

News Highlights in This Issue:

Laws to Stop Illegal Online Gambling Urged by 49 AGs	5
Law Journal on Search and Seizure Available	2
E-Mail Provider Not Liable for User's Child Pornography	10
FBI Survey: Computer Crimes Costs \$ 67 Billion/Year	16
Virginia Law Requires Schools to Teach Cyber Safety	21
Report Outlines Needs for Forensics Labs	21
Supreme Court Approves Electronic Discovery Rules	4
E-Mail Service of Elusive Overseas Defendant Allowed	9
Maryland Spam Law Does Not Violate Commerce Clause	13
Internet Coalition Initiates "Stop Badware" Site	17
Kentucky Legislature Outlaws Internet Hunting	21
Supreme Court Clarifies Anticipatory Search Warrants	13
Government Study Says VoIP May Be Taxed by States	18
Financial Body Has No Duty to Encrypt Client Database	12
Survey: 2/3 of Consumers Favor Net Neutrality	15
House Committee Passes Security Breach Legislation	22
Service by E-mail Allowed if Only Practicable Means	12
Free Internet Threat Meter Assesses Online Risks	20
Attorneys Suspended for Illegal Use of E-mail, Spyware	13
IRS Launches Repository for Phishing E-mails	19

Table of Contents

<u>Features</u>	2
Law Journal on Search and Seizure Available	
Net Victimization Seminar Held at Ole Miss	
FRCP Electronic Discovery Amendments Okayed	
<u>AGs Fighting Cyber Crimes</u>	5
49 AGs Urge Laws Stopping Illegal Online Gambling	
AG Lockyer and FTC Settle Spam Suit	
Connecticut AG Urges Changes to MySpace.com	
AG Crist: Judgment Against Katrina Fraud Web Site	
Illinois AG Sets Up ID Theft Hotline	
AG Kline Presents Internet Safety Workshop	
Louisiana AG Speaks at Cyber Crime Workshop	
AG Reilly Arrests Online Child Pornographers	
Michigan AG Arrests Online Child Predator	
AG Hatch Promotes ID Theft Legislation	
Mississippi AG Announces Plea in Phishing Case	
AG Nixon Files Felony Charges in ID Theft Case	
Nebraska AG Kicks Off Internet Safety Month	
AG Chanos: Internet Child Pornography Ring Indicted	
New Mexico AG's ICAC Unit Captures Net Predator	
AG Spitzer Sues Seller of E-Mail Addresses	
North Carolina AG Urges State Classes on Net Crimes	
AG Petro Holds Town Meeting on Internet Safety	
Pennsylvania AG's Unit Charges Internet Predator	
AG McMaster: Internet Predator Arrested	
South Dakota AG Says Child Pornographer Sentenced	
AG Abbott: Grand Jury Indicted Child Pornographer	
Utah AG Unveils ID Theft Reporting System	
AG McKenna Settles With Deceptive Net Advertiser	
<u>In the Courts</u>	10
<u>U.S. Supreme Court Watch</u>	13
<u>News You Can Use</u>	15
Survey: Net Neutrality Rules Would Prevent Abuse	
FBI: Computer Crime Costs \$67 Billion	
Survey: Google Should Not Hand Over User Data	
Most Spam Still Comes From U.S.	
Internet Coalition Launches Stop Badware Site	
Google to Censor Results in China	
Microsoft Announces New Blog Censorship Policy	
Government Study: VoIP, Video May Be Taxed	
NSA Issues Report on Removing Sensitive Data	
U.S. Conducts Test of Internet Defenses	
DOJ Launches Survey of Cyber Crime Statistics	
AOL, Yahoo to Charge Fee to Bypass Filters	
Coalition Fights AOL's Plan to Charge for E-Mail	
Symantec Internet Threat Meter is Free	
Deal Reached on .com Price Hikes	
IRS Launches Mailbox for Suspicious E-Mails	
<u>Publications You Can Use</u>	21
Report on Needs of Forensic Providers	
Document: Telephony Considerations of VoIP	
Bulletin: ID Theft	
<u>Legislation Update</u>	21
Virginia Mandates Cyber Safety Education	
Kentucky Legislature Outlaws Internet Hunting	
House Committee Passes Security Breach Bill	
House Committee Frees Net From Campaign Laws	
<u>Tools You Can Use</u>	22
AMBER Alert Documents Now in Spanish	
<u>Hold The Date</u>	23
Prosecuting Child Pornography, Exploitation	

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 and Violence Against Women 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.

LAW JOURNAL ON SEARCH AND SEIZURE PUBLISHED

The National Center for Justice and the Rule of Law (NCJRL) at the University of Mississippi announced that *The Search and Seizure of Computers and Electronic Evidence* in volume 75 of the Mississippi Law Journal has been published. The Journal articles stemmed from a symposium held in conjunction with a training conference entitled *Advanced Training on Search and Seizure of Computers and Obtaining Electronic Evidence* sponsored under the partnership between the National Association of Attorneys General (NAAG) and NCJRL. That conference was held on February 15-17, 2005 and attended in person by approximately 64 prosecutors from 34 Attorneys General offices. The symposium session of the conference was attended by an additional 55 attorneys and law professors as well as another 219 people who observed the symposium on the Internet. The articles in the Journal are summarized below.

Susan Brenner, Professor at the University of Dayton School of Law, poses the question of whether the Fourth Amendment's guarantee of privacy is adaptable to a world where technology is "increasingly pervasive." In her article entitled *The Fourth Amendment in an Era of Ubiquitous*

Technology, Professor Brenner observes that the physical and informational barriers that once served to differentiate our public and private lives are rapidly being eroded by technology. She offers insights on how to adapt the concept of privacy to accommodate the challenges of the 21st century and discusses impediments to protecting personal information, including the concepts of voluntary exposure and assumption of risk.

Orin Kerr, Associate Professor at George Washington School of Law, contends in his article, *The Warrant Process in the Era of Digital Evidence*, that the legal rules regulating the search warrant process must be revised in light of the demands of digital evidence collection. He asserts that existing rules are premised on the police obtaining a warrant to enter the place to be searched and then retrieving the property named in the warrant. Professor Kerr believes that computer technologies tend to bifurcate the process into two steps: the police must first execute a physical search to seize the computer hardware and then later execute a second electronic warrant to obtain the data from the seized computer storage. He asserts that the law has failed to account for this two-stage process and offers proposed amendments to Rule 41 of the Federal Rules of Criminal Procedure to update the warrant process for the era of digital evidence.

Christopher Slobogin, Professor at the University of Florida's Fredric G. Levin College of Law, observes in his article, *Transaction Surveillance by the Government*, that important information about our lives is stored in both written and digitized records that are housed in businesses, government agencies and other institutions. He notes that there is often an understanding that the information is private and will be used or viewed by a limited number of people for circumscribed purposes. He explores what he calls "transaction surveillance" by the government, which involves accessing already-existing records, either physically or through computer databanks, and accessing the identifiers of a transaction, such as the address of an e-mail recipient. Professor Slobogin observes that transaction surveillance is subject to far less regulation than physical or communications surveillance. He argues that transaction surveillance should be subject to much more legal monitoring and proposes significantly increasing the degree of protection to the probable cause level for personal records held by public and private entities and to the reasonable suspicion level for records readily available to the public. He concludes that only the Fourth Amendment, if properly construed, can provide adequate protection.

In *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, Tom Clancy, NCJRL Director and Visiting Professor at the University of Mississippi School of Law, outlines the application of Fourth Amendment principles to the search and seizure of computers and the digital information that is stored in them. He rejects the view that unique Fourth Amendment rules are needed to regulate computer and digital evidence searches and seizures, finding that computers are but containers and the data they contain are mere forms of evidence. He states that the mere fact that an item to be searched or seized is electronic evidence does not fundamentally change the Fourth Amendment analytical structure that governs. He also rejects expansion of the private search doctrine, used by some courts to permit government agents to open data files that had not

been open during a preceding private party search and are still not a search within the meaning of the Fourth Amendment.

Finally, in *Searches of Computers of Probationers*, Marc Harrold, Counsel for National Programs at NCJRL and Visiting Professor at the University of Mississippi School of Law, discusses the Fourth Amendment framework that regulates governmental programs monitoring the computer and Internet use of persons on probation. He surveys the technological and other tools available to facilitate that monitoring and examines the Supreme Court and lower court decisions in this area. He concludes that the "special needs doctrine," developed by the Supreme Court to assess the reasonableness of regulatory and other searches, will likely serve as the basis of assessing the reasonableness of the searches of probationers' computers.

An electronic copy of the articles may be accessed on NCJRL's web site, www.ncjrl.org, under Fourth Amendment/publications/2005. You may also obtain a hard copy of the Journal by contacting Hedda Litwin, Cyber Crime Counsel at the National Association of Attorneys General, at 202-326-6022 or hlitwin@naag.org.

FORMER AG BRADY IS KEYNOTE AT INTERNET VICTIMIZATION CONFERENCE

Jane Brady, former Attorney General of Delaware and now a Delaware Superior Court Judge, was the keynote speaker at a recent symposium on "Prosecutorial Responses to Internet Victimization" attended by prosecutors from state Attorneys General offices. The symposium, developed and hosted under the collaborative partnership between the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL), was held on April 4-6, 2006 at the University of Mississippi School of Law.

The first day of the symposium focused on the attributes and dimensions of Internet victimization. Presenters included Cindy Southworth, Director of Technology for the Safe and Strategic Technology Project at the National Network to End Domestic Violence, who spoke about how technology is being used in the commission of domestic violence and stalking. Kyle Duncan, Assistant Professor of Law at the University of Mississippi School of Law discussed child pornography and its ramifications, and Alison Turkel, Chief of Training for Child Abuse Programs at the American Prosecutors Research Institute, gave attendees an understanding of adolescent cyber victims.

Day 2 was devoted to a discussion of government responses to victimization and victimization issues arising during prosecution. Mark Harrold, Counsel for National Programs at NCJRL and Hedda Litwin, Cyber Crime Counsel for NAAG, moderated panels on such topics as the decision to prosecute, preparing the case after the decision to prosecute has been made and working with corporations on case investigations. The panels included several prosecutors from Attorney General offices, including Todd Lawson, Arizona Attorneys General's office; Kelly Carter, Michigan Attorney General's office; Jean Smith Vaughn, Mississippi Attorney General's office; and Richard Hamp, Utah Attorney General's office. Other panelists included Jack Cristin, Jr., Trust and Safety Counsel for eBay, John Deerin, Director of Security for the Bank of Tampa, Mike Robinson, U.S. Anti-Piracy Director for the Motion Picture Association of America, and Tom Sadaka, of Counsel to Berger Singerman. In addition to the panels, Patrick Corbett, Associate Professor of Law at Thomas M. Cooley Law School, told prosecutors "How to Investigate and Prosecute an Internet Fraud Case Without Going Broke."

The last day of the training covered sentencing ramifications of Internet victimization. John Curran, Deputy General Counsel at Stroz Friedberg, LLC, discussed applying the sentencing guidelines to Internet victimization. Richard Downing, Senior Counsel in the

Computer Crime and Intellectual Property Section at the Department of Justice, talked about looking beyond monetary losses in sentencing computer hacking crimes. Finally, Jayne Barnard, Cutler Professor of Law at the College of William and Mary School of Law, presented creative sanctions for online investment fraud.

Proceedings of the symposium will form the basis for a special issue of the Mississippi School of Law Journal, and is expected to be published by year end 2006.

HIGH COURT APPROVES FRCP ELECTRONIC DISCOVERY AMENDMENTS

The U.S. Supreme Court approved, without comment or dissent, the entire package of proposed amendments to the Federal Rules of Civil Procedure concerning the discovery of "electronically stored information." The amendments were transmitted to the court in September 2005 after the Judicial Conference unanimously approved them. Among the new rules approved are:

Civil Rule 16: Establishes the process for the court and the parties to address issues pertaining to the disclosure and discovery of electronic information,

Civil Rule 26: Requires the parties to discuss issues relating to the disclosure and discovery of electronic information during the discovery planning conference,

Civil Rule 33: Expressly provides that an answer to an interrogatory involving review of business records should involve a search of electronically stored information,

Civil Rule 34: Distinguishes between electronically stored information and "documents," and

Civil Rule 37: Creates a “safe harbor” that protects a party from sanctions for failing to provide electronically stored information lost because of the routine operation of the party’s computer system.

The package has been transmitted to Congress and will take effect on December 1,

2006 unless Congress enacts legislation to reject, modify or defer the amendments. The complete set of amendments may be accessed on the U.S. Court’s Federal Rulemaking web site at: <http://www.uscourts.gov/rules/newrules6.html#cv0804>.



AG INITIATIVES

ATTORNEYS GENERAL FIGHTING CYBER CRIME

MULTI-STATE

Forty-nine Attorneys General sent a letter to leaders of Congress urging them to pass legislation that would combat illegal gambling and ensure that the authority to set overall Internet online gambling regulations and policy remains at the state level. Signing the letter were the Attorneys General of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Guam, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin and Wyoming.

CALIFORNIA

Attorney General Bill Lockyer, together with the Federal Trade Commission (FTC), announced that the people behind a prolific spam operation have agreed to pay \$475,000 and to refrain from illegal activity. Optin Global, Vision

Media, Qing Kuang Yang and Peonie Pui Ting Chen violated federal and state laws by sending millions of junk e-mail messages hawking mortgage loans and other products and services. Attorney General Lockyer and the FTC had sued the defendants, alleging they had used third party affiliates to send the spam, which included links to web sites operated by the defendants. The settlement ends the litigation.

CONNECTICUT

Attorney General Richard Blumenthal sent a letter to MySpace.com asking the company to: 1) provide parents with free software to block access to the site; 2) raise the minimum age for a MySpace profile from 14 to 16 years; 3) allow only users 18 years of age or older to view adult material and prevent users under 16 years of age from making their profiles public; 4) add staff and technology to filter out and remove pornography and other prohibited content; 5) banish users who repeatedly post pornography; and 6) hire an independent watchdog to report inappropriate material and sexual predators directly to the board of directors. The letter came after discussions between Attorney General Blumenthal’s office and MySpace.com executives.

FLORIDA

Attorney General Charlie Crist announced the entry of a consent judgment in his civil lawsuit against Robert Moneyhan for unlawfully soliciting relief donations intended for Hurricane Katrina victims. Moneyhan registered domain names called katrinahelp.com, katrinadonations.com, katrinarelief.com, katrinarelieffund.com and katrinacleanup.com, but did not file registration documents with the state, as required by law. Attorney General Crist sued Moneyhan, alleging that he failed to register prior to seeking donations and that the web sites misrepresented that all of the donations collected would be used for storm victims. Through quick action by Attorney General Crist's office and Internet payment service PayPal, Moneyhan did not benefit financially from the sites. He has agreed to a permanent injunction barring him from soliciting donations without registering and subject to a \$20,000 penalty for a violation. Moneyhan has donated the web site names for noncommercial use and must also pay \$10,000 for the state's investigation costs.

ILLINOIS

Attorney General Lisa Madigan set up a new Identity Theft Hotline, (866) 999-5630, with advocates specially trained to help victims repair their credit, dispute fraudulent debts and prevent future crimes. Attorney General Madigan has also assigned a team of attorneys to her Identity Theft Complaint Unit to handle legal and policy issues raised by consumer complaints. The office has also created an Identity Theft Resource Guide, describing initial steps consumers should take in responding to identity theft, how to handle specific problems and consumer legal rights. The guide is online at: www.IllinoisAttorneyGeneral.gov/consumers/hotline.html.

KANSAS

Attorney General Phill Kline presented a NetSmartz workshop, his new Internet safety program, for state lawmakers. The presentation was made in coordination with the Kansas Alliance of Boys and Girls Clubs. Last year, state lawmakers created a grant to help fund Internet safety programs.

LOUISIANA

Attorney General Charles Foti, Jr. was the featured speaker at a cyber crime workshop that provided parents with tips and tools to protect their children from online predators. The workshop featured Attorney General Foti's High-Tech Crime Unit and included a real-time chat between an alleged predator and an investigator posing as an underage juvenile.

MASSACHUSETTS

Attorney General Tom Reilly announced the arrest of six men for trading child pornography online. Attorney General Reilly's investigators used a national tracking system to identify one child shown in the videos. State police arrested Ross Ciulla, who pleaded not guilty to possession of child pornography with intent to disseminate, possession of obscene matter with intent to disseminate and possession of child pornography. Robert Rich, Joseph Jaena, Raymond Lefebvre, Steven Bianchi and Massachusetts Institute of Technology student Debashish Sircar of New York were charged with distributing child pornography. Lefebvre and Bianchi allegedly sent child pornography through online chat rooms.

MICHIGAN

Attorney General Mike Cox's investigators arrested Glen Vellner for using the Internet to attempt to accost and solicit a minor for immoral purposes and for using the Internet to

attempt to disseminate sexually explicit material to a minor. Vellner is a convicted sex offender, having pled guilty to two counts of Criminal Sexual Conduct – Second Degree stemming from his sexual assault of two young children. Vellner was arraigned and a cash bond of \$1,000,000 was ordered. As this is his third offense, he could face up to 20 years in prison for these offenses.

MINNESOTA

Attorney General Mike Hatch flew to several cities to promote identity theft legislation. The legislative package would lower the frequency that consumers are required to provide their Social Security numbers and would prohibit businesses from refusing service to customers who don't supply their numbers. Another provision would require businesses to destroy or prevent access to certain personal records, and would require banks and health care companies to disclose to their customers when the confidentiality of their personal information is breached.

MISSISSIPPI

Attorney General Jim Hood announced that Robert Swilley pled guilty to a phishing scheme for fraud in connection with electronic mail. The plea was the result of a joint investigation by Attorney General Hood's Cyber Crime Unit and the Federal Bureau of Investigation, with prosecution by the U.S. Attorney's Office for the Southern District of Mississippi. Swilley spoofed the America Online (AOL) "You've got pictures" web site and collected names and passwords that he then sold to a business, which in turn spammed consumers. He was sentenced to three years probation and ordered to pay more than \$5,000 in restitution to AOL and a fine of more than \$7,000. He must also forfeit all computer equipment used in the commission of the crime to law enforcement officials

.Note: The Editor thanks Jean Smith Vaughn, Special Assistant Attorney General in the Office of

the Attorney General of Mississippi, for this news item.

MISSOURI

Attorney General Jay Nixon jointly filed felony charges with Polk County Prosecuting Attorney Ken Ashlock against Diana Johnson of Georgia and Shante Berry of Florida for an alleged identity theft operation. The alleged victim was contacted by a computer retailer advising her that someone had used her personal information to order more than \$3,000 in merchandise from the company's web site. Three digital cameras were charged to the victim's account, which was opened in her name using her name, social security number and date of birth without her consent. Investigators from Attorney General Nixon's office learned that packages were being shipped to a residence in Georgia frequented by Johnson, who allegedly would pick them up and re-ship them to Berry in Florida. The investigation also involved the Savannah-Chatham Metropolitan and Miami Police Departments and the U.S. Postal Inspection Service.

NEBRASKA

Attorney General Jon Bruning announced that April is "Internet Safety Month" and kicked it off by talking to a group of sixth and seventh graders about how to stay safe online. Attorney General Bruning will take his message on Internet safety to schools across the state.

NEVADA

Attorney General George Chanos announced the indictment of a Nevada man as part of an international Internet child pornography ring. The arrest was the result of cooperation between Attorney General Chanos' office, Immigration and Customs Enforcement, the Secret Service and the Reno Police. Court documents suggest that 65,000 files may have been shared across the Internet using

quasi peer-to-peer software and sophisticated encryption.

NEW MEXICO

Attorney General Patricia Madrid's Internet Crimes Against Children (ICAC) Unit captured Matthew Wagner, a suspected Internet predator. The Unit received a tip from the National Center for Missing and Exploited Children (NCMEC) that America Online had discovered someone using the screen name "tumbleweed393" and with the e-mail address tumbleweed393@aol.com was in possession of an image previously identified by NCMEC as child pornography. During the investigation, Unit agents identified Wagner as the user of the AOL account and located his residence. A warrant was served on his residence, and computer equipment and storage media were seized. A forensic examination revealed numerous child pornography images. If the court accepts Wagner's plea, he could be ordered to serve up to seven and a half years and pay up to a \$25,000 fine.

NEW YORK

Attorney General Eliot Spitzer sued Gratis Internet for the selling of e-mail addresses obtained from millions of consumers despite a promise of confidentiality. The consumers thought they were simply registering to see a web site offering free iPod music players or DVD movies and video games. Gratis promised on sign up pages not to sell or rent their addresses. However, the company sold access to their e-mail information to three independent e-mail marketers, and millions of solicitations ensued.

NORTH CAROLINA

Attorney General Roy Cooper sent a letter to sheriffs and police chiefs across the state asking them to take advantage of state-sponsored classes to learn how to catch Internet predators on the

Internet. More than 60 officers are scheduled to receive the training by May 2006. The effort comes in the wake of a new law, effective December 1, 2005, that makes it a felony, rather than a misdemeanor, to proposition an undercover police officer posing as a child on the Internet.

OHIO

Attorney General Jim Petro held a town hall meeting for parents, educators and other community members to learn about ways to protect children from dangers on the Internet. Members of Attorney General Petro's Child and Elder Protection Section and Bureau of Criminal Identification and Investigation joined with the Ohio Parent-Teachers Association, Parma Police Department, City of Parma and Parma City School District to present an informational program entitled "Use Your NetSmartz." They provided examples of computer crimes against children, as well as guidance on how to prevent sexual predators and other criminals from communicating with unsuspecting children on the Internet.

PENNSYLVANIA

Attorney General Tom Corbett's Child Predator Unit arrested and charged John Briggs with attempting unlawful contact with a minor and criminal use of a communications facility. Briggs thought he was chatting with a 13-year-old girl, but his conversations were really with an undercover officer of the Unit. He was arrested when he arrived to meet the girl at a shopping center. He was being held on \$50,000 bail.

SOUTH CAROLINA

Attorney General Henry McMaster announced that Michael Reusswig was arrested after an investigation by his Internet Crimes Against Children Task Force. Reusswig was arrested by the city of Charleston Police Department, a partner on the Task Force, on charges of Criminal Solicitation

of a Minor, a felony offense punishable by up to 10 years imprisonment, and attempted criminal sexual conduct with a minor, a felony offense punishable by up to 20 years imprisonment. According to arrest warrants, Reusswig was chatting online with a person he thought to be a 13-year-old girl, but in reality, he was soliciting sex from a police department officer. He was arrested when he arrived for a meeting with the “girl.”

SOUTH DAKOTA

Attorney General Larry Long announced that Donald Freidel was sentenced to four consecutive 10-year sentences in prison following his conviction on four counts of child pornography. Freidel was previously convicted twice of molesting children. The current sentencing may amount to a life sentence since Freidel is 77 years old. The case was prosecuted by Chief Deputy Attorney General Mark Barnett and Assistant Attorney General Todd Love in cooperation with the Yankton County State’s Attorney’s Office.

TEXAS

Attorney General Greg Abbott’s Cyber Crimes investigators announced a grand jury indictment of Ron Guzman on nine counts of child pornography, including several lewd videos of children stored on his iPod, and six counts of promotion of child pornography. The investigators executed a search warrant at Guzman’s home after a tip from the National Center for Missing and Exploited Children that he was posting sexually explicit images of children online. Forensic exams of external media and his IPOD revealed several images and video of child pornography.

UTAH

Attorney General Mark Shurtleff unveiled the Identity Theft Reporting Information System *IRIS), a new web site that will be “ID Theft Central” for victims of identity theft. Victims can

file a complaint on the site, www.idtheft.utah.gov, and it will be sent to the proper law enforcement agencies. They can also follow a series of steps to help resolve problems caused by the crime. The public at large will be able to get the latest information about current scams, phishing or illegal solicitations on the site. IRIS is a collaborative effort between Attorney General Shurtleff’s office and all Utah law enforcement agencies. Funding for the project was provided by the Utah Commission on Criminal and Juvenile Justice and the Utah Bankers Association. Technical Supervisor Scott Morrill of Attorney General Shurtleff’s office is the project manager.

WASHINGTON

Attorney General Rob McKenna announced a settlement with SoftwareOnline.com, Inc. after a four-month investigation by his High-Tech Fraud Unit. The company allegedly misrepresented that its InternetShield and Registry Cleaner products were necessary to prevent attacks from malicious web sites and computer crashes, bombarded potential customers with pop-up ads and used deceptive billing practices. Under the settlement, the company admitted to multiple violations of the state Consumer Protection Act. It also agreed to pay \$400,000 in civil penalties, with \$250,000 suspended on condition of complying with the settlement; make refunds to customers who filed complaints; and pay \$40,000 in attorneys’ costs and fees. Assistant Attorney General Katherine Tassi was the lead prosecutor on the case.

WISCONSIN

Attorney General Peg Lautenschlager announced that her office will partner with NetSmartz, the national children’s online safety program, which will be provided free to state children, parents and educators. The partnership will enhance the work of Attorney General Lautenschlager’s Internet Crimes Against Children (ICAC) Task Force, which has trained more than 80 volunteers and partnered with 25 law enforcement agencies statewide.



IN THE COURTS

In Computer Intrusion Case, Computer Security Contractor May Be Considered a “Victim” as Well as Person Owning Computer

United States v. Millot, 2006 U.S. App. LEXIS 430 (8th Cir. January 9, 2006)

Click Deal Encouragement to Skip Reading Online Contract Was Deceitful and Thus Invalidated Forum Selection Clause in Contract

Scarcella v. America Online, Inc., 2005 WL 3542868 (N.Y. App. Div. 2005)

Municipality Exceeded Its Regulatory Authority Under State Law When It Denied Permits for Wireless Communications Facilities Based on Aesthetic Impact

Sprint PCS Assets, LLC v. City of La Canada Flintridge, 435 F.3d 993 (9th Cir. 2006)

A Valid Defamation Claim Takes Precedence Over Any Right to Speak Anonymously on the Internet

Klehr Harrison Harvey Branzburg & Ellers v. JPA Development Inc., 2006 Phila. Ct. Com. Pl. LEXIS 1 (2006)

Late Fee Liquidated Damages Provisions In Cable Internet Service Provider’s Standardized Service Contract Were Invalid Because They Were Not Individually Negotiated With Subscribers

Util. Consumers’ Action Network, Inc. v. AT&T Broadband of S. California, Inc., No. 06 CDOS 630 (Cal. App. 2d January 20, 2006)

E-Mail and Web Hosting Service Provider Not Civilly Liable for User-Disseminated Child Pornography

Doe v. Bates, No. 5:05CV91 (E.D. Tex. January 18, 2006)

Web Site That Posts Consumer Complaints After Embellishing Them Cannot Claim Section 230 Immunity

Hy Cite Corp. v. Badbusinessbureau.com, LLC, 2005 U.S. Dist. LEXIS 38082 (D. Ariz. Dec. 27, 2005)

Complaint Alleges Sufficient Damage and Interference to Computer System to Survive Motion to Dismiss

Kerrins v. Intermix Media, Inc., No. 2:05-cv-05408-RGK-SS (C.D. Cal. Jan. 10, 2006)

Web Site Was Provider of “Interactive Computer Service” as Defined by Communications Decency Act and Thus Was Immune From Liability for Publishing Information Provided by Third Party

Landry-Belle v. Various, Inc., No. 05-CV-01526 (W.D. La. December 27, 2005)

And see...

Web Host Service Provider, Having No Other Connection to Alleged Infringer Than Providing Web Hosting Services, Is Immune From Liability for Third Party Content Posted by Customer

Whitney Information Network, Inc. v. Verio, Inc., 2006 WL 66724 MD Fla. January 11, 2006)

Electronic Record Is Barred Absent Proof of Integrity of Computer Producing It

In re Vinhnee, 2005 WL 3609376 (BAP 9th Cir. December 16, 2005)

Search Engine's Cache Feature Constitutes Fair Use and Qualifies for the Digital Millennium Copyright Act's Safe Harbor for Online Service Providers

Field v. Google, No. CV-S-04-0413-RCJ-LRL (D. Nev. January 12, 2006)

State Consumer Fraud Action Unavailable to Non-Resident Web Site User

Shaw v. Hyatt International Corp., 2005 WL 3088438 (ND Ill. November 15, 2005)

Sex Offender Should Have Been Classified as Moderate Risk, Thus His Name and Picture Should Not Appear on Public Web Site

McCray v. Nebraska State Patrol, 270 Neb. 225, 701 NW2d 349 (2005)

No Actionable Claim Because Unsolicited Fax Advertisements Were Sent Before State Established Cause of Action

Chair King, Inc. v. GTE Mobilnet of Houston, Inc., 2006 Tex. LEXIS 97 (Tex. February 3, 2006)

Company Name in Domain of E-Mail Address Does Not Give Message Sender Authority to Contract

CSX Transportation, Inc. v. Recovery Express, Inc., No. 04-02293 (D.Mass. February 1, 2006)

Merely Advertising Products for Sale on the Internet is Not Enough to Establish Jurisdiction

ICP Solar Technologies, Inc. v. TAB Consulting, Inc., No. 05-CV-111 (D. NH January 31, 2006)

See also...

Single Unlawful E-Mail Sent to Forum is Insufficient to Support Jurisdiction
Fenn v. Mleads Enterprises, Inc., No. 20041072 (Utah February 10, 2006)

But see...

Accessing Data and Presence of E-Mail Servers in Forum Satisfied Minimum Contacts for Jurisdiction

Flowserve Corp. v. Midwest Pipe Repair, LLC, 2006 WL 265521 (ND Tex., February 3, 2006)

Internet User Lacked Fourth Amendment Privacy Interest in Personal Information Given to Internet Service Provider

In re Property of Forgione, No. CR05-1845500 (Conn. Super. Ct. January 6, 2006)

Employee Must Produce in Discovery E-Mails Allegedly Hacked by Supervisor
Rozell v. Ross-Holst, 2006 WL 163143 (SDNY January 20, 2006)

Convicted Child Pornographer's Mandatory Minimum Sentence Does Not Violate the Eighth Amendment Given the Crime's Severity

United States v. Gross, No. 05-1538 (7th Cir. February 14, 2006)

Patriot Act's Changes to Wiretap Law Authorize Gathering of E-Mail Addresses

In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Trace & Trace Device on E-Mail

Account, No. 2006-0011 (D.DC February 2, 2006)

Operator of a Web Site About Prostitution Services Lacks Clean Hands for the Court to Enter Preliminary Injunctive Relief

First Global Communications, Inc. v. Bond, 2006 WL 278566 (WD Wash., Feb. 3, 2006)

Use of USB Memory Stick and Hotmail Account to Export Pricing Data Supports Claim Under Computer Fraud and Abuse Act

HUB Group, Inc. v. Clancy, 2006 US Dist. LEXIS 2635 (ED Pa., January 26, 2006)

Lost Profits Due to Data Theft and Travel to Discuss Impact of Theft Not Covered by Computer Fraud and Abuse Act

Nexans Wires S.A. v. Sark-USA, Inc., No. 05-3820 (2d Cir. February 13, 2006)

Blogger Not Subject to Personal Jurisdiction Without Evidence of Book Sales From Web Site

Software Development and Investment of Nevada v. Wall, No. 2:05-cv-01109-RLH-LRL (D. Nev. February 13, 2006)

Service of Process by E-Mail Permitted Where Traditional Methods “Impracticable”

Tishman v. The Associated Press, (Slip Op.) 2005 WL 288369 (SDNY February 6, 2006)

Financial Institution Has No Duty to Encrypt Customer Database

Guin v. Brazos Higher Education Service Corp., Inc., No. 05-668 (D. Minn. February 7, 2006)

Inability of Net Pharmacy Defendants to “Be Confronted” By Witnesses Who Appeared Via Video Conference Violated Sixth Amendment Rights

United States v. Yates, No. 00-00109 CR-N-1 (11th Cir. February 13, 2006)

The Federal Food, Drug and Cosmetic Act Enables Courts to Order Disgorgement Against Web Site Operator That Improperly Assisted U.S. Citizens in Procuring Prescription Medicines From Canadian Pharmacies

United States v. RX Depot, Inc., No. 05-5003 (10th Cir. February 22, 2006)

Police May Search Computer Hard Drives for Child Pornography If Computer Owners “Open the Door” By Subscribing to Web Sites Selling the Images

United States v. Williamson, No. 0530150 (9th Cir. March 13, 2006)

Affidavit in Support of Search Lacked Sufficient Indicia of Probable Cause Since It Contained No Evidence That Defendant Downloaded or Possessed Child Pornography

United States v. Gourde, 2006 WL 574302 (9th Cir. March 9, 2006)

Employer’s Claims Against Employee Are Reinstated Where Employee Accessed Computer Without Authority After His Breach of Loyalty Terminated His Employment

Int’l Airport Centers, LLC v. Citrin, (Slip Op.) No. 05-1522 (7th Cir. March 8, 2006)

Communications Assistance for Law Enforcement Act (CALEA) Allows Tracking User of Another’s Cell Phone

In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register

With Caller Identification Device and Cell Site Location Authority on a Certain Cellular Phone, No. MISC:2:06 MC 00028 (SDW. Va. February 17, 2006)

Unauthorized Content “Scraping” by Competitor Web Site May Give Rise to Claim for Unjust Enrichment

ShopLocal LLC v. Cairo, Inc., (Slip. Op.) 2006 WL 495942 (N.D. Ill., February 27, 2006)

Maryland Commercial Electronic Mail Law Does Not Violate Commerce Clause

MaryCLE, LLC v. First Choice Internet, Inc., 2006 WL 1736 (Md. App. 2006)

Note: The Editor thanks Steven Sakamoto-Wengel, Deputy Chief, Consumer Protection Division, Office of the Attorney General of Maryland, for this information.

Attorney Suspended From Practice of Law for Illegal Use of E-Mail

In the Matter of Julia Ellis Brown, No. 26129 (S.C. March 27, 2006)

Note: the Editor thanks Jim Bogle, Senior Assistant Attorney General in the Office of the Attorney General of South Carolina, for alerting us to this case.

And see...

Attorney Indefinitely Suspended From Practice of Law for Misuse of “Spyware”

In re Petition for Disciplinary Action Against Kristine Katherine Trudeau, 2005 WL 3007005 (Minn. Nov. 7, 2005)

Note: The Editor thanks Linda Jensen of the Office of the Attorney General of Minnesota for alerting us to this case.

U.S. SUPREME COURT WATCH

OPINION ISSUED:

United States v. Grubbs (No. 04-1414), 377 F.3d 1072 (9th Cir. 2004)

The Court unanimously reversed the Ninth Circuit’s ruling that the Fourth Amendment requires an anticipatory search warrant to state with particularity the conditions precedent to its execution. Jeffrey Grubbs purchased a videotape containing child pornography from a web site operated by an undercover postal inspector. Prior to delivering the tape to Grubbs, the Postal Inspection Service obtained an anticipatory search warrant based upon an affidavit with a “triggering condition” stated as it would not be executed until the parcel had been received and physically taken into Grubbs’ residence. However, the affidavit was not incorporated into the warrant. Two days later, an undercover postal inspector delivered the package, which was signed for by Grubbs’ wife and taken into the residence. Grubbs was immediately detained and the warrant was executed. Grubbs admitted ordering the videotape and was arrested.

At trial, he moved to suppress the evidence seized during the search, arguing that the warrant was invalid because it did not state a “triggering condition.” The U.S. District Court for the Eastern District of California denied the motion, but the Ninth Circuit reversed, agreeing with Grubbs that the warrant was invalid because it did not specify a “triggering condition,” which the court said was necessary so that the person about to be served could “police the officers’ conduct.”

The Supreme Court unanimously reversed. In an opinion written by Justice Scalia, the Court held that an anticipatory search warrant will satisfy the Fourth Amendment if two prerequisites are satisfied: 1) there must be a fair probability that contraband or evidence of the crime will be found, and 2) there must be probable cause to believe that the “triggering condition” will occur. The Court found that both conditions had been satisfied in the instant case. As to the “triggering condition” argument, the Court stated that the Fourth Amendment specifies only two items that must be particularly described in the warrant: the place to be searched and the persons or things to be seized. As to “policing the officers’ conduct” with a “triggering condition,” the Court noted that neither the Fourth Amendment nor the Federal Rules of Criminal Procedure even require that a copy of the warrant be provided prior to the search. The individual is protected by the impartial judgment of a judicial officer and the right to suppress evidence wrongly obtained.

Justice Souter, joined by Justices Stevens and Ginsberg, filed an opinion concurring in the judgment and concurring in part with the opinion. They disagreed with the statements in the opinion that the individual has no right to obtain an accurate declaration of the government’s authority to search.

ARGUED:

eBay v. MercExchange (No. 05-0130), 401 F.3d 1323 (Fed. Cir. 2005), *argued March 29, 2006*

The dispute between eBay and MercExchange, a small Virginia patent

holding firm, began in 2001 when MercExchange sued eBay for allegedly infringing on its patent that enabled the “Buy It Now” feature used on eBay’s site. A jury in the U.S. District Court for the Eastern District of Virginia awarded MercExchange \$35 million for infringement, and the company then moved for a permanent injunction to prevent future use by eBay. Although under *Continental Paper Bag Co. v. Eastern Paper Bag Co.*, 210 US 405 (1908), there is a legal presumption in favor of an injunction against the infringer, the court denied the motion, finding that MercExchange, which licenses but does not practice its patents, would not suffer irreparable harm without an injunction. However, the U.S. Court of Appeals for the Federal Circuit disagreed, finding no justification for deviating from the *Continental Paper* rule.

eBay asked the Justices to decide whether the Federal Court erred in applying a general rule that, absent exceptional circumstances, a district court must issue a permanent injunction after a finding of infringement. The Court ordered the parties to also argue whether it should reconsider its precedents on when it is appropriate to issue an injunction in patent infringement cases. eBay contends that the Federal Circuit’s “near-automatic injunction rule” conflicts with §283 of the Patent Act which states: “The several courts having jurisdiction of cases under this title may grant injunctions in accordance with the principles of equity to prevent the violation of any right secured by patent...” eBay argues that by saying “may,” not “shall,” Congress gave the federal courts discretion to grant or deny injunctive relief. Further, they argue that if the four factor test for

issuing an injunction - irreparable injury, adequacy of remedy at law, balancing of the hardships and the public interest – had been applied, the Federal Circuit should have affirmed the district court’s denial of an injunction. MercExchange responded that denials of injunctions have generally involved a significant public interest. They argue that the Federal Circuit clearly applied equitable considerations to the facts even if it did not recite the four-part test for issuing an injunction.

CERTIORARI DENIED:

Nitke v. Gonzalez (No. 05-526), No. 01 Civ. 11476 (SDNY July 25, 2005)

The U.S. Supreme Court denied an appeal by photographer Barbara Nitke and the National Coalition for Sexual Freedom who claimed that the Communications Decency Act violated Nitke’s free speech rights to post

pictures of sadomasochistic sexual behavior on the Internet. That law requires those sending obscene communications on the Internet to take reasonable actions to keep the communications away from children, such as requiring a credit card or adult access code as proof of age. Nitke’s attorney had argued that her work is art and not obscene and is therefore protected by the First Amendment. The denial affirmed a decision last year by a special three-judge panel at the U.S. District Court for the Southern District of New York which upheld the 1996 law.



NEWS YOU CAN USE

SURVEY: NET NEUTRALITY RULES WOULD PREVENT ABUSE

More than two-thirds of respondents in a survey by three consumer groups – the Consumer Federation of America, Consumers Union and Free Press – said the large telecommunications and cable companies offering broadband services should adhere to network neutrality principles, which would guarantee that broadband users can go to any legal web sites they want and run any applications

they want. According to the survey of 1000 people, performed in the fourth quarter of 2005, 47 percent of respondents also said they believe that broadband providers will voluntarily support network neutrality principles. Additionally, 55 percent supported a national net neutrality policy, with 54 percent favoring Congressional action. Congress is supposed to consider adding net neutrality principles when it debates a telecommunications reform bill this year, but large broadband providers such as Comcast and Verizon have generally opposed the rules as unneeded

regulation, saying they have no plans to block access to sites. The survey results are available at http://www.consumerfed.org/pdfs/net_neutrality_poll.pdf.

FBI SAYS COMPUTER CRIME COSTS \$67 BILLION

Dealing with viruses, spyware and other computer crimes costs U.S. businesses \$67.2 billion a year, according to the FBI. The FBI calculated the cost by extrapolating results from a survey of 2,066 organizations, finding that 64 percent suffered a financial loss from computer security incidents over a 12-month period. The average cost per company was more than \$24,000, with the total cost reaching \$32 million for those surveyed. Responding to worms, viruses and Trojan horses was most costly, followed by computer theft, financial fraud and network intrusion. Respondents spent nearly \$12 million to deal with virus-type incidents, \$3.2 million on theft, \$2.8 million on financial fraud and \$2.7 million on network intrusions. Antivirus software is almost universally used, with 98.2 percent of respondents stating they use it. Firewalls follow in second place with 90.7 percent, and anti-spam and anti-spyware are each used by about 75 percent of respondents. Biometrics and smart cards were used by only four and seven percent of respondents, respectively. Intrusion prevention or detection systems were used by 23 percent and virtual private networks (VPNs) by 46 percent. The organizations surveyed were companies in Iowa, Nebraska, New York and Texas that were established for more than three

years, had more than five employees and had more than \$1 million in revenue.

SURVEY: GOOGLE SHOULD NOT HAND OVER USER INFORMATION

A majority of people believe that Google should not release information to the government about its users' search habits, according to a survey conducted by the Pokemon Institute, a think tank that studies privacy in businesses and government. More than one third of those surveyed said they would even stop using Google if the company did so. Pokemon used 1,017 responses to tally its results after e-mailing more than 16,000 people in a national database of Americans who have volunteered to be surveyed on a variety of issues. The survey also revealed that 89 percent of Google users believe their web searches are "kept private," while 77 percent think that Google does not capture information that identifies them. The administration has requested that Google, AOL, Yahoo and Microsoft turn over statistical data about web searches for a court case. The survey also found that 14 percent of respondents were more willing to release Internet search data if authorities are "targeting criminal activities."

MOST SPAM STILL COMES FROM U.S.

Almost one quarter of the world's spam in the last three months of 2005 was sent from computers in the United States, according to antivirus company Sophos. While the U.S. still tops the chart, these figures represent a decline in the amount of U.S.-generated

spam, which according to Sophos is due in part to the crackdown against fraudulent e-mail. The U.S. is closely followed by China with 22.3 percent, and South Korea rounds out the top three with 9.7 percent. Sophos bases its numbers on a scan of all junk mail caught by its spam traps. The remaining top 10 countries, in order of amount of spam, are France, Canada, Brazil, Spain, Austria, Taiwan, Poland, Japan and Germany.

INTERNET COALITION LAUNCHES ANTI-“BADWARE” SITE

A corporate-sponsored web site was launched by the Berkman Center at Harvard and the Oxford Internet Institute as a clearinghouse for Internet users on spyware and other malicious software. The site, <http://www.stopbadware.org>, is being underwritten by Google Inc., Sun Microsystems Inc. and Chinese computer maker Lenovo Group Ltd. The coalition, which is receiving unpaid advice from Consumer Reports WebWatch, posts reports on applications that contain viruses and worms as well as software deemed by tests to be safe. It will identify any free games, screensavers and other programs known to attach spyware or adware to its downloads. The site will also name the developers of software and malware, as well as the companies that use such platforms to run ads.

GOOGLE TO CENSOR RESULTS IN CHINA

Google rolled out a new version of its search engine using China’s web suffix “.cn.” Because of government

barriers set up to suppress information, Google’s China users previously have been blocked from using the search engine or have encountered lengthy delays in response time. To obtain the Chinese license, Google agreed to omit web content that the country’s government finds objectionable. Google will base its censorship decisions on guidance provided by the Chinese government. Neither Google’s e-mail nor blogging services will be offered in China because the company doesn’t want to risk being ordered by the government to turn over anyone’s personal information. Initially Google’s Chinese service will be limited to searching web pages and images, and the company will also provide local search results and a special edition of its news service that will be confined to government-sanctioned media.

But see...

MICROSOFT ANNOUNCES NEW BLOG CENSORSHIP POLICY

Microsoft announced a new policy for dealing with government requests to block content that violates local laws. The new policy states that the company will remove content only when it “receives a legally binding notice from the government indicating that the material violates local laws” or when the content violates MSN contract terms. When blog content is blocked due to local laws, the rest of the world will continue to have access. Microsoft will also ensure that users know why content has been blocked by notifying them that access has been limited due to government restrictions. Microsoft had been criticized after it removed an MSN

Spaces blog posted by Chinese journalist Zhao Jing.

GOVERNMENT STUDY: VOIP, VIDEO CAN BE TAXED

State and local governments may be able to tax certain aspects of Internet use under a Federal law designed to ban such fees, according to a Government Accountability Office (GAO) study commissioned by Congress to examine the Internet Tax Freedom Act. First passed in 1998 and renewed after extensive debate in 2004, the law prevents state and local governments from taxing “a service that enables users to access content, information, electronic mail or other services offered over the Internet.” However, the GAO said that services like Voice over Internet Protocol (VoIP) and video offerings by Internet service providers remain fair game for taxation under the law. At issue is the GAO’s finding that the tax ban doesn’t apply to “acquired services,” which are the actual wires, cables, fibers and other hardware used to carry Internet traffic to users. That means that theoretically an Internet service provider that leases fiber from a telecommunications company for its network could be subject to taxes. Telecommunications companies and Internet service providers, including BellSouth, America Online, Comcast and Verizon Communications sent a joint letter saying that the law itself indicated a contrary position. It should also be noted that of the eight states surveyed for the report, California, North Dakota, Texas and Virginia said they aren’t currently collecting taxes on “acquired services” anyway, and Kansas, Mississippi, Ohio and Rhode Island

stopped collecting such taxes as of November 1, 2005.

NSA ISSUES REPORT ON REMOVING SENSITIVE DATA

The National Security Agency (NSA) released “Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PDF,” a 13-page paper. Following several incidents in which sensitive data was unintentionally included in computer documents and subsequently revealed, the NSA wanted users to understand that information hidden in an electronic document can almost always be recovered. The paper also deals with the removal of metadata from documents, giving step-by-step instructions on how to strip a Microsoft Word document of confidential information and then convert it to an Adobe Systems PDF file. The paper may be accessed at <http://www.nsa.gov/snac/vtechrep/I333-TR-015R-2005.pdf>.

US CONDUCTS TEST OF INTERNET DEFENSES

The U.S. concluded “Cyber Storm,” its biggest exercise to date testing how it would respond to devastating attacks over the Internet from anti-globalization activists, hackers and bloggers. The Department of Homeland Security (DHS) coordinated the week-long exercise, with participation by more than 115 government agencies, companies and organizations. Experts depicted hackers who shut down electricity in 10 states, failures in vital systems for online banking and retail sales, infected discs

mistakenly distributed by commercial software companies and critical flaws discovered in core Internet technology. There was no impact on the real Internet, as attacks were only simulated on isolated computers. DHS promised a full report on results from the exercise by summer 2006.

DOJ LAUNCHES SURVEY OF CYBER CRIME STATS

The Department of Justice (DOJ) launched its first national survey to measure the prevalence and impact of cyber crime on U.S. businesses. Conducted by DOJ's Bureau of Justice Statistics and the Department of Homeland Security's National Cyber Security Division, the survey will estimate the number of cyber attacks and incidents of fraud and theft of information in 2005, as well as the resulting losses. It will also measure the extent of security incidents, details of the incidents, the monetary costs and other consequences of the incidents, as well as the computer security measures companies use to combat cyber crime. DOJ expects to complete the survey by year end 2006.

AOL, YAHOO TO CHARGE FEE TO BYPASS FILTERS

Yahoo Inc. and America Online Inc. (AOL), two of the biggest e-mail account providers, announced they will introduce a service charging senders a fee to route their e-mail directly to a user's mailbox without first passing through junk-mail filters. Fees will range from one quarter of a cent to one cent per e-mail, and e-mails from users of the service will bear a seal alerting

recipients that they are legitimate. Both companies filter e-mail by searching for keywords commonly contained in spam and fraudulent e-mail. AOL also strips images and web links from many messages to prevent the display of pornographic pictures and malicious web addresses. The program is being offered through Goodmail Systems, Inc. and will target banks, online retailers and other groups that send large amounts of e-mail. Companies who want to use the service must also pledge that they will only contact people who have agreed to receive their messages.

But not so fast...

COALITION FIGHTS AOL'S PLAN TO CHARGE FOR E-MAIL

A 50-member coalition of unlikely partners, including MoveOn.org, Gun Owners of America and the Association of Cancer Online Resources, have joined forces to fight America Online's (AOL's) plan to charge businesses for commercial e-mail. The group has created a web site, dearaol.com, which includes an open letter to AOL. AOL's certified mail system would require advertisers to pay two to three dollars per 1,000 messages to ensure delivery to AOL's 25.5 million subscribers. E-mail of companies on the plan comes with digital tokens recognized by AOL security defenses. Although the plan is optional, AOL and Goodmail Systems, its tech partner, say they cannot guarantee that all non-certified e-mail with web links and images would get through. AOL subscribers will still be able to block mail from certified senders by adjusting anti-spam tools on their accounts.

SYMANTEC INTERNET THREAT METER IS FREE

Symantec launched its Internet Threat Meter, a free service that will provide information on the current risk level associated with e-mail, web surfing, instant messaging and file-sharing. Available on the company's web site, www.symantec.com, the threat meter will rate online activity as low, medium or high risk. The rating is based on triggers related to malicious software, phishing and online fraud, vulnerabilities, online attacks and spam. For the indicator to move higher, there must be a notable threat increase. The Threat Meter also offers a few hints and provides links to other web pages for more detailed advice.

DEAL REACHED ON .COM PRICE HIKES

The board of the Internet Corporation for Assigned Names and Numbers (ICANN) approved, by a vote of 9-5 with one abstention, a deal under which Verisign Inc., which operates the servers for .com web sites, can raise annual fees for .com domain names by meeting specified conditions. Verisign currently sells .com addresses for six dollars (five euro) each to registrars who then sell them to the public. The deal limits Verisign's annual price increases to seven percent in four of the next six years. In two of the years, Verisign

could raise fees by the same percentage only in response to a security threat or to comply with an ICANN mandate. The deal has faced opposition from some registrars, who have complained about the price increases and the fact that, as with previous contracts, it gives Verisign the first right to renew the contract with ICANN when it expires. The deal still must be approved by the U.S. Department of Commerce.

IRS LAUNCHES MAILBOX FOR SUSPICIOUS E-MAILS

The Internal Revenue Service (IRS) established an electronic mailbox, phishing@irs.gov, for taxpayers to send information about suspicious e-mails they receive that claim to come from the IRS. Instructions on how to properly submit one of these e-mails can be found on the IRS web site, www.irs.gov, by entering the term "phishing" in the search box in the upper right hand corner and opening the article entitled "How to Protect Yourself From Suspicious E-Mails." The IRS will use the information, URLs and links in the bogus e-mails to trace the hosting web sites and alert authorities to help shut them down.

Note: The Editor thanks Esther Chavez, Director of E-Commerce Legislation, Office of the Attorney General of Texas, for this information.



PUBLICATIONS YOU CAN USE

“Status and Needs of Forensic Science Service Providers: A Report to Congress”

This report addresses the needs for forensic service providers in the crime laboratory. It recommends the creation of a national Forensic Science Commission that would discuss issues such as manpower and equipment requirements, continuing education policies, professionalism and accreditation standards and collaboration among forensic science laboratories. It is only available online at: <http://www.ojp.usdoj.gov/nij/pubs-sum/213420.htm>.

“Telephony Considerations of Voice over Internet Protocol”

This document describes how Voice over Internet Protocol (VoIP) allows voice communications to be transported digitally through a network using Internet Protocol standards. It is only available online at:

<http://www.ncjrs.gov/pdffiles1/nij/212976.pdf>.

“Identity Theft, 2004”

This bulletin presents data from the National Crime Victimization survey on identity theft victimization and its consequences. It is based on new questions about identity theft that were added to the survey in July 2004 and can be downloaded at:

<http://www.ojp.usdoj.gov/bjs/pub/pdf/it04/pdf>.

LEGISLATION UPDATE

CYBER SAFETY

Virginia Governor Tim Kaine signed into law a bill requiring all state public schools to teach students about Internet safety. The law, which takes effect on July 1, 2006, directs the Department of Education to issue guidelines to schools for integrating Internet safety into their regular curriculum.

INTERNET HUNTING

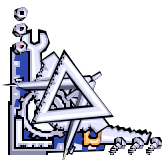
The Kentucky Legislature voted to outlaw the practice of using the Internet to fire remote-controlled rifles at live animals. Under the bill, HB 289, all Kentuckians would be banned from hunting on such sites, even if the target is in another state or country. At least ten other states have passed similar legislation. A spokesman for Governor Ernie Fletcher said the governor intends to sign the bill.

DATA BREACH DISCLOSURE

The U.S. House Energy and Commerce Committee unanimously passed legislation requiring data brokers to disclose security breaches if there is a “reasonable risk” of identity theft. H.R. 4127, the Data Accountability and Trust Act (DATA) also requires data brokers, defined as companies that sell non-customer data to non-affiliated third parties, to implement effective security safeguards to protect collected data, appoint and identify a person in the organization responsible for security and have a security policy in place that explains the “collection, use, sale, other dissemination and security” of the data they hold. In addition, data brokers must also post “conspicuous” notice on their web sites in the event of a breach. The bill directs the Federal Trade Commission (FTC) to establish “rigorous” national standards for data brokers to protect the personal information of consumers. Data brokers that experience a breach would be subject to FTC or independent audits for a period of five years after the breach. The bill now moves to the full House for vote.

ONLINE FREEDOM OF SPEECH

The Committee on House Administration of the House of Representatives unanimously approved H.R. 1606, the Online Freedom of Speech Act, which would amend campaign finance laws to free bloggers and other Internet communicators from possible regulation by the Federal Elections Commission (FEC) and give Internet publishers many of the same freedoms that newspapers and magazines enjoy. The bill, which was introduced by Representative Jeb Hensarling (R-TX), is only one sentence long and simply says that the portion of federal election law that deals with publications aimed at the general public “shall not include communications over the Internet.” It was originally brought up before the full House in November 2005, but failed to receive the necessary two-thirds majority required to pass items on the suspension calendar. The FEC is under court order to finalize rules to extend a 2002 campaign finance law to the Internet. If Congress doesn’t act, the final FEC regulations could cover everything from regulating hyperlinks to politicians’ web sites to forcing disclosure of affiliations with campaigns. Opponents of the legislation warn that the measure would allow illicit activities to take place online, such as relationships between bloggers and political candidates that are not disclosed.



TOOLS YOU CAN USE

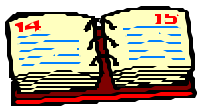
Several documents on AMBER Alert are now available in Spanish. Listed below are their names and the address where they can be accessed:

- ? “AMBER Alert: Bringing Abducted Children Home”
<http://www.ncjrs.gov/pdffiles1/ojdp/bc000716.pdf>

? “AMBER Alert Fact Sheet: Effective Use of the National Crime Information Center (NCIC)” <http://www.ncjrs.gov/pdffiles1/ojjdp/fs000309.pdf>

? “AMBER Alert: Best Practices Guide for Broadcasters and Other Media Outlets” <http://www.ncjrs.gov/pdffiles1/ojjdp/209519.pdf>

? Reference pocket card to promote recovery of missing children
<http://www.ncjrs.gov/pdffiles1/ojjdp/lt000505.pdf>



HOLD THE DATE!

Please mark your calendars for an in-depth training conference on **Investigating and Prosecuting Child Pornography and Child Exploitation Cases**, developed and sponsored by the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL). It will be held on November 14-16, 2006 at the University of Mississippi School of Law, and air or automobile travel will be reimbursed for all prosecutors from Attorney General offices. More information will be available in August 2006. Please contact Hedda Litwin, NAAG Cyber Crime Counsel, at 202-326-6022 or hlitwin@naag.org to receive conference updates.