales Tax Bill Endorsed	
Bill Banning State Net Sales Tax Introduced	
Florida Spyware Bill Pre-Filed	
Georgia House Passes Security Freeze Bill	
ID Theft/Phishing Bill Introduced in Kentucky	
Senate Committee Passes Data Security Bill	
Delaware Sex Offender Law Effective	
Florida Pornography Victims Bill Introduced	
New York Sex Offender Bill Introduced	
Bill Requiring ISPs to Report Porn Advances	
Internet Safety Grant Bill Advances	
Missouri Net Stalking Bill Passes Committees	
Colorado House Passes Anti-Spam Bill	
Computer Fraud Bill Introduced in House	
Computer Hunting Bill Introduced in Senate	
Copyright Infringement Bill Introduced	
Net Neutrality Bill Introduced in House	

In the Courts

Pointing Cell Phone Camera is Intimidation	
ISP Cannot Reveal Blogger Identity	
Net Pharmacist's Enhanced Sentence Upheld	
Suspect Not Required to Reveal Password	
Forum Selection Clause Controls in Dispute	
No Evidence of Spoliation in E-Mail	
E-Discovery Must Likely Lead to Evidence	

In the Supreme Courts

Maine Law to Stop Net Tobacco Preempted	
Patent Royalty Case Argued	
No Cert for Challenge to Copyright System	
Dispute Over Wireless Bills Denied Cert	

News You Can Use

Two Studies See Rise in Net Financial Crime	
Report: 47% of Adults Self-Google	
Teen Tech Use Increasing, Per Report	
Coupons Available for Switch to Digital TV	
Privacy Survey: U.S. Near Bottom	
Researchers: Wi-Fi Virus Attack Possible	
NLRB Says Employers Can Ban Union E-Mail	
ICANN Acts to Halt Domain Name "Tasting"	
California Task Force: More Broadband	
Study: Concerns About Net Privacy, Safety	
FCC Probes P2P Management Complaints	
Study Finds E-Bay Buyers Save Big	
Report: Online Fraud More Sophisticated	
Copyright Guidelines Set By 3 Universities	
Survey: Networking Sites Safer Than Others	

Tools You Can Use

NIJ Offers Paper on Crime Lab Backlogs	
Information Security Video Available	

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.

WHY ATTORNEYS NEED TO UNDERSTAND E-DISCOVERY³

By Hedda Litwin, NAAG Cybercrime Counsel

All you have to do is take a look at the sheer volume of information that is generated and stored electronically to understand why it is impossible for any attorney to avoid e-discovery issues. One widely cited study estimates that 93 percent of all documents are created in electronic form, and less than one-third of those ever make it to printed form.¹ In addition, we all know that electronic communication, whether it be e-mails or instant messaging, have taken the place of telephone conversations. One study has estimated that 31 billion e-mails are sent out each day.² The sheer volume of data is staggering, with one gigabyte of data being able to hold about 1,000 novels or being roughly equivalent to 18 hours of MP3 play. In addition to computers, there is a wealth of portable devices out there – all containing data and all discoverable.

The above does not, of course, include data that is not visible and was not intentionally created – the most useful of which is metadata. Metadata is not intentionally created by the user but is created or amended by the computer. It contains all sorts of useful information, such as the date and time the document was created and amended, the identity of the person creating it and the edits made to it. Metadata can be very helpful for uncovering the history of documents and whether the documents have been subject to tampering.

This proliferation of electronic information led to the recent amendments to the Federal Rules of Civil Procedure. The substance of the amendments has been adopted by, or is in the process of adoption by, several states, including Mississippi and New Jersey. The amendments address major areas regarding the retention and

discovery of electronic information, such as the need to address electronic discovery issues during the first meeting of the parties; discovery of both accessible information and information that is not easily accessible; the assertion of privilege; and the limit of sanctions for electronically stored information that is inadvertently lost during normal computer operations. Failure to preserve electronically stored information, failure to make disclosure and failure to cooperate in discovery can result in severe penalties, so if for no other reason, attorneys need to understand the amended rules to avoid sanctions.

The problem with getting up to speed on electronic discovery is that while there is no shortage of trainings and conferences on this issue, all of them target attorneys in private practice. Hence, NAAG is filling this gap by sponsoring “Best Practices in E-Discovery,” a conference developed under its NAGTRI training initiative and designed for civil,

enforcement attorneys and prosecutors from Attorneys General offices, which will be held May 13-15. If you are handling cases involving discovery, this course is for you.

For more information about the course, please contact Hedda Litwin, NAAG Cybercrime Attorney, at hlitwin@naag.org or (202) 326-6022.

¹Richard E. Best, “Why Discover Electronic Data?” at http://californiadiscovery.findlaw.com/electronic_data_discovery.htm.

²Stephen D. Willinger and Robin M. Wilson, “Negotiating the Minefields of Electronic Discovery,” 10 Rich. J.L. & Tech. 52, 28 (2004).

³Article reprinted from NAAG Gazette, Volume 2, Number 3, February 29, 2008.

AGs FIGHTING CYBER CRIMES

MULTI-STATE

Fifty Attorneys General announced the Joint Statement on Key Principles of Social Networking Safety, an agreement with MySpace.com in which the social networking site agreed to take steps to better protect children on its web site. The agreement culminates nearly two years of discussions between MySpace and the Attorneys General. Under the agreement, MySpace, with the support of the Attorneys General, will create and lead an Internet Safety Technical Task Force to explore and develop age and identification verification tools for social networking sites. Among the changes and

policies to which MySpace agreed were allowing parents to submit their children’s e-mail addresses to MySpace so the company can prevent anyone using those addresses from setting up profiles, making “private” the default setting for profiles of 16- and 17-year-olds, promising to respond within 72 hours to complaints of inappropriate conduct and committing more staff and resources to review and classify photographs and discussion groups. The complete Joint Statement is available on the NAAG web site, www.naag.org.

ARIZONA

Attorney General Terry Goddard was the keynote speaker at the 11th Annual Kids Concerned About Local Legislation program at the state Legislature. Attorney General Goddard spoke to more than 400 students in the fourth through sixth grades on Internet safety.

FLORIDA

Attorney General Bill McCollum's CyberFraud Task Force reached a \$1 million settlement with World Avenue, LLC, a Delaware company operating out of Florida which promotes Internet-marketed goods and services, most of them offering free gifts to consumers who sign up for the offers. The settlement resolves litigation filed by Attorney General McCollum's Economic Crimes Division alleging the company's offers of free merchandise upon completing certain program requirements were deceptive. The settlement specifies that companies must disclose all information necessary for consumers to make an informed choice. It also provides that World Avenue will pay \$1 million to enable Attorney General McCollum to continue establishing high standards of Internet marketing. The company has already provided reimbursements or appropriate restitution to affected consumers. A copy of the settlement can be accessed at [http://www.myfloridalegal.com/webfiles.ns/WF/MRAY-7AWJVZ/\\$file/NiuTechAVC.pdf](http://www.myfloridalegal.com/webfiles.ns/WF/MRAY-7AWJVZ/$file/NiuTechAVC.pdf).

IDAHO

Attorney General Lawrence Wasden, together with local, state and federal law enforcement agencies and prosecutors, announced the formation of the Idaho Internet Crimes Against Children (ICAC) Task Force. Attorney General Wasden's office received a \$250,000 grant from the Office of Justice Programs, U.S. Department of Justice, to fund the task force's first year of operation. The funds will be used to train and equip investigators and prosecutors for task force operations. A 14-member governing board of state law enforcement agencies and lead affiliate local

law enforcement agencies will oversee distribution and expenditure of funds. Steve Bywater, Deputy Attorney General and Chief of the Criminal Law Division, will chair the board and administer the grant.

ILLINOIS

Attorney General Lisa Madigan's Internet Crimes Against Children (ICAC) Task Force took Stephen McConaughay into custody on child pornography charges after a search of his residence revealed several computers and computer hard drives allegedly containing such images. After receiving a cyber tip from the National Center for Missing and Exploited Children, the task force executed a search warrant on McConaughay's home with the assistance of the Huntley and South Elgin Police Departments, the Department of Homeland Security's Immigration and Customs Enforcement, the Kane County Sheriff's Office and the McHenry County State's Attorney's Office.

KENTUCKY

Attorney General Jack Conway participated in an Internet safety forum held at a middle school in Louisville. The event was hosted by state representative John Yarmuth.

LOUISIANA

Attorney General James Caldwell's High Technology Crime Unit joined forces in an investigation with the Kenner Police Department and the St. Tammany Sheriff's Office which resulted in the arrest of Eugene Mathas Jr. at his residence. The 50-year-old Mathas allegedly contacted over the Internet what he believed to be a 14-year-old child, encouraging the "child" to engage in inappropriate acts and sending the "child" lewd videos of himself. The "child" was actually an undercover investigator.

MASSACHUSETTS

Attorney General Martha Coakley announced plans to launch a high tech forensics lab

that will specialize in cybercrime cases, as well as training law enforcement to handle electronic evidence. The facility will be led by David Papargiris, a veteran computer forensics investigator formerly with the Norwood Police Department. Christopher Kelly, who formerly directed the Computer Crime Division at the Suffolk County District Attorney's Office, was named as the managing attorney for Attorney General Coakley's Cybercrime Division. The lab will be funded by a \$142,000 Byrne Grant from the Executive Office of Public Safety and Security.

MISSISSIPPI

Attorney General Jim Hood announced that Timothy Patterson, who was prosecuted by Attorney General Hood's Cyber Crime Unit, was sentenced following a guilty plea to possession of ten images of child pornography. Patterson will serve five years in prison, after which he must register as a sex offender and will be on five years of supervised probation. His probation period will include limits on his Internet usage, as well as random checks by Attorney General Hood's Cyber Crime Unit. He will also pay court costs, a \$1,000 fine to the crime victims' compensation fund, \$500 to the Tallahatchie Circuit Clerk and \$500 in investigative fees to Attorney General Hood's office. The case was investigated, forensically analyzed and prosecuted by the Cyber Crime Unit based on a cyber tip from the National Center for Missing and Exploited Children.

MISSOURI

Attorney General Jay Nixon filed a lawsuit against www.PublicData.com for allegedly selling private information, such as social security numbers, that can be used by identity thieves. State residents who had a driver's license before 2005 could be affected, because after that year drivers were required to use an identification number other than their social security number. Attorney General Nixon is asking the court to order the company to disable its web site to prevent social security numbers from being obtained.

NEW MEXICO

Attorney General Gary King's Internet Crimes Against Children (ICAC) Task Force arrested Chris Girule, a/k/a Jonathon Duran, on one count each of Criminal Sexual Penetration, Forgery and Concealing Identity and eight counts of Sexual Exploitation of Children. Task force members initially used a search warrant citing probable cause that child pornography would be found at his residence, but Girule gave investigators a false ID. Consultation with the FBI revealed his true identity as well as the fact that he was wanted on probation warrants. A subsequent forensic examination of evidence gathered at Girule's residence resulted in the arrest.

NEW YORK

Attorney General Andrew Cuomo issued a subpoena to Comcast Corp., the nation's largest cable company, requesting information on its handling of Internet traffic. Comcast has been the subject of complaints, as well as a Federal Communications Commission hearing over its alleged throttling of file-sharing traffic on its cable modem service.

NEW JERSEY

Attorney General Anne Milgram spoke at a regional Internet safety training session held at the Bergen County Police Academy, part of an ongoing Internet safety training initiative for school teachers and administrators conducted by her office and the state Department of Education. The all-day session covered cyberbullying, the potential dangers of social networking and chat rooms, the behavioral traits of sexual predators and the methods they use to lure potential victims.

OKLAHOMA

Attorney General Drew Edmondson revealed his top 10 list of consumer crimes during the annual Consumer Protection Day at the state Capitol. Internet fraud, which includes online

auctions, deceptive service providers and bogus online retail sales, once again topped the list.

OREGON

Attorney General Hardy Myers entered into a settlement with Ad TelAmerica Inc., a Texas-based company, and its president, Barbara Sommer, under which the company agreed to stop its practice of offering state businesses “free” placement in an online Yellow Pages if they paid \$594 a year for print and CD listings. Several businesses had filed complaints with Attorney General Myers’ office after receiving bogus invoices and solicitations from the company. Ad TelAmerica will also make refunds to seven businesses.

PENNSYLVANIA

Attorney General Tom Corbett’s Child Predator Unit agents arrested Jeffrey Diltz, who is accused of using Internet chat rooms to sexually proposition what he thought was a 13-year-old girl, as well as sending nude and sexually explicit webcam videos to the “girl.” The “girl” was actually an undercover agent using an online profile. Diltz was arrested at his home by Unit agents with assistance from the Berwick Police Department. Agents also executed a search warrant at Diltz’s home, seizing five computers, a webcam and several data storage devices which will be analyzed by Attorney General Corbett’s Computer Forensics Unit as part of an ongoing investigation. Diltz is charged with two counts of unlawful contact with a minor and one count of criminal use of a computer, all of which are third degree felonies punishable by up to seven years in prison and a \$15,000 fine. The case will be prosecuted by Deputy Attorney General Michael Sprow of the Unit.

SOUTH CAROLINA

Attorney General Henry McMaster announced that Dennis Powell, Jr. was arrested in an undercover Internet sting conducted by the Lexington County Sheriff’s Department, a member

of Attorney General McMaster’s Internet Crimes Against Children (ICAC) Task Force. Powell was arrested on one count each of Criminal Solicitation of a Minor and Attempted Dissemination of Obscene Material, both felony offenses punishable by up to 10 years imprisonment, and one count of Attempted Criminal Sexual Conduct with a Minor, a felony offense punishable by up to 20 years imprisonment. Arrest warrants allege that Powell solicited sex on the Internet from what he believed to be a 12-year-old girl, but was actually an undercover sheriff’s deputy. He was arrested when he arrived to meet the “girl” for sex. A search warrant executed at Powell’s home resulted in the seizure of a computer, a digital camera, an image scanner and other computer-related items. The Richmond County Sheriff’s Department, also a task force member, assisted with the case, which will be prosecuted by Attorney General McMaster’s office.

TEXAS

Attorney General Greg Abbott’s Cyber Crimes Unit arrested Paul Kirksey, a police officer, for online solicitation of a minor. Kirksey was arrested after he e-mailed sexually explicit images to what he believed to be a 13-year-old girl, but was actually an undercover Unit investigator. The Unit also served an evidentiary search warrant on Kirksey’s residence.

VIRGINIA

Attorney General Bob McDonnell spoke at a state middle school about the success of three Internet safety video games provided free to area schools. He was joined by Mike Gallagher, CEO of the Entertainment Software Association, which funded the effort, and Judi Warren, President of Web Wise Kids, the organization distributing the software. The video games help students learn how to maintain a higher standard of personal safety and responsibility online. It will be available free to Virginia parents online.

LEGISLATION UPDATE

Online Sales Taxes

SOUTH DAKOTA. On February 13, the South Dakota Senate Taxation Committee endorsed H.B. 1017, a measure that makes into law the state's current practice of applying its sales and use tax to all products downloaded from the Internet. The bill was introduced at the request of the revenue department and will be forwarded to the full Senate.

INTRODUCED IN U.S. HOUSE. On February 7, Representative Rick Boucher (D-VA) reintroduced H.R. 5267, a bill that would expand the federal prohibition against state taxation of interstate commerce to include taxation of out-of-state transactions involving all forms of property (currently only tangible personal property is covered) and prohibit state taxation of an out-of-state entity unless that entity has a physical presence in the state. It has been referred to the House Judiciary Committee.

Spyware

FLORIDA. On February 7, state Senator Jeremy Ring of Florida pre-filed S.B. 1658, a bill that would make persons who introduce spyware or other "contaminants" onto a computer without consent subject to criminal prosecution. A similar bill is supposed to be filed in the state House. The legislative session is scheduled for March 4 through May 2.

Identity Theft/Phishing/Data Breaches

GEORGIA. The state House passed H.B. 130, 167-2, a bill which would allow consumers to block outside access to their credit histories temporarily or permanently. It would cost them \$3 to place or remove a "security

freeze" on an individual credit account. The bill has now been referred to the state Senate.

KENTUCKY. With the support and input of Kentucky Attorney General Jack Conway, H.R. 553 was introduced on February 15 to combat identity theft and phishing. The bill would require businesses to notify consumers if their personal information has been compromised by improper record disposal or online security breach. Businesses must take reasonable steps to protect the data, and if information is compromised, they could be civilly liable for losses incurred by consumers. The bill would also require businesses to keep social security numbers hidden in mailings, remove identification numbers on benefit cards and require security measures for web sites requiring customers to enter their social security numbers. It would criminalize "phishing," where e-mails or web sites mimic legitimate businesses to scam consumers, and will allow victims, the Attorney General, Internet service providers and owners of web sites or trademarks to sue the perpetrators for damages. In addition, the bill would benefit victims of identity theft by expediting the process for obtaining a court order to be used to dispute fraudulent charges.

PASSED U.S. SENATE COMMITTEE. The Senate Commerce, Science and Transportation Committee passed S. 1178, a bill sponsored by Senator Daniel Inouye (D-HI) that would require any commercial business or non-profit that acquires or maintains personal information to develop, implement and enforce a written plan for the data's security. It would also require them to notify the Federal Trade Commission of any breach involving 1,000 or more individuals or one that has a likely risk of identity theft. It also prohibits such entities from soliciting a social security number from an individual unless

there is a specific use it provides unmatched any other identifier. The bill would also authorize a consumer to place a security freeze on his or her credit report. The bill allows enforcement by state attorneys general but preempts state laws requiring notification of data breaches and those related to the use of social security numbers.

Internet Crimes Against Children

DELAWARE. Delaware's enhanced sex offender registration law took effect on January 1. Offenders are now required to register with the state Bureau of Identification. Low risk offenders must then report in person to police once a year; moderate risk offenders must report every six months; and high risk offenders must report quarterly. Offenders will now have three days to register after being freed, as opposed to seven days previously.

FLORIDA. On January 29, S.B. 1442, a bill supported by Attorney General Bill McCollum that would make Florida the first state to allow victims of child pornography to seek civil remedies against those who download and distribute images of the victim's abuse, was introduced in the state Senate. The bill will also allow the Attorney General's Office to pursue these cases on behalf of the victims at their request. The legislation would also create an electronic notification system that would allow the victims to maintain their privacy while still being heard and considered in criminal court cases. A companion bill, H.B. 605, was introduced in the state House. A summary of the bill can be accessed at: [http://mufloridalegal.com/webfiles.nsf/WF/MRAY-7BYKJ7/\\$file/ExploitedChildren'sRightsAct.pdf](http://mufloridalegal.com/webfiles.nsf/WF/MRAY-7BYKJ7/$file/ExploitedChildren'sRightsAct.pdf)

NEW YORK. On January 29, A 9859, a bill supported by Attorney General Andrew Cuomo that would bar from social networking sites all Level 3 sex offenders (the most dangerous) and sex offenders who used the Internet to commit sex crimes or crimes against minors, was introduced. Under the bill, all

registered sex offenders would be required to submit their e-mail addresses and other Internet identifiers to the state Division of Criminal Justice Services within 10 days of their creation, with failing to do so considered a violation of their probation or parole. The bill would authorize the state to share those addresses with social networking sites. The companion state senate bill is S 6875.

PASSED U.S. SENATE COMMITTEE. The Senate Committee on Commerce, Science and Transportation favorably reported S. 1965, a bill sponsored by Senator Ted Stevens (R-AK) that would impose a forfeiture penalty and increase civil fines on Internet service providers (ISPs) for failure to report child pornography as required under the Victims of Child Abuse Act. It would also authorize the Center for Missing and Exploited Children to provide images of child pornography to ISPs to assist in stopping further transmission. The bill would also require elementary and secondary schools with computer access to the Internet to educate minors about appropriate online behavior.

PASSED U.S. SENATE COMMITTEE. The Senate Judiciary Committee favorably reported S. 2344, a bill sponsored by Senator Robert Menendez (D-NJ) that would create a grant program to provide age-appropriate Internet education for children.

Internet Stalking and Harassment

MISSOURI. The state Senate Judiciary and Civil and Criminal Jurisprudence Committees passed S.B. 818, a bill that incorporates recommendations made by Governor Matt Blunt's Internet Harassment Task Force. The bill expands the definitions of both stalking and Internet harassment and also enhances the penalties. Currently, harassment is a class A misdemeanor, but under the bill it would become a class D felony if 1) it is committed by an adult against a person 17 years

of age or younger; 2) it is committed with the purpose of frightening, intimidating or causing emotional disturbance; 3) or the perpetrator has previously committed the crime. Currently, stalking is a class A misdemeanor for the first offense and a class D felony for the second offense if committed within five years. The bill takes away the requirement that the second offense be committed within five years. The bill also requires public schools to have a written policy about reporting of harassment.

Spam

COLORADO. On February 12, the Colorado House passed H.B. 1178, a bill that would establish civil sanctions and criminal penalties for parties who violate the federal CAN-SPAM Act or send other kinds of unsolicited commercial e-mail messages. The bill would consider the violation of the Act a deceptive trade practice and would create a new misdemeanor e-mail fraud offense. The bill has been sent to the state Senate.

Computer Fraud

INTRODUCED IN U.S. HOUSE. Representative John Conyers, Jr. (D-MI) introduced H.R. 4175, a bill that would include computer fraud within the definition of racketeering activity and expand penalties for conspiracies to commit computer fraud, as well as extortion attempts involving threats to access computers without authorization. It would provide for restitution, including forfeiture of property, for victims of such fraud and identity theft. The bill would authorize the Attorney General and state attorneys general to bring civil actions and seek injunctive relief for violations of federal data security laws. The bill has been referred to the Judiciary Committee's Subcommittee on Crime, Terrorism and Homeland Security.

Computer-Assisted Remote Hunting

INTRODUCED IN U.S. SENATE. Senator Sheldon Whitehouse (D-RI) introduced S. 2422, a bill that would prohibit and establish penalties for anyone who makes available a computer or software that would enable computer-assisted remote hunting. The bill has been referred to the Senate Judiciary Committee.

Intellectual Property

INTRODUCED IN U.S. HOUSE. Representative John Conyers (D-MI) introduced H.R. 4279, a bill that would enhance penalties for infringement of a copyright, for trafficking in counterfeit labels or packaging and for causing serious injury or death while trafficking in counterfeit goods. The bill would also enhance civil and criminal forfeiture provisions for copyright infringement and provide restitution to those injured. It would also direct the Office of Justice Programs to provide grants to state and local law enforcement agencies to combat intellectual property theft and infringement crimes. The bill has been referred to the House Judiciary Committee's Subcommittee on Courts, the Internet and Intellectual Property.

Net Neutrality

INTRODUCED IN U.S. HOUSE. On February 12, Representative Edward Markey (D-MA) introduced H.R. 5353, a bill promoting the principle of net neutrality that would require the Federal Communications Commission to assess whether broadband providers are blocking or interfering with consumers' rights to access, send or receive content, applications and services over networks. It has been referred to the House Committee on Energy and Commerce.

IN THE COURTS

WITNESS INTIMIDATION: CELL PHONE CAMERA

Commonwealth v. Casiano, No. 06-1503 (Mass.). The Massachusetts Appeals Court upheld a lower court verdict by ruling that pointing a cell phone camera at a witness in a criminal case is witness intimidation. While in a courthouse awaiting trial, defendant David Casiano acted as if he were taking cell phone photos of an undercover police officer who was scheduled to testify against him. While Casiano later claimed that his cell phone wasn't operational in the courtroom, the court denied his request to introduce records from his cell phone provider as proof. The undercover officer testified that having his picture on the Internet could jeopardize his investigations as well as the safety of his family. Casiano was found guilty of intimidating of intimidating a witness.

DEFAMATION: ANONYMOUS BLOG

In re Does 1-10, 2007 WL 4328204 (Tex. Ct. App. December 12, 2007). A Texas court of appeal ordered a trial court to vacate its order compelling a blogger's Internet service provider (ISP) to reveal the blogger's name and address. The case revolves about a blogger page called "The Paris Site," operated by an anonymous blogger using a pseudonym, on which critical remarks about the Essent hospital in Paris, Texas were posted. Essent sued the 10 John Does (the blogger operator and the others who posted comments), alleging defamation and trade disparagement. Essent then filed an ex parte request for an order compelling the blogger's ISP to

disclose his identity. The court did so, and the ISP then sent notice to the blogger pursuant to the Cable Communications Act, which requires that the ISP notify the subscriber before disclosing personal information. The blogger appealed, and the appellate court found in his favor, acknowledging that the right to speak anonymously online is protected by the First Amendment, and that mere allegations of wrongdoing are insufficient to overcome that right.

INTERNET PHARMACIES: ENHANCED SENTENCES

U.S. v. Hanny, 2007 WL 4322265 (8th Cir. December 12, 2007). The 8th Circuit Court of Appeals upheld the sentence of Dr. Thomas Hanny for conspiring to distribute controlled substances over the Internet. Hanny, a retired surgeon, went to work for two Internet pharmacies, writing Internet-mediated prescriptions. One of the pharmacies was subsequently shut down by law enforcement, and a cease-and-desist letter was issued to Hanny, which he ignored at his own peril. Hanny was convicted, and the court applied U.S.S.G. §201.1(b)(5), which requires the court to apply a two-level sentence enhancement for "the distribution of any controlled substance through mass marketing by means of an interactive computer service." Hanny appealed the enhancement, arguing that the government had not introduced any evidence that the Internet pharmacies used spam or other mass advertising methods. The government contended that the mere existence of an e-commerce web site constituted mass marketing, and the 8th Circuit agreed,

stating that “a public, interactive web site reachable by an ordinary web search engine is, at the least, a billboard on the information superhighway.”

5TH AMENDMENT: ENCRYPTED FILES

In re Boucher, 2007 WL 4246473 (D. Vt. November 29, 2007). The U.S. District Court for the District of Vermont ruled that a child pornography suspect cannot be forced to reveal the password to the encrypted files on his computer because to do so would violate his Fifth Amendment right against self-incrimination. Sebastien Boucher’s car was inspected as he crossed the border from Canada. With Boucher’s consent, a border agent viewed the contents of his laptop and found suspected child pornography. Boucher was arrested, but when government forensic experts examined the laptop, they found that they could not get into the drive they wanted because it was encrypted. A federal grand jury issued a subpoena requiring Boucher to provide the password to the encrypted drive, but Boucher moved to quash the subpoena, asserting his Fifth Amendment right against self-incrimination. The government argued that Boucher could just type the password in without revealing it. The court rejected this argument, finding that such an action would be tantamount to unconstitutionally compelled testimony against his own interest, and it quashed the subpoena.

INTERNET CONTRACTS: FORUM SELECTION CLAUSE

Krause v. Chippas, 2007 WL 4563471 (N.D. Tex. December 28, 2007). The United States District Court for the

Northern District of Texas transferred the case based upon a forum selection clause found in the online Service and Usage Agreement. Donald Krause sued William Chippa, d/b/a Futurescom.com, a day trading site that he joined which required users to accept its terms prior to entering the site. The agreement states that any controversy shall be arbitrated, litigated or otherwise resolved in Palm Beach County, Florida, and that use of the web site or its services “signifies” the user’s consent to the terms of the agreement. Krause claimed he never consented to the agreement, but evidence showed that the agreement was clearly stated when he made payment for services. The district court held that a forum selection clause such as the one in the instant case is enforceable, and Krause could be charged with constructive knowledge of its terms where the forum selection clause was included on the web site when Krause accessed it. The forum selection clause controlled, absent a strong showing that its enforcement would be unreasonable or unjust or was invalid due to fraud or overreaching.

E-DISCOVERY: SPOLIATION

Bakhtiari v. Lutz, 2007 WL 3377215 (8th Cir. November 15, 2007). The 8th Circuit Court of Appeals held that a lower court did not abuse its discretion in finding no evidence of spoliation of e-mail messages. Alireza Bakhtiari filed suit against the University of Missouri, alleging civil rights and Title VII violations resulting in his termination as a teaching assistant. After Bakhtiari was terminated, but prior to his suit, the university’s IT staff had backed up the contents of his e-mail account onto two CDs, then deleted the e-mail messages from the server as part of routine maintenance. In response to an e-

discovery request, the university turned over the two CDs to Bakhtiari, but he claimed that large amounts of e-mails were missing. Bakhtiari moved for sanctions for spoliation against the university for deleting the e-mail from the server, but the court denied the motion. On appeal, the appellate court affirmed, finding that the university staff had taken appropriate steps to back up the data and that Bakhtairi may himself have caused the missing data. Following its own holding in *Greyhound Lines, Inc. v. Wade*, 485 F.3d 1032, 1035 (8th Cir. 2007), the court reiterated that a party is guilty of spoliation if the court finds that it “intentionally destroyed evidence with a desire to suppress the truth,” and in the instant case there was no evidence that the university so acted.

E-DISCOVERY: CELL PHONE IMAGES

Smith v. Café Nora, 2007 U.S. Dist. LEXIS 73071 (D.D.C. October 2, 2007). The D.C. District Court held that Fed. E. Civ. P. 26 is not an “all or nothing”

proposition, and the probative value of sought-after materials must outweigh their prejudice. Andrei Smith, a former host and waiter at Café Nora, a D.C. restaurant, filed suit against the restaurant alleging sexual harassment. The complaint also included an allegation that a restaurant manager sent him an e-mail on his cell phone containing pornographic images. Café Nora sought the production of the images stored on Smith’s cell phone, arguing that those images were reasonably likely to result in the discovery of admissible evidence. Smith opposed the discovery, and while admitting that the images existed, claimed they were prejudicial and therefore inadmissible. The district court noted that while parties are afforded broad leeway in discovery, they do not have carte blanche and the discovery request must reasonably be calculated to yield admissible evidence. The court ordered Smith to preserve the images, but ordered inspection of the images only by a designated attorney.

IN THE SUPREME COURT

Decided

In *Rowe v. New Hampshire Motor Transport Association*, No. 06-457, the Court unanimously held that the Federal Aviation Administration Act of 1994 preempts two provisions of a Maine law intended to prevent Internet sales of tobacco to minors. The first provision requires a seller of tobacco products to use a delivery service that obtains age verification and the signature

of the addressee; the second provision deems a carrier to know that the package contains tobacco and is being sent by an unlicensed retailer if the exterior of the package contains tobacco markings and the retailer is not on the state list of licensed retailers. Maine had argued that federal law does not preempt state regulation for public health and safety, but the Court said that despite the importance of the public health objective, the Maine law would require companies to use delivery services “that differ significantly” from the average marketplace and at much higher cost.

The Court concluded that both Maine provisions are “related to a ... service of any motor carrier,” 49 U.S.C. § 1450© (1), because they “substitute” the state’s “own government commands for ‘competitive market forces’ in determining ... the services that motor carriers can provide.”

Argued

On January 16, the Court heard oral argument in *Quanta Computer, Inc. v. LG Electronics*, No. 06-937, a case that addresses the controversial issue of whether the holder of a patent can seek royalties from downstream purchasers following the sale of the patent to an initial purchaser. LG Electronics owned a group of patents, including microprocessor chips used in personal computers. It licensed the patents to Intel, but in a separate agreement excluded from the license any Intel customer that combined a licensed Intel microprocessor chip with non-Intel components. Intel advised all of its customers by letter of this exclusion.

Quanta, one of the petitioners, purchased the microprocessor chips from Intel and used them to make computers for Dell, Hewlett-Packard and Gateway. LG Electronics sued Quanta and other customers for violating the ‘condition’ of Intel’s license by not paying patent royalties to LG. Quanta argued that the license they purchased was not restricted and therefore royalties were not due. They further argued that the only reasonable use for the chips was to be integrated into devices such as computers, so it was against existing case law to claim patent infringement against downstream purchasers who used Intel’s product for its sole use.

The trial court ruled for Quanta and held that Intel’s license exhausted LG’s downstream patent royalty rights. The court said that after one link in the chain has paid a royalty for a patent, no other link should have to pay a royalty. The U.S. Court of Appeals for the Federal Circuit reversed, finding that in the instant case the sale to Intel was expressly conditional.

A ruling in the case is expected by July.

Cert Denied

On January 7, the Court declined to grant certiorari in *Kahle v. Ashcroft*, 487 F.3d 697 (9th Cir. 2007), a First Amendment case that challenges changes in the U.S. copyright system from an opt-in to an opt-out system. The Internet Archive and the Open Content Alliance and their respective founders, Brewster Kahle and Rick Prelinger, sued the U.S. government for changing the copyright system. Previously, copyright holders had to renew their copyrights after their terms expired in order to preserve their exclusive right to reproduce their work. The Copyright Renewal Act of 1992 removed the renewal requirement, so copyright holders would have to explicitly remove the copyright if they no longer wanted it. Prompted by *Eldred v. Ashcroft*, 537 U.S. 186 (2003), which challenged the constitutionality of the Sonny Bono Copyright Term Extension Act, the plaintiffs argued that such a drastic change in copyright law required a review of its effect on freedom of speech. The Ninth Circuit Court of Appeals rejected their argument.

On January 22, the Court also declined to review *Sprint Nextel Corp. v. Nat’l Ass’n of State Utility Consumer*

Advocates, No. 06-1184, therefore letting stand a ruling that precluded wireless communications providers from listing taxes and other government fees as separate line items on consumers' bills. The wireless providers wanted the Court to overturn the ruling, arguing that state and local governments were trying to "hide" taxes and fees by preventing providers from listing them separately.

The advocate group, which supported the ruling, countered by arguing that wireless providers often add a perplexing assortment of charges, separate from state and local taxes, to consumers' bills. The case centers on the Federal Communications Commission's 2005 ruling that federal law prevents states from barring separate line items.

NEWS YOU CAN USE

TWO STUDIES FIND RISE IN INTERNET FINANCIAL CRIMES

Two newly published studies report acceleration in Internet financial crimes. First, the Ponemon Institute study, funded by security companies PGP and Vontu, found that the average cost for a business victimized by a data breach rose 30 percent this year to \$6.3 million. It also reported that businesses hit by data breaches lost \$197 per compromised record in 2007, compared with \$182 in 2006. Thirty percent of that increase came from sales that the companies would have expected if technical problems and damage to their brand names had not occurred. The survey also found double the amount of breaches by third party organizations, such as contractors, outsourcers and consultants, over those breaches occurring two years ago. The full study can be accessed at http://www.pgp.com/downloads/research_reports/ponemon_reg_direct.html. The Federal Trade Commission (FTC) report, which was based on telephone interviews with almost 5,000 people, estimated that more than eight million Americans were victims of identity

theft in 2005. Of the victims, more than one in three reported that they experienced further problems due to the theft even after they recovered their money and identity, including being denied new credit and loans, having their utilities cut off or being subject to a criminal investigation. Five percent of victims said that when an identity thief was charged with a crime, the thief gave the victim's name or personal information to police. The full FTC report can be accessed at <http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>.

PEW REPORT #1: MORE AMERICANS ARE SELF-GOGLING

An increasing number of adult Internet users in the U.S. are Googling themselves, as well as their friends, co-workers and romantic interests, according to a study by the Pew Internet and American Life Project. The report found that 47 percent are looking for this information through a search engine, up from 22 percent in 2002. Americans under 50 years of age and those with more education were more likely to self-Google, according to the study. Although men and women equally searched for online information about themselves, women were slightly more likely to look up information about someone they

were dating. While most searches were innocuous, the study found that one-third looked up public records, such as bankruptcies and divorce proceedings. Another one-third searched for someone else's photograph. Three-quarters of self-searchers say they have only done so once or twice, but do consider what they find accurate. Only four percent found embarrassing or inaccurate online information. The study data was based on a telephone survey of 1,623 Internet users. The entire report can be accessed at http://www.pewinternet.org/pdfs/PIP_Digital_Footprints.pdf.

PEW REPORT #2: TEEN HIGH TECH USE ON THE RISE

The Pew Internet and American Life Project's "Teens and Social Media" study found an increase in the number of teens conducting their social lives with the use of technology, especially the Internet. Among the more striking trends was that 63 percent of teens have a cell phone, with 55 percent reporting that they use the phone daily to talk with friends. The study also found that 35 percent of online teen girls blog, compared with 20 percent of online teen boys. The growth in blogs tracks, but does not overlap, teen use of social networking sites, with 41 percent of teens who use MySpace, Facebook or similar sites reporting they send messages to friends via these sites daily and 55 percent reporting that they have a profile on these sites. Of those teens with profiles, 42 percent say they also blog, while 70 percent say they read others' blogs and 76 percent post comments to a friend's blog. While blogs are more prevalent with girls, the study found that YouTube and video sharing sites tend to be boys' domains. Online teen boys are more likely than girls to post video files by a 19 percent to 10 percent margin. The complete report can be accessed at

http://www.pewinternet.org/PPF/r/230/report_display.asp.

COUPONS AVAILABLE TO AID SWITCH TO DIGITAL TV

The National Telecommunications and Information Administration began accepting requests for two \$40 coupons per household to be used toward the purchase of television converter boxes. Beginning in February 2009, anyone who does not own a digital set and gets their programming via over-the-air antennas will no longer receive a picture unless they buy a box for each set, which is expected to cost between \$50 and \$70 and will be available at most electronics retail stores. Viewers who have satellite or cable service will not need a box. The Neilson Company estimates that 14.3 million households, or about 13 percent of the 112.8 million television households in the U.S., rely on over-the-air broadcasts for television programming. Congress has set aside \$1.5 billion for the coupon program, which basically works on the honor system. To request a coupon, consumers can apply online at <http://www.dtv2009.gov>. There is also a 24-hour hotline to take requests, 1-(888) DTV-2009 (1-(888) 388-2009).

PRIVACY SURVEY FINDS U.S. LOSING GROUND

Greece, Romania and Canada had the best privacy records of 47 countries surveyed by Privacy International, a London-based watchdog group. Australia was ranked 19th, higher than Slovakia but lower than South Africa and New Zealand. The report noted that although privacy was improving in the former communist states of eastern Europe, it was declining in Western Europe, most likely due to concerns about terrorism, immigration and border security. Malaysia, Russia and China ranked worst, but Great Britain and the

United States also were ranked in the lowest performing group of “endemic surveillance societies.” The survey considered factors such as legal protections, enforcement, data sharing, the use of biometrics and prevalence of closed circuit cameras. The full report may be accessed at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-559458](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559458).

GLOOMY RESEARCH: WI-FI VIRUS ATTACK POSSIBLE

If criminals were to target unsecured wireless routers, they could create an attack that could take over thousands of Wi-Fi networks in urban areas such as Chicago or New York City, according to a research paper by Steven Myers, an assistant professor at Indiana University, and researchers from the Institute for Scientific Interchange in Torino, Italy. The researchers theorized that the attack would work by guessing administrative passwords and then instructing the routers to install new worm-like firmware, which would in turn cause the infected router to attack other devices in its range. The research team used what is known as the Susceptible Infected Removed (SIR) model to track the growth of this attack, a methodology typically used to estimate such things as influenza outbreaks and computer virus infections. Although the team did not develop an attack code that could be used to carry out the infection, they believe it would be possible to write code that guessed default passwords by first entering the default administrative passwords that shipped with the router, and then trying a list of one million commonly used passwords. The researchers believe that 36 percent of passwords can be guessed using this technique. They also believe that even some routers that use encryption can be cracked if they use the popular Wired Equivalent Privacy (WEP) algorithm. The researchers’ model is based on data compiled

from the Wireless Geographic Logging Engine (WIGLE), a volunteer-run effort to map Wi-Fi networks around the world. Using this data, they were able to map out large networks made out of Wi-Fi routers that were each no more than 45 meters (49 yards) from the network, with the largest such network in New York, consisting of 36,807 systems.

NLRB LIMITS UNION USE OF E-MAIL

In a 3-2 ruling, the National Labor Relations Board (NLRB) held that it was legal for employers to prohibit union-related e-mail if employers had a policy barring employees from sending e-mail for “non-job-related solicitations” for outside organizations. The ruling is a setback for labor unions, which argued that e-mail systems have become a gathering place where employees should be able to communicate freely with co-workers to discuss matters of mutual concern. The ruling entailed *The Register-Guard*, an Oregon newspaper, and three e-mail messages sent by Suzi Prozanski, a newspaper employee who was also president of the Newspaper Guild’s unit. Her e-mails urged employees to march in a town parade and wear green to show support for the union in contract negotiations. The ruling comes as labor unions continue to struggle to reverse their membership declines, now representing only 12 percent of the nation’s workforce, down from 35 percent in the 1950s. The full decision can be accessed on the Board’s web site, <http://www.nlr.gov>.

ICANN MOVES TO STOP DOMAIN NAME “TASTING”

Board members of the Internet Corporation for Assigned Names and Numbers (ICANN) voted unanimously for a policy change that would make the web site registration process more expensive for domain “tasters,” who are entrepreneurs taking advantage of a five-day grace period to

sample domain names, keeping the few that might generate advertising, at a cost of about \$6.25 per domain, and dropping the rest before paying. The grace period was originally designed to rectify legitimate mistakes, such as registrants mistyping the domain name they were about to buy. The “tasting” practice ties up millions of domain names at any given time. Currently, in addition to the domain cost, a 20-cent surcharge per domain goes to ICANN, but ICANN has always refunded that fee if the registrar failed to purchase the domain within the five days. The new policy will not refund the fee, so it will now cost a “taster” who typically buys 100,000 domains, but only keeps one, \$20,000. ICANN has not yet announced when the new policy will take effect.

CALIFORNIA TASK FORCE URGES WIDER BROADBAND ACCESS

The California Broadband Task Force issued a report warning that slow Internet speeds and scattered adoption of broadband across the state would inhibit the state’s ability to compete in the global economy. The task force found that only one-half of state citizens had high-speed Internet access at home, despite its wide availability in the state. Broadband speeds varied widely, with 99 percent of residents in Los Angeles and Orange County able to subscribe to broadband at rates of 10 megabytes per second or higher, compared to only six percent of Bay Area residents. According to the task force’s research, 1.4 million Californians have no access to broadband service, and less than 60 percent of the northern Sierra has broadband. The task force issued seven recommendations, including expanding the broadband infrastructure to all citizens and removing obstacles to private sector investment. It also recommended streamlining the permitting process, as well as establishing a public-

private partnership to ensure that every household with a child has a computer and high speed access. Formed last year by Governor Arnold Schwarzenegger, the 21-member task force included representatives from local governments, telecommunications firms, state universities and nonprofit groups. The final report may be accessed at <http://www.calink.ca.gov/taskforcereport/>.

INTERNET STUDY: MORE CONCERN ABOUT PRIVACY, ONLINE KIDS

In 2007, 61 percent of adult Americans said they were very concerned about the privacy of personal information when shopping online, an increase from 47 percent in 2006, according to an annual study by the University of California’s Center for the Digital Future. As of 2007, two-thirds of adult Internet users shop online, compared with half that number in 2006. The majority spend \$100 or less a month, but two-thirds of online shoppers have reduced their buying. Among other findings, 62 percent of parents are more likely to withhold Internet use as punishment, compared with 47 percent in 2006 and 32 percent in 2000. For the first time, denying Internet use is equal as a punishment to banning television. Almost two-thirds of parents worry about kids participating in online communities, and one-half believe online predators to be a threat. The survey also found that newer users were more likely to access the Internet through a dial-up connection, as well as spending more time than veterans in playing online games, with an average of 1.2 hours per week. Another finding was that 21 percent of Internet users have stopped a newspaper or magazine subscription because they could get access online, while one-half of Americans who read a print edition of a newspaper said they would miss it if they cancelled. The study was based on 2,021 randomly selected Americans who were contacted by telephone.

FCC INVESTIGATES P2P MANAGEMENT COMPLAINTS

The Federal Communications Commission (FCC) posted requests for public comment about two petitions, both dealing with the question of how Internet service providers manage peer-to-peer (P2P) file-sharing traffic on their networks. One petition was filed by consumer advocacy groups that support net neutrality regulations, including Free Press, Public Knowledge, Media Access Project and Consumers Union, which responded to reports that Comcast was throttling P2P traffic by asking the FCC to declare that “degrading” P2P traffic violates the FCC’s Internet policy statement. That statement says that consumers can generally use the applications and access the web sites of their choosing, with an exception for “reasonable network management.” The other petition was from Vuze, a file-sharing application specializing in videos, which asked the FCC to “clarify” what it means by “reasonable network management.” The FCC is also seeking feedback on a third petition, filed by the same consumer groups as filed the first petition, asking the FCC to declare that text-messaging services are subject to federal telecommunications law that bars telecommunications companies from, engaging in “unjust or unreasonable discrimination” related to charges, services and other practices. That request stems from a situation in which Verizon Wireless initially refused to carry text messages from a reproductive rights group.

STUDY: EBAY BUYERS SAVE BIG BUCKS

E-Bay buyers saved \$7 billion that they might otherwise have been ready to spend, according to a study of eBay auction behavior in 2003 by Wolfgang Jank and Galit Schmueli, two associate professors of

decision and information technologies at the University of Maryland’s Robert H. Smith School of Business. They collaborated on the research with Ravi Bapna, an associate professor at the school who generated data for the study. Applying a linear projection to the findings would mean that buyers saved \$8.4 billion in 2004 and about \$19 billion in 2007. The study sought to calculate “consumer surplus” – the difference between the top price buyers were ready to pay and what they actually paid. The research examined consumer purchase data from more than 4,500 U.S. and European auctions. The data was drawn from a web venture by Bapna called Chiper.com, which allows consumers to bid automatically in the closing minutes of auctions. The data is then adjusted to account for eBay bidders who place bids manually rather than by automated bids. The study will be published in a paper titled “Consumer Surplus in Online Auctions” in the Journal of Information Systems Research.

ONLINE FRAUD MORE SOPHISTICATED IN 2007

A year-end report by the Washington Post describes the different types of online fraud seen in 2007. Hackers attempted to get users to go to particular sites that would install spyware on their computers, particularly before the Superbowl and on “Cyber Monday” after Thanksgiving, when there is a surge in online shopping. The report also noted a 100 percent increase in spam e-mails, which can be partially attributed to the “Storm worm,” an e-mailed Trojan horse program that infected computers after users went to footage of storms on the European coast. The number of spam e-mails rose to 120 billion messages daily, or about 20 spam e-mails per day for every person in the world. Another development was the use of phishing attacks to trick users into entering their personal bank account data at fake e-commerce and banking sites. Other attacks involved e-mails

appearing to come from the Better Business Bureau asking users to view a complaint, but when the user opened the “complaint,” spyware was installed on the computer. The full report may be accessed at

<http://www.washingtonpost.com/wp-dyn/content/article/2007/12/20/AR2007122001266.html>.

PUBLISHERS, UNIVERSITIES AGREE ON COPYRIGHT GUIDELINES

The Association for American Publishers (AAP) announced an agreement with Hofstra, Syracuse and Marquette Universities on copyright guidelines for educational materials in digital format. The guidelines affirm that these materials should be treated under the same copyright principles as those in printed format. The negotiations about the guidelines began after teachers began posting copyrighted materials online for multiple students without getting permission from the publishers. The AAP hopes that the guidelines will serve as a model for other universities. Each of the three universities tailored these guidelines to meet their own needs. The guidelines for Hofstra can be accessed at

http://www.hofstra.edu/pdf/about/Policy/policy_ereserves.pdf; for Syracuse, at <http://sunews.syr.edu/copyright.cfm>; and for Marquette, at

http://www.marquette.edu/library/reserve/ereserve_copyright_Guide-lines.pdf

SOCIAL NETWORKING SITES: SAFER THAN ALTERNATIVES?

Social networking sites such as MySpace and Facebook may be safer places for children to chat than other types of sites, according to a survey conducted by Internet Solutions for Kids, a California-based non-profit organization, and the University of New Hampshire. The survey, which involved 1,588 children between ages 10 to 15, found that 28 percent had been harassed through a social networking site, compared to 33 percent on other Internet sites. In addition, 55 percent of online harassment was conducted via instant messaging. The survey also found that one in seven children reported an unwanted sexual solicitation online in the past year, as compared to only four percent reporting a solicitation via a social networking site. A surprising finding was that most of the children who received a sexual solicitation were aware that it came from an adult. In 95 percent of cases referred to law enforcement, adult offenders were honest about being an adult, and 79 percent were honest about their intentions. The study’s authors suggest that targeting social networking sites may not be the best method of combating cyberbullying and sexual solicitation, but say programs should focus on mental health interventions for vulnerable children and Internet safety education that applies to all types of online communication. The survey appeared in the Paediatrics journal. It can be accessed at <http://pediatrics.aappublications.org/cgi/reprint/121/2/e350>.

TOOLS YOU CAN USE

Managing Backlogged Crime Laboratory Cases

“Increasing Efficiency in Crime Laboratories,” a National Institute of Justice (NIJ) publication, describes how laboratories across the country have successfully used managerial advances, such as process mapping, efficiency forums and business process management, to reduce backlogs. It can be accessed at <http://www.ncjrs.gov/pdffiles1/nij/220336.pdf>.

Securing Government in a Digital World

A new video, “At Risk! Securing Government in a Digital World,” has been released by the National Association of State Chief Information Officers (NASCIO). It is intended to raise awareness of the need for continuous and sufficient levels of resources dedicated to information technology security. It can be viewed in streaming format, or a copy can be ordered at no cost, on their web site, www.nascio.org.

**National Attorney General Training and Research Institute
NAGTRI**

BEST PRACTICES IN E-DISCOVERY TRAINING

May 13-15, 2008
University, MS 38677

NOMINATION FORM - RETURN BY APRIL 18, 2008

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

MEETING ID NO. # 0805_EDIS

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

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

Name (as it should appear on badge): _____	Full Mailing Address: _____
Title: _____	_____
Phone Number: _____	_____
Fax Number: _____	_____
E-mail: _____	_____
Attorney General Office: _____	

Travel By (Check one): Air Rail Car

State Bar registration number(s)
(For CLE credit)

State _____ Number _____

State _____ Number _____

Dietary Restrictions? If so describe: _____

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

(NAAG Use Only):

This Nominee Has Been Approved To Attend This Training: Yes (____) No (____)