

News Highlights in This Issue:

“Cybercrime and Juveniles” Conference Set	18
26 AGs Settle With Online Directory	3
Suit for Posting Personal Data Online Fails	8
South Dakota Outlaws Text Message Threats	10
Survey Finds Lack of Security by Mobile Users	12
Guide on Sting Operations Available	18
Virginia Spam Statute Upheld	8
Roger Servers Used by Hackers on the Rise	13
Iowa Enacts Tax Breaks for Web Portals	10
Cyberbullying Resources Available to Download	17
CD-ROM Not a Computer Under CFAA	9
Maryland Repeals Tax on Computer Services	10
Cybersquatting Increase by 33 percent	14
Bad Faith Not Found in Spoliation Claim	9
New York to Collect Tax for Online Purchases	11
Teen Not Buying CDs, Using Digital Downloads	14
E-Discovery: “Burdensome” Must be Defined	10
IP Bill Contains State Grants Provision	11
Researchers Find How to Steal Encrypted Data	15
Online Pharmacy Bill Includes State Provisions	11

Table of Contents

<u>Features</u>	
Michigan Sting Nets Predators	2
Cybercrime and Juveniles Course Offered	18
<u>AGs Fighting Cyber Crimes</u>	3
26 AGs Settle With Online Directory	
AG Goddard Sues Internet Stone Business	
Connecticut AG Sends Inquiry to Gossip Site	
AG Biden Unveils Child Predator Unit Offices	
Florida AG Says Predator Sentenced	
AG Baker Announces Sentence for Predator	
Hawaii AG Says Predator Sentenced After Plea	
AG Wasden Says Net Tobacco Seller Penalized	
Kentucky AG: e-Bay Seller Indicted for Fraud	
AG Caldwell’s Unit Arrests Predator	
Mississippi AG: Child Pornographer Convicted	
AG Nixon Sues Personal Search Web Site	
New Jersey AG Subpoenas JuicyCampus.com	
AG King’s Office Gives Net Safety Presentation	
North Carolina AG Arrests Predator	
South Carolina AG’s ICAC Arrests Predator	
AG Abbott Announces Plea by Pornographer	
Virginia AG Announces Net Safety Finalists	
AG Shurtleff Says 3 Pornographers Arrested	
Washington AG Sues Under Spyware Law	
<u>In the Courts</u>	7
Kazaa User Found to be Pornography Distributor	
Suit by Victim for Posting Personal Data Fails	
Virginia Spam Statute Upheld	
Claim That “Live Bidding is Safe Not Preempted	
CD ROM Not “Computer” Under CFAA	
Court Finds Poor Keyword Search, No Bad Faith	
“Burdensome” Discovery Objection Needs Details	
<u>Legislation Update</u>	10
South Dakota Bans Text Message Threats	
Iowa Gives Tax Exemption for Web Portals	
Maryland Tax on Computer Services Repealed	
New York to Tax Online Purchases	
House IP Bill Contains State Grants	
Senate Online Pharmacy Bill Allows State Suits	
House Committee Bill Providers Surplus Computers	
Parental Control Technology Study in House Bill	
Internet Gambling Bill Introduced in House	
<u>News You Can Use</u>	12
Alliance to Block Pedophiles Use of Cell Phones	
13 Nations Cited as Lax in Fighting Piracy	
Survey Finds Most Mobile Users Lack Security	
ICANN Panel Finds No Domain “Snatching”	
Rogue Servers Used by Hackers Increasing	
DHS Approves Passenger Security Technology	
RIAA Sends Pre-Litigation Letters to Colleges	
Cybersquatting Rises 33 Percent	
Teens Get Music By Downloads, Not CDs	
U.S., Europe Lead Rise in IT Governance	
Researchers Find How to Steal Encrypted Data	
Internet Has Unexpected Effects on Journalism	
FCC Grant Will Foster Telemedicine in Rural Areas	
Airwave Auction Winners Announced	
New Chair of FTC Announced	
Map of State Data Breach Laws Available	
Over 1 Million Pages of Federal Decisions Posted	
Record Number of Cybersquatters Ousted	
<u>Tools You Can Use</u>	17
Resources to Deter Cyberbullying Posted	
Guide to Sting Operations 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.

MICHIGAN “STING” NETS PREDATORS

By Tom Lambert, Chief Information Officer
Office of the Attorney General of Michigan

One rode his bicycle 10 miles in 15-degree weather. Another was dropped off by his sister and entered the home while exposing himself. Another was so interested in getting to his destination that he knowingly drove on a flat tire.

All three had one thing in common: they were among 27 alleged Internet predators hoping to prey upon young children; instead, they were greeted by law enforcement officials during an undercover operation.

The sting was a collaborative effort between Attorney General Mike Cox's Office, the Wayne County Sheriff's Office and the Van Buren Township Department of Public Safety. In all, 27 Internet predators were arrested. All of the predators, with the exception of one who was on a business trip, resided in Michigan. A physician was among those arrested. They were all male and ranged

in age from 19 to 57 years old, with the average age at 30 years. Evidence seized by law enforcement officers included video cameras, laptop computers, beer, condoms, lotion and videotapes.

"Law enforcement has a clear choice in dealing with the danger of Internet predators – either react after a child has been subjected to an assault or be proactive and intervene before they harm a child," said Attorney General Cox. "For us, this is an easy choice. We're going after all those who use the dark side of the Internet to target children. And let this be a message to all those who would put children in harm's way – we're watching you."

Including the sting arrests, Attorney General Cox's Child and Public Protection Unit has arrested 185 Internet Sexual predators since 2003. The office

also created the Michigan Cyber Safety Initiative (Michigan CSI), an Internet safety education program with customized presentations for kindergarten through eighth-grade students and a community seminar. More than 1,600 presentations have been

given to more than 150,000 students to date.

A criminal charge is merely an accusation, and defendants are presumed innocent until and unless proven guilty.

AGs FIGHTING CYBER CRIMES

MULTI-STATE

A total of **26 Attorneys General** reached a settlement with Florida-based Direct Billing, LLC, doing business as USDirectory.com, an Internet Yellow Page listing service, resolving allegations that the company engaged in deceptive business practices. The states alleged that the company sent “activation” checks to businesses and organizations in small amounts, but on the back of the checks, in very fine print, was language stating that by depositing the check, the recipient was authorizing Direct Billing to bill them monthly fees. According to the terms of the settlement agreement, Direct Billing has agreed to no longer use activation checks as a marketing tool. The company will also pay \$400,000 to the states for restitution to former customers and for their investigative costs. The company must also contact customers that used the activation checks and inform them of their right to cancel their agreement and their potential eligibility for a refund. The states participating in the settlement are: Alaska, Arizona, Arkansas, California, Connecticut, Delaware, Florida, Idaho, Illinois, Louisiana, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, North Carolina, North Dakota, Oregon, Pennsylvania, South Carolina, Tennessee, Texas and West Virginia.

ARIZONA

Attorney General Terry Goddard filed a lawsuit against Top Stone, Inc., an Internet business that markets marble and granite products, alleging that Top Stone routinely failed to deliver merchandise to consumers within a reasonable period of time or sometimes not at all, while still requiring customers to make large deposits when placing an order. Attorney General Goddard has sought to enjoin Top Stone from conducting business in Arizona. The suit also asks for civil penalties of up to \$10,000 per violation of the state Consumer Fraud Act to be assessed, for restitution to consumers harmed by the company’s conduct and for the costs of the investigation and reasonable attorney’s fees. Assistant Attorney General Taren Ellis is handling the case.

CONNECTICUT

Attorney General Richard Blumenthal sent a letter to college gossip web site JuicyCampus.com, which allows students at colleges and universities to post anonymous gossip, asking for information and documents on enforcement of its rules prohibiting libelous, defamatory and abusive postings. In spite of the ban, students and administrators complain that the site is rife with malicious falsehoods and provides no means to report and remove such abuses.

DELAWARE

Attorney General Joseph R. Biden, III joined other state officials to unveil the new offices of their Child Predator Task Force at their headquarters in Dover. Attorney General Biden also announced that almost 30 new police agencies have been added to the Task Force. The Task Force was established last June by the Delaware Department of Justice and the State Police, with support from the U.S. Attorney's Office and other federal agencies. Last October, the Task Force received a \$250,000 grant from the U.S. Department of Justice, which it used to enhance its forensic capabilities, facilitate staff training and secure the new office space.

FLORIDA

Attorney General Bill McCollum announced that Gabriel Garay was sentenced to three years in prison after he pled guilty to four counts relating to the use of a computer to commit crimes against a minor. Garay was arrested as part of a sweep for sexual predators conducted by the Polk County Sheriff's Office and was prosecuted by Attorney General McCollum's Office of Statewide Prosecution. He admitted to contacting online, sending graphic images of himself and arranging a sexual encounter with what he believed to be a 14-year-old girl but was actually a deputy sheriff. Garay was arrested when he arrived for the encounter. He pled to Use of a Computer to Seduce a Child, Attempted Use of a Computer for Child Exploitation and two counts of Transmitting Material Harmful to Minors and faced up to 20 years in prison. After his prison term, Garay will be on sex offender probation for two years and must register as a sex offender.

GEORGIA

Attorney General Thurbert Baker announced that Ricky Labrew was sentenced to 30 years in prison after entering a plea to 56 counts of Sexual Exploitation. Labrew will also be subject to special conditions of parole, including registration as a sex offender, prohibition of Internet use and of

contact with minors. The investigation began when ISP Yahoo reported to the National Center for Missing and Exploited Children that images of child pornography were being uploaded to Yahoo Internet groups. An investigation revealed that Labrew, a state Department of Transportation engineer, had been uploading child pornography onto the computers at his work place using his personal AOL account and Yahoo e-mail address. Labrew was prosecuted by Senior Assistant Attorney General Kimberly Schwartz and Assistant Attorney General Daniel Hiatt in Attorney General Baker's office.

HAWAII

Attorney General Mark Bennett announced that Marc Fossorier was sentenced following a guilty plea to five years of probation and one year of incarceration for Electronic Enticement of a Child in the First Degree. He also is required by law to register as a sex offender. Fossorier used the Internet to solicit sexual conduct from a Special Agent in Attorney General Bennett's office, whom he believed to be a 15-year-old girl. He arranged to meet the "girl" at a shopping center and was arrested when he arrived by law enforcement agents of the state Internet Crimes Against Children Task Force.

IDAHO

Attorney General Lawrence Wasden announced that a \$163,225 civil penalty has been imposed on Scott Maybee, a high-volume Internet tobacco seller, who sold his products on such web sites as smartsmoker.com, ordersmokesdirect.com and buycheapcigarettes.com. Maybee was also enjoined from engaging in future illegal tobacco sales. Attorney General Wasden obtained a judgment and order against Maybee for violations of the state's Tobacco Master Settlement Agreement Complementary and Prevention of Minors' Access to Tobacco Acts, resolving a lawsuit Attorney General Wasden filed against Maybee for repeated violations of these laws. The lawsuit had alleged that Maybee sold more than two million cigarettes that were not on Attorney General Wasden's Directory of Compliant Tobacco

Product Manufacturers and Brand Families, in violation of the state's Complementary Act.

KENTUCKY

Attorney General Jack Conway announced that Erica McGinn, a former resident of Nebraska, was indicted for failing to deliver a Lexus she sold on eBay to a Kentucky resident for more than \$30,000. In fact, she never owned a Lexus. Investigators charged McGinn with one count each of Theft by Failure to Make Required Disposition of Property Over \$300, a Class D felony, and Unlawful Access to a Computer Network in the First Degree, a Class C felony, which together carry a sentence of up to 10 years imprisonment. Attorney General Conway's Office of Consumer Protection used telephone and bank records, working with the Council Bluffs, Iowa Police Department and eBay to locate McGinn in North Carolina, where she was subsequently arrested on an outstanding auto theft charge.

LOUISIANA

Attorney General James "Buddy" Caldwell's High Technology Crime Unit (HTCU) investigators arrested Jason Wesley at his place of employment subsequent to the execution of a search warrant at his residence. Wesley allegedly contacted a member of the HTCU who he believed to be a 14-year-old female during an undercover online operation and engaged in chats of a sexual nature. Wesley was booked into prison on charges of Indecent Behavior With a Juvenile and Computer-Aided Solicitation of a Minor. The Livingston Parish Police Department assisted with the arrest, and the Baton Rouge Police Department assisted in the search of the residence.

MISSISSIPPI

Attorney General Jim Hood announced that Rubin Renfrow, a former school teacher, was convicted by a jury on possession of child pornography. At trial it was shown that Renfrow received images of child pornography by e-mail from people in Russia, which he saved in a folder

called "pedo." Attorney General Hood's prosecutors tried the case with the Simpson County District Attorney.

MISSOURI

Attorney General Jay Nixon filed a lawsuit against A1 Peoplesearch, LLC of Texas, doing business as a1peoplesearch.com, alleging that the web site provides access to personal information, such as Social Security numbers, addresses, dates of birth and criminal records, to anyone with a credit card, allowing such a purchase for as little as 97 cents. Both the Federal Driver Privacy Protection Act and its state counterpart allow individuals and businesses to obtain information contained in a driving record, but only for specified uses. The lawsuit asks that the court issue a temporary restraining order, and eventually a permanent injunction, requiring disabling of the web site to the extent it allows searches by, or retrieval of, Social Security numbers. It also asks for civil penalties and the costs of investigating and prosecuting the case.

NEW JERSEY

Attorney General Anne Milgram's prosecutors subpoenaed the records of JuicyCampus.com, a web site that publishes anonymous, often malicious, gossip about college students. The information subpoenaed seeks data on how the web site is run. The investigation began when a student came forward who had been terrorized by posts on the site that included her address, and will look at whether the web site may be violating the state's Consumer Fraud Act by suggesting that it does not allow offensive material but providing no enforcement of that rule and no way for users to report or dispute the material. Attorney General Milgram has also subpoenaed the site's advertising agency, Adbrite, to determine how JuicyCampus.com represented its operation and what advertising keywords the site requested, and Adbrite has promised complete cooperation.

NEW MEXICO

Attorney General Gary King's Office gave an Internet safety presentation to sixth through eighth grade students at a state middle school. The program was designed to help the students learn how to protect themselves from online predators.

NORTH CAROLINA

Attorney General Roy Cooper's State Bureau of Investigation (SBI) Computer Crimes Unit arrested Michael Ingraham, a former youth soccer coach, on charges of possession of child pornography. The SBI launched the investigation when Ingram's name came up as a person of interest in an unrelated investigation. Ingram consented to a search of his home computers, and a subsequent forensic examination revealed image and video files of child pornography which appeared to have been downloaded from the Internet. Ingram faces seven felony counts each of second degree and third degree sexual exploitation of a minor for possession of child pornography. He will be prosecuted by the Durham County District Attorney's Office.

PENNSYLVANIA

Attorney General Tom Corbett's Child Predator Unit arrested James Stone, accusing him of using the Internet to sexually proposition what he believed was a 12-year-old girl but was actually a Unit undercover agent. Stone, using the screen name "Spanther5," allegedly posed as an 18-year-old boy in an Internet chat room created to discuss Playstation video games to approach the "girl," subsequently sending sexually explicit videos via a webcam. Stone was arrested at his home by Unit agents assisted by the Philadelphia police. Agents executed a search warrant and seized two computers and pornographic material, which will be analyzed by Attorney General Corbett's Computer Forensics Unit. Stone is charged with seven counts of unlawful contact with a minor and one count of criminal use of a computer, all third degree felonies each punishable by up to seven years in prison and a \$ 15,000 fine. He has been temporarily arraigned

and lodged in prison in lieu of \$100,000 bail. The case will be prosecuted by Deputy Attorney General Michael Sprow of the Unit. The Lower Providence Township Police Department also assisted in the investigation.

SOUTH CAROLINA

Attorney General Henry McMaster announced that Larry Robertson was arrested during an undercover Internet sting conducted by the City of Maudlin Police Department, a member of Attorney General McMaster's Internet Crimes Against Children Task Force. Robertson 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. Arrest warrants allege that Robertson solicited sex from an undercover police officer whom Robertson believed to be a 13-year-old girl. He further arranged to meet the "girl" for sex at a predetermined location, where he was arrested upon his arrival. The Spartanburg County Sheriff's Office, another Task Force member, assisted in executing a search warrant on Robertson's home, resulting in the seizure of one laptop, three computer towers, one web camera and one digital camera. Robertson was assigned a \$15,000 bond. The case will be prosecuted by Attorney General McMaster's Office.

TEXAS

Attorney General Greg Abbott announced that James Butler pled guilty to 10 counts of child pornography possession and was sentenced to five years in prison for each count, with the sentences to run concurrently. Upon release, Butler must register as a sex offender. Butler was investigated and prosecuted by Attorney General Abbott's Cyber Crimes Unit. The investigation revealed that Butler had created a false profile on MySpace, where he claimed to be a 14-year-old boy, and used that profile to e-mail child pornography to a young teenager in Illinois. The child's mother reported the incident to the National Center for Missing and

Exploited Children, which turned the case over to the Unit.

VIRGINIA

Attorney General Bob McDonnell announced the three student team finalists in the state Youth Internet Safety contest. The finalists were selected from more than 200 submissions from 85 different schools in the Commonwealth. State citizens could vote for the winning ad on <http://www.projectsafetynetva.com>.

UTAH

Attorney General Mark Shurtleff announced that members of the Utah Internet Crimes Against Children Task Force arrested three child pornography suspects after an investigation named “Operation Spring Cleaning.” The Task Force also served 13 search warrants for computers believed to have been used to upload and view illegal child pornography videos and photographs. The investigation included agents from Attorney General Shurtleff’s Office, the Utah Departments of Public Safety and Corrections, the FBI, the U.S. Marshal’s Office, the Duchesne County Sheriff’s

Office and the West Valley, Salt Lake City, Layton, Tooele and Murray Police Departments.

WASHINGTON

Attorney General Rob McKenna filed suit against Ron Cook of Arizona, the owner of Messenger Solutions, LLC., for violations of the state’s Computer Spyware Act, including transmitting malicious software, attempting to coerce consumers into purchasing software and misrepresenting the necessity of software for security purposes. The complaint alleges that Cook coerced consumers into buying software to block computer pop-ups by first bombarding them with ads for pornography and Viagra. Consumers who downloaded the software were victimized again when the software caused their computers to blast messages to other PCs at the rate of one message every two seconds. The suit requests an injunction to stop the deceptive behavior, as well as civil penalties and refunds for consumers. The case is being handled by Assistant Attorney General Katherine Tassi.

IN THE COURTS

DISTRIBUTION OF CHILD PORNOGRAPHY: KAZAA FILES

United States v. Sewell, 2008 WL 150704 (8th Cir. January 17, 2008). The 8th Circuit Court of Appeals upheld a conviction of a defendant on a charge of publishing a “notice” offering to distribute child pornography through the defendant’s use of Kazaa file-sharing software. Walter Sewell was indicted on several counts, including distributing and attempting to distribute child pornography, possession of child pornography and publishing a notice offering to distribute child pornography.

Sewell pled guilty to acquiring and distributing child pornography, as well as one count of publishing a notice, but preserved the right to file a motion to dismiss that charge on appeal. The U.S. District Court for the Western District of Missouri rejected Sewell’s motion. Sewell appealed, arguing that in downloading child pornography via Kazaa and sharing the files with other users, he did not cause to be published a notice offering to distribute child pornography, which is an essential element of the offense. The 8th Circuit rejected Sewell’s argument, concurring with the prosecution that the notice

clearly demonstrated that Sewell was offering to distribute child pornography.

**RIGHT OF PRIVACY: WEB
POSTING OF PERSONAL
INFORMATION**

Lambert v. Hartman, 2008 U.S. App. LEXIS 4019 (6th Cir., February 25, 2008). The 6th Circuit Court of Appeals ruled that an identity theft victim's civil rights suit under 42 U.S.C. § 1983 against a state agency that posted her personal information on a public web site is not viable because her fundamental constitutional rights are not implicated. Cynthia Lambert received a traffic citation for speeding and later found that the citation, which included her social security number and other personal identifying information, had been posted on the Clerk of Hamilton County (Ohio)'s web site. She sued the clerk and the County Board of Commissioners, alleging that the publication of the citation violated her constitutional right to privacy under the 14th Amendment. She also claimed that her identity had been stolen as a direct result of the posting, causing her economic damage, and she also raised pertinent state law claims. The county moved to dismiss the complaint for failure to state a claim under § 1983. The U.S. District Court for the Southern District of Ohio, concluding that Lambert's claim must fail because her privacy interest did not reach a constitutional level, granted the motion and then dismissed her state law claims without prejudice. Lambert appealed, arguing again that her constitutional right to privacy was violated. The appeals court affirmed the lower court's decision on the same basis.

**SPAM STATUTE:
CONSTITUTIONALITY**

Jaynes v. Commonwealth, 2008 WL 539744 (Va. February 29, 2008). The Virginia Supreme Court upheld the conviction of a spammer under the unsolicited bulk electronic mail provisions of the state's Computer Crimes Act. Jeremy Jaynes, a North Carolina resident, sent more than 50,000 unsolicited e-mails advertising specific products on six separate occasions to America Online (AOL) subscribers. All of the e-mails had falsified routing and transmission information, but investigators used a complex database search to identify Jaynes as the sender. While executing a search of Jaynes' home, police found a cache of compact discs containing millions of e-mail addresses and e-mail user names, including millions of AOL subscribers. Jaynes was convicted by a jury and appealed, alleging that the court lacked subject matter jurisdiction and that the statute was unconstitutionally vague and violated both the First Amendment and Dormant Commerce Clause. The Virginia Appeals Court found no merit to his arguments and upheld the conviction. Jaynes appealed again. The state Supreme Court found that Virginia had jurisdiction to criminally prosecute the out-of-state spammer because Jaynes clearly intended to send his e-mails to AOL subscribers and knew his e-mails would utilize AOL servers, which were located in Virginia. The court also rejected Jaynes' claims that he had standing to raise a First Amendment defense and that the statute was void for vagueness.

SECTION 230 IMMUNITY:
ONLINE MARKETING
REPRESENTATIONS

Mazur v. eBay, Inc., 2008 WL 618988 (N.D. Cal. March 4, 2008). A federal district court found that an online auction site's assertion that live bidding is "safe" is not preempted by 47 U.S.C. 230. eBay offers its users the opportunity to participate via the Internet in "live bidding," at auction houses currently taking place through third party vendors. eBay's marketing materials described the third party vendors as "safe," "carefully screened" and "reputable," and that the bidding was against floor bidders at the physical location of the auction. Michele Mazur sued eBay, claiming that shill bidders at the auction resulted in her overpaying. eBay claimed Section 230 immunity and said that any untruth in its statements were attributable to third party vendors. The U.S. District Court agreed as to Mazur's claim that eBay knew of the illegal conduct and her claim that eBay was liable for information provided by a third party, but the court found that eBay's statement regarding safety created an expectation regarding the auction's procedures that went beyond editorial discretion.

COMPUTER FRAUD AND ABUSE
ACT: CD ROM

GWR Medical, Inc. v. Baez, 2008 WL 698995 (E.D. Pa. March 13, 2008). A federal district court held that a CD-ROM does not meet the definition of "computer" under the Computer Fraud and Abuse Act (CFAA). When GWR Medical terminated Hector Baez, Baez took with him a CD-ROM containing training materials and, allegedly, trade secrets. GWR sued him in the U.S.

District Court for the Eastern District of Pennsylvania for violation of the CFAA, which states that "whoever intentionally accesses a computer without authorization or exceeds authorized access" and obtains information violates the law. GWR claimed that by keeping the CD-ROM, Baez exceeded the authorization he had. Baez moved to dismiss the claim, arguing the CD-ROM was not a computer. The court divided the CFAA's definition of a computer into three parts: 1) "an electronic, magnetic, optical, electrochemical or other high speed data processing device," 2) "performing logical, arithmetic or storage functions," which 3) "includes any data storage facility or communications facility directly related to or operating in conjunction with such device." The court found that the CD-ROM lacked the requirement that it process information, and therefore dismissed the claim.

E-DISCOVERY CASES

SPOILIATION: INADEQUATE
KEYWORD SEARCHES

Diabetes Centers of America v. Healthpia America, Inc., 2008 WL 336382 (S.D. Tex. February 5, 2008). The U.S. District Court for the Southern District of Texas denied both parties' requests for an instruction on spoliation, finding no evidence that either party acted in bad faith. In this highly contested case, defendant Healthpia alleged that Diabetes Centers failed to preserve and produce critical e-mails that were adverse to them. At a hearing on a spoliation motion, the counsel for Diabetes Centers "fell on his sword" by saying it was his, not his client's, fault because he entrusted the task of searching the records to a junior

associate who used inadequate search terms in selecting relevant records. He also filed his own motion for spoliation, alleging that Healthpia had intentionally destroyed electronic evidence. Healthpia admitted some e-mail had been lost, but blamed it on stolen laptops. The court denied both motions for lack of a finding of bad faith.

**“BURDENSOME” PRODUCTION
OF E-MAILS: SPECIFICITY**

City of Seattle v. Professional Basketball Club, LLC, 2008 WL 539809 (W.D. Wash. February 25, 2008). The U.S. District Court for the Western District of Washington ruled that an objection to the production of electronically stored information on the basis that it is

burdensome must be specific as to the reasons it is burdensome. The City of Seattle requested that Professional Basketball Club (PBC), LLC search for and produce responsive e-mails for six of its eight members. PBC produced approximately 150,000 e-mails from two members, but objected to producing e-mails of the other four members because it was burdensome and would generally result in irrelevant documents. The court found that the basis of the requested e-mails might lead to relevant information. It then observed that an assertion that discovery would be burdensome, without more, was insufficient to satisfy Fed. R. Civ P. 26(b)(2)(B) and granted the City’s motion.

LEGISLATION UPDATE

Text Message Threats

On March 13, **South Dakota** Governor Mike Rounds signed H.B. 1313 into law, a bill, effective July 1, that will revise an existing law to make ominous or annoying text messages illegal. The law applies to traditional telephones, cell and satellite phones and computers linked to the Internet by cable television. The law makes it a crime to terrorize, threaten, harass or annoy with lewd language; threaten physical injury or property damage; attempt to extort money or valuables; or disturb repeatedly by anonymously contacting people. Violations carry a maximum one year in jail and a \$2,000 fine. The full text of the legislation can be accessed at <http://www.legis.state.sd.us/sessions/2008/Bills/HB1313P.htm>.

Internet and Computer Taxes

Iowa Governor Chet Culver signed H.F. 2233 into law, which provides for sales and property tax exemptions to businesses that establish web search portal companies in the state. The new law provides state sales tax exemptions on the sales or rentals of computers and equipment necessary for the maintenance and operation of a web search portal business, as long as the business is located in the state and invests a minimum of \$200 million in the state in its first six years of operation.

On April 8, **Maryland** Governor Martin O’Malley signed a bill repealing the state’s new tax on computer services before it was to take effect in July. The six percent “tech tax” had been initiated by a Senate panel during the three-week special session last fall and was not

included in Governor O'Malley's revenue proposals.

A recent **New York** law requires out-of-state Internet retailers to begin collecting sales tax on purchases made in New York, effective June 1. State budget officials estimate that the law will bring in \$50 million in revenue this year and \$73 million the following year, New York has sent notices to the 500 largest e-tailors in the state, advising them to register and begin taxing purchases. The law affects companies doing \$10,000 or more worth of business in the state and that have agents in the state. Failure to comply would result in a state audit and assessment for past liabilities. Since eBay is a marketplace, it is not required to collect sales taxes, but retailers on eBay meeting the \$10,000 with agents in the state criteria are. The tax was proposed by then-Governor Eliot Spitzer and then dropped, but Governor David Paterson included it in the state budget so the legislature could decide. It is referred to as "the Amazon tax" since Amazon has sued the state over its implementation.

Intellectual Property Enforcement

The **U.S. House of Representatives** ("House") passed H.R. 4279, a bill to strengthen intellectual property enforcement, by a 2/3 majority. The bill, sponsored by Representative John Conyers (D-MI), would create stiffer penalties for piracy and counterfeiting, including increasing maximum fines from \$1 million to \$2 million for willful use of a counterfeit mark. It also makes it illegal to export counterfeit goods. The bill reorganizes and provides additional resources to the Justice Department to prioritize intellectual property violations, establishing an Intellectual Property Enforcement Representative to coordinate federal efforts. H.R. 4279 also provides \$25 million in grants to help state and local law enforcement combat intellectual property crimes. The bill has been referred to the U.S. Senate ("Senate") Judiciary Committee.

Online Pharmacies

On April 1, the **Senate** unanimously passed S, 980, a bill sponsored by Senator Dianne Feinstein (D-CA) prohibiting the delivery and/or distribution of controlled substances over the Internet without a valid prescription. A valid prescription is defined as a prescription issued for a legitimate purpose by a practitioner who has conducted at least one in-person medical evaluation of the patient. The bill also imposes reporting and registration requirements on online pharmacies, including notifying the applicable state boards of pharmacy prior to operation. It also authorizes states to obtain injunctions or obtain damages and other civil remedies against online pharmacies deemed a threat to state citizens. The bill has been referred to the House Committees on the Judiciary and on Energy and Commerce.

Surplus Computer Equipment

The **House Committee on Oversight and Government Reform** passed H.R. 752, a bill sponsored by Representative G.K. Butterfield (D-NC) that directs Federal agencies to donate excess and surplus electronic equipment to qualifying small towns, counties, schools, non-profits and libraries.

Internet Safety

On March 3, the **House Committee on Commerce, Science and Transportation** reported out S. 602, a bill sponsored by Senator Mark Pryor that would require the Federal Communications Commission to study advanced blocking and parental control technology.

Internet Gambling

On March 4, Representative Jim McDermott (D-WA) introduced H.R. 5523, a bill that would impose an Internet gambling license fee on Internet gambling operators and require them to file returns identifying the individuals placing bets with them. It would also impose

withholding tax on annual Internet winnings of more than \$5,000, as well as impose a 30 percent excise tax on winnings by non-resident aliens. Lastly, it would impose an excise tax on the

wagers of any individual who places a wager with an unlicensed Internet operator. The bill has been referred to the **House Ways and Means Committee**.

NEWS YOU CAN USE

ALLIANCE TO BLOCK PEDOPHILES SENDING IMAGES BY CELL PHONE

The GSM Association (GSMA), a global trade association of more than 700 mobile firms, launched the Mobile Alliance “to create significant barriers to the misuse of mobile networks and services for hosting, accessing or profiting from child sexual abuse content.” Members of the Alliance commit that they will implement “Notice and Take Down” procedures that will result in the rapid removal of child sexual abuse content they are notified about on their own networks. Planned measures include a block on mobile phone access of web sites with abusive content and hotlines to report services carrying inappropriate images. Joining GSMA in founding the Alliance are Hutchinson 3G Europe, mobilkom austria, Orange FT Group, Telecom Italia, Telefonica/02, Telenor Group, TeliaSonera, T-Mobile Group, Vodafone Group and dotMobi.

13 NATIONS LISTED AS WORST IN FIGHTING PIRACY

The International Intellectual Property Alliance, an industry coalition of the software, music and movie industries,

released their annual list of countries with the worst records of fighting piracy of copyrighted goods. Listed were Argentina,

Canada, Chile, China, Costa Rica, Egypt, India, Mexico, Peru, Russia, Saudi Arabia, Thailand and Ukraine. The Alliance asked the U.S. Trade Representative’s office to place these countries on the “priority watch list” for copyright theft. It also recommended placing 29 other countries or territories on the lower priority “watch list,” including the following new additions to the list: Bangladesh, Brunei, Greece, Israel, Kazakhstan, Lebanon, Nigeria, Spain, Sweden and Turkey. The Alliance also said that it “conservatively” estimates that U.S. companies lost \$30 - \$35 million in worldwide sales in 2007.

SURVEY: MOST MOBILE USERS HAVE NO SECURITY

More than three-quarters of mobile users have no security, according to a survey by McAfee, a security vendor. The survey was conducted on McAfee’s behalf by Datamonitor, an analysis firm, of mobile users in the U.S., United Kingdom and Japan. It found that 79 percent of mobile device users do not use any anti-virus or other security software, and 15 percent were not sure if their device had such software. However, McAfee acknowledged that these percentages may be somewhat misleading because many mobile products, such as Blackberries and iPhones, have generally not been the target of malware nor are there anti-virus solutions available. Sixty percent of users said they expect mobile operators to have primary responsibility for protecting their mobile devices. The survey

also found that users of advanced mobile services, such as web surfing, were more concerned about security. The complete report may be accessed at http://www.mcafee.com/us/research/mobile_security_report_2008.html.

PANEL: DOMAIN TASTING BUT NO DOMAIN SNATCHING

A committee of the Internet Corporation for Assigned Names and Numbers (ICANN), the organization which has oversight of domain name policies, has found no evidence that insider information is being used to “snatch” desired Internet addresses to make money from the individual or business that actually wants to register them. The Security and Stability Advisory Committee said that the 120 claims they reviewed generally resulted from misunderstandings about the process. They recommended better education in how the system works. However, the committee did find that the practice of domain “tasting,” in which someone uses a loophole in registration policies to test the financial worth of a domain name for up to five days, and then returns it for a full refund if it is not up to expectations, is tying up millions of Internet addresses. The report did not examine a controversial practice of “front running,” under which domain name sellers grab names that people search for on its web site but do not immediately register.

RESEARCHERS FIND INCREASE IN ROGUE SERVERS

Rogue servers controlled by hackers that reroute Internet traffic from infected computers to fraudulent web sites are being used more often to launch attacks, according to a paper published by researchers at the Georgia Institute of Technology and Google Inc. The peer-reviewed paper, “Corrupted DNS Resolution Paths: The Rise of a

Malicious Resolution Authority,” estimates that approximately 68,000 servers on the Internet are returning malicious Domain Name System (DNS) results, meaning unsuspecting users with compromised computers can be directed to a sham web site. The hackers who hijack DNS queries seek to obtain personal information and take over infected machines. The report also noted that the rogue DNS servers sometimes direct users to the legitimate web site, deceiving users into thinking that there is no problem with their Internet access. The paper was presented at the Internet Society’s 2008 Network and Distributed System Security Symposium by researchers David Dagon, Chris Lee and Wenke Lee from Georgia Institute of Technology and Niels Provos from Google Inc.

US SELECTS PASSENGER CHECK SYSTEM

SITA, an information technology firm owned by a consortium of more than 600 air transport firms, won approval from the U.S. Department of Homeland Security for a system providing passenger details to border authorities within approximately two seconds. Currently, airlines flying to, from or over the U.S. must submit a manifest listing all passengers and crew, as well as passengers’ travel document details, to U.S. Customs and Border Protection 30 minutes in advance of departure to be checked against a terrorist watch list. Industry officials have been concerned about the resulting possibility of frequent delays and disruption in airport operations. The SITA Advanced Passenger Information System Quick Query would enable an airline to send manifest information to Customs and Border Protection as each passenger checks in and receive an immediate board/no board response. The system could also be used with automatic kiosks and for telephone and Internet check-in.

RIAA SENDS 13TH WAVE OF PRE-LITIGATION LETTERS

The Recording Industry of America (RIAA) sent its 13th mailing of pre-litigation settlement letters consisting of another 401 letters to administrators of 12 universities. The letters cite individuals associated with specified IP addresses for online music theft over the universities' computer networks via peer-to-peer services, and the administrators were asked to forward them to those individuals. This mailing went to the following alphabetic list of universities followed by the number of letters each received: Columbia University, 50; Drexel University, 33; Indiana University, 40; North Carolina State University, 35; Ohio State University, 30; Purdue University, 28; Tufts University, 20; University of Maine System, 32; University of New Hampshire, 32; University of Southern California, 50; and University of Virginia, 16. Recipients of the letters are told they have the opportunity to avoid a potential copyright infringement lawsuit by settling out of court for a reduced fee.

ONLINE COUNTERFEITING RISES 33 PERCENT

“Cybersquatting,” the use of domain names designed to mimic those of large brands, has risen 33 percent compared with one year ago, according to a study by MarkMonitor, a provider of enterprise brand protection. Cybersquatters frequently use misspellings in web site addresses to attract users looking for name brands, earning money through pay-per-click advertising or selling counterfeit products. The study noted that some of the biggest increases in brand mimicry were in apparel, which increased almost 50 percent, and food and beverage, which increased 67 percent. However, the study did find that recent crackdowns on such counterfeiting has had an effect. For

example, kiting, a form of cybersquatting in which a domain name is registered for only a short time, is declining. The study found that the United States is the leading source of web sites hosting brand abuse with 68 percent, followed by Germany at nine percent, the United Kingdom at four percent and China, two percent.

CD SALES SLUMP AMONG TEENS

Only 52 percent of teenagers bought compact discs in 2007, compared with 62 percent in 2006, illustrating the music industry's anguished transition from CDs to digital downloads, according to a report by research firm NPD Group. The good news was that 29 million people bought music from online music stores last year, a 21 percent increase from 24 million in 2006, but it did not offset the drop in CD sales and the effect of people illegally downloading music. According to the report, almost one million consumers stopped buying CDs altogether last year. Although the average Internet user obtained six percent more music overall last year, both by legal and illegal means, they spent 10 percent less on music. The report also underlined a generational divide, with the increase in legal online sales spurred by people aged 36 to 50.

U.S., EUROPE LEAD INCREASE IN IT GOVERNANCE

Most businesses across the world are increasing their IT governance practices, according to the “IT Governance Global Status Report 2008.” The report finds that 34 percent of respondents, compared to 19 percent in 2005, are implementing practices affecting the performance and security of their IT systems. The study, commissioned by the IT Governance Institute (ITGI) and conducted every two years, surveyed 750 executives from 23 countries. The survey also found that 24 percent of companies are considering plans

to introduce IT governance practices, compared to 22 percent in 2005 and 18 percent in 2003. Additionally, only 20 percent said their companies were not considering such practices, compared to 36 percent in 2005 and 42 percent in 2003. By region, North America and Europe have the highest adoption of IT governance initiatives, with one-half of respondents in each region having already implemented such practices. Next came Asia, with 44 percent of executives reporting implementation, followed by South America, with 27 percent. The survey also found that 40 percent of executives identified the chief information officer as the person driving the effort, with 28 percent identifying the chief executive officer. The full report can be accessed on the organization's web site, www.itgi.org.

PRINCETON RESEARCHERS LEARN HOW TO STEAL ENCRYPTED DATA

Princeton University researchers announced they had discovered a new vulnerability in the dynamic random access (DRAM) chip found in computers, commonly known as computer memory. It was originally believed that data was lost when the computer was turned off, but the Princeton team found that the data actually fades out over a period of time ranging from seconds to minutes. According to the team's blog, this finding is significant because it would enable an attacker "to read the full contents of memory by cutting power and then rebooting into a malicious operating system." The researchers also found that if the DRAM chips are cooled, they retain the data for much longer. The full report can be accessed at <http://citp.princeton.edu.nyud.net/pub/coldboot.pdf>.

INTERNET HAS UNEXPECTED EFFECT ON JOURNALISM

The Internet has deeply changed journalism, although not in ways that were expected, according to the Project for Excellence in Journalism's annual State of the News Media report. Although previously speculated that the Internet would democratize journalism, offering many new voices, the scope instead seems narrower, with many web sites packaging news that has been produced elsewhere. The report noted that two news stories – the Iraq war and the 2008 presidential election campaign – accounted for one quarter of the stories in all media last year. Without news about Iraq, Iran and Pakistan, the rest of the news stories from all other countries outside the U.S. accounted for less than six percent of the news. The report also noted that most news web sites are no longer final destinations, with many sites offering options to navigate to other sites for more information.

FCC GRANT TO ENLARGE TELEMEDICINE IN WEST

A \$15.5 million grant from the Federal Communications Commission to the Center for Telehealth and Cybermedicine Research at the Health Sciences Center will be used to design, build, operate and evaluate a Southwest Telehealth Access Grid, a broadband network serving rural areas that lack such technology. The grid of networks will support rural systems and connections to more than 500 sites, primarily in Arizona and New Mexico, and including several Indian Health Service sites in California, Colorado, Nevada, Texas and Utah. The grid would improve the network for patient care and training health professionals, as well as allow people to go into emergency mode for disasters. Telemedicine offers virtual travel to bring the patient to specialized care, allowing doctors to diagnose problems

earlier and adjust the patient's care. For example, specialized cameras can screen for eye diseases associated with chronic conditions, such as diabetes, allowing early intervention to prevent potential blindness.

WINNERS OF AIRWAVES AUCTION ANNOUNCED

AT&T Inc. and Verizon Wireless, the two largest cell phone companies, dominated bidding in the government airwaves auction, accounting for \$16 billion of the \$19.6 billion bid in the auction, according to an Associated Press analysis of the Federal Communications Commission (FCC) data. Verizon Wireless, a joint venture between Verizon Communications Inc. and British telecom Vodafone Group PLC, bid \$9.4 billion and won nearly every license in the consumer-friendly "C Block," enough to cover every state except Alaska. AT&T bid \$6.6 billion and Qualcomm Inc. bid \$1.03 billion. The auction failed to attract significant new competitors to the cellular telephone market, although one new entrant, Frontier Wireless LLC, owned by direct broadcast satellite television company EchoStar Corp., bid \$712 million, winning almost enough licenses to create a nationwide footprint. The spectrum was available for bid because of the nationwide transition to digital broadcasting, and the money raised will be used to help public safety programs and offset the budget deficit.

KOVACIC NAMED AS NEW FTC CHAIR

William Kovacic was named as the new chairman of the Federal Trade Commission (FTC), replacing Deborah Platt Majores, who resigned at the end of March. Majores has accepted a position overseeing antitrust issues for Proctor & Gamble. Kovacic served as the FTC's general counsel from 2001 through 2004 and has served as

one of the FTC's five commissioners since January 2006. His appointment as chairman, which does not require Senate confirmation, took effect on March 31. With Majores' departure, the FTC has only four commissioners, and a fifth commissioner will require Senate confirmation.

MAP OF STATE DATA BREACH LAWS AVAILABLE

An interactive map of all states that have data breach notification laws was published by CSO, a security information web site. When a user clicks on a particular state, the map provides information about that state's data breach notification law. The site noted that there are only 11 states without such laws, and that most states have followed California's lead on the issue. The map can be accessed at <http://www.csoonline.com/read/020108/ammap/ammap.html>.

OVER 1 MILLION PAGES OF FEDERAL DECISIONS NOW ONLINE

A joint venture between web site Public Resource.org and Creative Commons has made available online 1.8 million pages of federal case for free. This first release includes all U.S. Supreme Court and U.S. Court of Appeal decisions since 1950 and is equivalent to 1,858 volumes of case law or a stack of books 348 feet tall. The purchase of this extensive case data was made possible by donations from a group that includes the Omidyar Network and individuals David Boies and John Gilmore and the Elbaz Family Foundation. Creative Works is a non-profit promoting the creative re-use of artistic and intellectual works; Public Resource is a non-profit founded to create public works projects on the Internet. The case law can be accessed at <http://bulk.resource.org/courts.gov>.

RECORD NUMBER OF CYBERSQUATTERS REPORTED

The World Intellectual Property Organization (WIPO), a U.N. agency based in Geneva, reported it had ousted a record number of “cybersquatters” from web sites with domain names referring to trademarked companies, foundations and celebrities in 2007. The WIPO received 2,156 complaints alleging “abusive registration of trademarks on the Internet,” up 18 percent from 2006 and 48 percent more than in 2005. Most complaints came from the pharmaceutical, banking, telecommunications, retail and

entertainment sectors. Domain name disputes included Airbus’s A380 jet, the 2010 FIFA World Cup, Harvard Business School, Lance Armstrong’s Livestrong Foundation, talk show host Oprah Winfrey and The Simpsons television show. One-fourth of the cases were settled without a WIPO panel decision. Of the rest, in 85 percent of cases the panels transferred the disputed domain names to the complainant, and in 15 percent of the cases the panel ordered no change in registration. Most domain name complainants came from the U.S., France and Britain, while the majority of respondents were based in the U.S. Britain and China.

TOOLS YOU CAN USE

Cyberbullying Public Service Resources

The National Crime Prevention Council, in partnership with the Bureau of Justice Assistance, produced a public service video called “Chicken” to help prevent cyberbullying. The video targets early teen-aged boys. This and other public service announcements, banners and resources are available on the Council’s web site at <http://www.ncpc.org>.

Sting Operations

“Sting Operations,” a COPS Office Response Guide,” presents a broad approach to crime types and the sting operations that target them. The guide is designed to help law enforcement agencies decide whether a sting operation is the correct response by reviewing benefits and negative consequences. The guide can be accessed at <http://www.cops.usdoj.gov/ric/ResourceDetail.aspx?RID=443>.

“CYBERCRIME AND JUVENILES” CONFERENCE SET FOR AUGUST

Mark your calendars for the “Cybercrime and Juveniles” training conference to be held August 12-14 at the University of Mississippi School of Law in Oxford, Mississippi. The conference, developed under the National Association of Attorneys General’s (NAAG’s) partnership with the National Center for Justice and the Rule of Law, will focus on both crimes against juveniles and crimes committed by juveniles.

The conference is FREE for attorneys from Attorneys General Offices, and TRAVEL EXPENSES will be reimbursed under the partnership. Watch your e-mail for the announcement and registration forms!

YOU CAN BE IN THE HEADLINES!!!!

The Cybercrime E-Newsletter is always interested in feature articles, such as the story about the Michigan sting operation in this issue. The article could be about an interesting case in which you were involved, a new initiative in your office or a new technique you have used in a case. We are interested in both civil enforcement and criminal cases. Contact Hedda Litwin, Cybercrime Counsel, at hlitwin@naag.org or (202) 326-6022 with your ideas.