



CYBERCRIME NEWSLETTER

News Highlights in This Issue

Computer Search and Seizure Training Held	2
Pop-Up Ads Don't Violate State Spam Law	9
New Jersey Enacts Internet Predator Law	6
LAPD Seeks More Use of Facial Recognition Software	10
Bulletin on Juvenile-Involved Pornography Published	12
Alleged File Sharers Must Be Given Notice of Rights	8
Report Finds Phishing Attacks Have Escalated	11
Ban on Internet Access Taxes Renewed	7
Law Enforcement Intelligence Guide Available	12
Supreme Court to Hear Grokster Case on March 29	2
Microsoft Launches Anti-Piracy Initiative	12
One E-Mail to State Resident is Sufficient "Contact"	9
Industry, Law Enforcement Launch Digital Phishnet	11
FDIC Study Gives ID Theft Prevention Tips	10
E-Rate Programs for School Internet Reauthorized	7

Table of Contents

Features	2
Computer Search and Seizure Training Held Supreme Court to Hear Grokster Case	
AG Initiatives	3
AG Lockyer Discusses Megan's Law Web Site Florida AG Charges Six With ID Theft AG Stumbo Proposes Internet Pharmacies Law Louisiana AG Arrests Officer With Pornography AG Cox Arrests Online Sexual Predator Montana AG Makes Offender Database Available AG Ayotte Awards Grant for Cyber Research New Jersey AG Arrests 39 for Child Pornography AG Petro Introduces Cards for ID Theft Victims Oklahoma AG Announces Plea for Auction Fraud AG Myers Indicts Online Tobacco Retailer Pennsylvania AG Sues Online Diploma Spammers AG Lynch Arrests Online Sexual Predator South Carolina AG to Prosecute First Predator AG Abbott Successfully Prosecutes Predator Utah AG Announces Joint ID Theft Task Force	
In the Courts	8
News You Can Use	9
UN Internet Governance Group Established File-Sharing Survey Targets Artists Google to Scan Books From Major Libraries FDIC Study Recommends ID Theft Prevention LAPD Seeks More Recognition Software FTC Issues Final Can Spam Rules Report: Phishing Attacks Increase Digital Phishnet Launched Survey: Blog Readership on the Rise Five Companies Compete for .Net Registry Microsoft Launches Anti-Piracy System	
Tools You Can Use	12
Intellectual Property Case Statistics Published Law Enforcement Intelligence Guide Offered Juvenile Pornography Bulletin Released	
Legislation Update	6
New Jersey Enacts Internet Predator Law No Fee Government Broadband Law Signed Supercomputing Bill Signed Into Law Senate Passes Digital Piracy Bill Internet Access Tax Ban Law Enacted E-Rate Program Reauthorized Video Voyeurism Bill Signed Into Law	

CYBER CRIME TRAINING FOCUSES ON SEARCH AND SEIZURE

By Hedda Litwin, Cyber Crime and Violence Against Women Counsel

An intense training on search and seizure of computers and obtaining electronic evidence was held on February 15-17, 2005 at the University of Mississippi School of Law. The training, developed under the partnership between the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL), was combined with NCJRL's Fourth Amendment Symposium and was offered at no cost to prosecutors from Attorney General offices. It featured sessions on Fourth Amendment applicability of computer searches, wiretapping and eavesdropping, the Electronic Communications Privacy Act, pen registers and trap and trace devices, the Privacy Protection Act, and child pornography searches. Speakers at the Symposium included Orin Kerr, associate professor of law at the George Washington School of Law and former honors attorney in the Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice; Susan Brenner, professor of law at the University of Dayton School of Law; and Christopher Slobogin, professor of law at the University of Florida College of Law. The faculty also included John Grossman, chief of the Corruption, Fraud and Computer Crime Division of the Office of the Massachusetts Attorney General; Don Colcolough, director of investigations and security at America Online; Dick Murray, assistant U.S. attorney for the Western District of Michigan; and Sherita Sullivan, forensics investigator at the Office of the Attorney General of Michigan. Patrick Corbett, professor of law at Thomas Cooley School of Law, was the keynote dinner speaker.

A basic cyber crime training for prosecutors with little or no experience in digital evidence will be given on May 3-5, 2005 under the partnership between NAAG and NCJRL at the University of Mississippi. The training is open to prosecutors from the Offices of Attorneys General, and travel expenses for the training will be reimbursed. Registration forms will be sent to all offices in March, and will be posted on NAAG's web site, www.naag.org. For additional information, please contact Hedda Litwin, Cyber Crime and Violence Against Women Counsel, at (202) 326-6022 or hlitwin@naag.org.

SUPREME COURT TO DECIDE FILE SWAPPING CASE

By Hedda Litwin, Cyber Crime and Violence Against Women Counsel

On March 29, 2005, the Supreme Court will hear arguments in *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, Docket No. 04-480, the closely followed case involving peer-to-peer (P2P) file sharing. The case pits the world's largest movie studios and music companies as plaintiffs against two comparatively small companies, Grokster and StreamCast, who produce the Grokster and Morpheus P2P file-sharing software used to send and/or receive movies and music over the Internet. The entertainment companies argue that most of the music and movies swapped by users of the Grokster and Morpheus P2P software is copyrighted, and thus the users have no distribution rights. They charge that Grokster and StreamCast are liable for the copyright infringement of their users because they either contribute to the infringement (contributory infringement) or the infringement is theirs (vicarious infringement).

In April 2003 a federal district court in Los Angeles ruled against the entertainment companies, finding that the software produced by Grokster and StreamCast had many noninfringing applications, similar to VCRs and photocopiers. That decision was affirmed by

the Ninth Circuit in August 2004, and three months later, the plaintiffs petitioned the Supreme Court. The closest Supreme Court decision is *Sony Corp. v Universal Studios* (sometimes referred to as the Sony Betamax case) of 1984, in which the Court found that sellers of VCRs were not contributorily liable for their users' copyright infringement. However, there are significant differences between the two cases. First, unlike the Sony Betamax case, the major use of the software in the *Grokster* case involves copyright infringement and is therefore illegal. Second, the stakes riding on the outcome of the *Grokster* case are much greater. If the entertainment companies win, they will be entitled to huge damage awards and injunctions, and it is probable that they will not survive. It would also have a chilling effect on the use of P2P software. However, if the entertainment companies lose, we can probably expect to see a proliferation of P2P software and providers. Or perhaps the Court will fashion a compromise that will require some oversight of its users by the P2P providers. We have but a few months to wait.



AG INITIATIVES

CALIFORNIA

Attorney General Bill Lockyer demonstrated and discussed a new Megan's Law Internet web site containing photographs, home addresses and other identifying information for 63,000 of the state's estimated 110,000 sex offenders who have registered with local law enforcement. Home addresses are listed for 33,500 of the most serious offenders.

FLORIDA

Attorney General Charlie Crist filed charges against six people accused of running an identity theft ring that robbed at least 10 victims of \$20,000. Michael Wendyger, Penny Livingston, Betty Sue Phillips, John Johnson Jr., Autumn Burdette and Gregory Bobo, all of whom have lengthy arrest records, face charges of burglary, identity theft and using or possessing the identification of another without consent. The suspects allegedly created false driver's license templates by scanning stolen licenses into a computer and making counterfeits bearing their own photographs. Several suspects even used their own mug shots posted on the Polk County Sheriff's web site.

The suspects allegedly assumed the identities of people who had mail stolen from the post office or their home mailboxes and passed fraudulent checks. The arrests and charges are the result of a nine month investigation by the Florida Department of Law Enforcement, the U.S. Postal Inspection Service and the Office of Statewide Prosecution.

KENTUCKY

Attorney General Greg Stumbo proposed legislation that would stop the unregulated distribution of pharmaceuticals through the Internet. The bill, BR 1133, incorporates best practices from other state laws, as well as recommendations from Attorney General Stumbo's Task Force on Internet Pharmacy Regulation. It now goes before the General Assembly for consideration.

LOUISIANA

Attorney General Charles Foti announced the arrest of a former police officer for possession of child pornography. Attorney General Foti's Internet Crimes Against Children Task Force worked with the Houma, South Carolina police

on the investigation. Michael Rains, a two-year veteran of the police department, had downloaded pornographic images, some of children, from the Internet. A search warrant of Rains' home computer revealed images of child pornography. Rains resigned from the police department prior to the completion of the investigation.

MICHIGAN

Attorney General Mike Cox arrested Wayne Kennedy, who used the Internet to send obscene images and arrange a sexual encounter with a 14-year-old girl persona that was actually an investigator in Attorney General Cox's office. Kennedy faces one count of Child Sexually Abusive Activity and one count of using the Internet to commit the crime of Child Sexually Abusive Activity, each a 20-year and/or \$100,000 felony; and one count of distributing obscene matter to a minor, a four-year and/or \$5,000 felony. The Ferndale, Michigan Police Department assisted Attorney General Cox's investigators on the case. Kennedy is the 23rd arrest in Attorney General Cox's new campaign to use undercover investigators to identify and prosecute child predators.

MONTANA

Attorney General Mike McGrath's Division of Criminal Investigation has made its Sexual and Violent Offender Registry (SVOR), a complete database of sexual and violent offenders, available through a new online service. The SVOR has been available free of charge via the Internet, but the new service will also allow users, especially companies that perform background checks, to download the database for a \$300 fee. Users must accept an online use agreement prior to downloading the database. The new service can be found on the state's official web site, or on www.doj.state.mt.us, the web site of Attorney General McGrath's office. It was cooperatively developed and is supported by Attorney General McGrath's office, the Information Technology Services Division of the state Department of Administration, and

Montana Interactive, a wholly owned subsidiary of eGovernment provider NIC.

NEW HAMPSHIRE

Attorney General Kelly Ayotte's office awarded a \$400,000 grant to Justiceworks at the University of New Hampshire, the new home for a nationally recognized research team from Dartmouth. Justiceworks will support the strategic plan to combat cyber crime developed by Attorney General Ayotte's office and its statewide law enforcement partners. The work will include surveying the existing investigative capabilities in the state and cataloging the expertise available.

NEW JERSEY

Attorney General Peter Harvey, together with State Police Superintendent Rick Fuentes, announced the arrest of 39 people on child pornography charges based on an investigation using new file sifting technology to detect child pornography files shared over the Internet, then traced back to the computers on which they were stored. Special Agent Flynt Waters of the Wyoming Internet Crimes Against Children (ICAC) Task Force monitored the technology. The investigation, Operation Guardian, was conducted by Attorney General Harvey's Division of Criminal Justice, State Police detectives from the Child Protection and Cyber Crime Bureau and the state ICAC task force. Those arrested included a high school hockey coach, a lawyer and a pediatric neurosurgeon.

OHIO

Attorney General Jim Petro introduced wallet-sized Theft Verification Passport cards that identity theft victims will be able to get from the state to show creditors, banks and police while trying to recover from financial losses or crimes committed by others. The cards will verify a person's identity through a photograph, fingerprint and signature. The victim must report the identity theft to police, and the crime must be confirmed. The victim then fills out an application with personal information entered

into a web site maintained by Attorney General Petro's office. The victim must also undergo a background check to receive the card. More than a dozen Greater Cincinnati police agencies have already received the software for, or information about, this new program.

OKLAHOMA

Attorney General Drew Edmondson announced that Steven Young pled guilty to six felony counts of e-Bay auction fraud under the state Consumer Protection Act. Young received a five year deferred sentence on each of the counts and was ordered to pay a \$150 judicial assessment for each count, victim compensation assessment of \$50 per count, restitution of \$16,408 and court costs. Young, who operated on the eBay site under seven different names, received payment for items he auctioned from 25 victims, but never delivered the merchandise. The case was handled by Assistant Attorney General Julie Bays.

OREGON

Attorney General Hardy Myers announced the indictment of Otamedia S.A., the largest Internet retailer of cigarettes, also doing business as Yessmokes.com, Yessmoke.com and dutyfreecig.com, on charges of racketeering, engaging in business as a cigarette distributor without a license, unlawful distribution of cigarettes, computer crime and failure to comply with tobacco delivery sales requirements by selling tobacco products to minors. Otamedia S.A. is registered in Belize and operates from Switzerland. The company accounts for more than 40 percent of the Internet cigarette business in the United States. The indictment culminates a six-month-long investigation by the Oregon Tobacco Tax Compliance Task Force, a cooperative effort between Attorney General Hardy's office, the state Department of Revenue and the State Police. State law requires all Internet distributors of tobacco products to be licensed, to pay the state cigarette tax, to notify the state Department of Revenue of the names of

cigarette purchasers and to verify that a purchaser is at least 18 years of age.

PENNSYLVANIA

The Pennsylvania Attorney General's Office sued two men for allegedly violating state law by sending out junk e-mail touting an online university that grants diplomas in 72 hours. Alton and Craig Poe are accused of conducting a "massive illegal spam campaign" that used misleading subject lines, forged e-mail addresses and random dictionary words to thwart spam filters to sell bogus academic degrees from "Trinity Southern University." The University, which is not accredited by any recognized organization and claims to be based in Dallas, advertises that its degrees require "no classes to attend – no tests to take." Doctoral degrees can be purchased online for \$599, and an "executive MBA" program costs \$499. The office is requesting an injunction against both men, as well as civil fines starting at \$1,000 for each violation of the state's consumer protection law.

RHODE ISLAND

Attorney General Patrick Lynch announced the arrest in Massachusetts of Timothy Sheldon of Rhode Island for allegedly soliciting a person he believed was under 18 years of age in an Internet chat room. The online chat was posted on a web site called Perverted Justice. The investigation was led by Special Assistant Attorney General Paul Carnes, who screened the case and filed a criminal information charge. Sheldon is the first person to be charged under the Indecent Solicitation of a Child statute that became law on August 11, 2004.

SOUTH CAROLINA

Attorney General Henry McMaster announced that Donald Brink of North Carolina would be the first person to be prosecuted for violating the state's new Child Internet Predator law, a statute that Attorney General McMaster supported. The new law, enacted in April 2004,

makes it a crime to stalk, lure or entice a child for abduction or assault. Brink was arrested on three counts of Criminal Solicitation of a Minor, a felony punishable by up to 10 years imprisonment and/or a \$5,000 fine for each count. Brink allegedly used the Internet and telephone to solicit sex from what he believed to be a 13-year-old girl, but in reality was a South Carolina Law Enforcement Division (SLED) agent. The case was developed by Attorney General McMaster's Internet Crimes Against Children (ICAC) Task Force, using the state Computer Crimes Center.

TEXAS

Attorney General Greg Abbott won a victory in the trial of Michael Kilpatrick, a former Hewlett-Packard employee, who was found guilty on three counts of Internet sex crimes to physically harm a child. Kilpatrick was sentenced to a maximum 20 years in prison and fined \$10,000. Kilpatrick attempted to meet an individual he believed to be a 13-year-old girl who he solicited for sex in an Internet chat room. The "girl" was an undercover investigator from Attorney General Abbott's Cyber Crimes Unit. Kilpatrick was arrested by Cyber Crimes officers, Hays County, Texas Sheriff's deputies

and officers from the U.S. Secret Service when he attempted to meet the "girl." Kilpatrick was charged with criminal solicitation of a minor, attempted aggravated assault of a child and attempted sexual performance by a child, all felony offenses. Assistant Attorneys General John Saba and Laura Poppo prosecuted the case.

UTAH

Attorney General Mark Shurtleff joined with the U.S. Attorney for Utah and officials from the FBI, Secret Service and Postal Inspection Service in announcing a new joint task force. The announcement coincided with 12 indictments of 25 people by a federal grand jury for identity theft charges. Part of the focus of the task force will be on educating the public about preventing identity theft, including protecting driver's licenses and checkbooks from theft and securing mailboxes. The Salt Lake City District Attorney, Utah Department of Public Safety, Salt Lake City Sheriff's office and Ogden, Utah and West Valley, Utah police departments have also signed on to the task force.



LEGISLATION UPDATE

INTERNET PREDATORS

New Jersey enacted legislation making it a crime to lure a person via the Internet into a vehicle or location with a criminal intent in mind. The bill, A-2864, was signed into law on January 18, 2005 by Acting Governor Richard Codey and became Public Law 2005, c.1. Under the new law, it is a third-degree crime to attempt "via electronic or any other means, to lure or entice a person into a motor

vehicle, structure or isolated area, or to meet or appear at any place with a purpose to commit a criminal offense with or against the person lured or enticed or against any other person." A conviction for luring under the law cannot merge with a conviction of any other criminal offense, and a court must impose separate sentences for each. In addition, a court may not suspend or make any other noncustodial disposition of any person sentenced under the law.

BROADBAND SERVICES

A telecommunications bill prohibiting a government or any entity it creates from offering broadband for a fee was signed into Pennsylvania law on November 30, 2004. HB 30 poses a hurdle for the city of Philadelphia's ambitious plan to provide broadband service throughout the city via WiFi wireless LAN access points. The project is intended to encourage economic growth and help poor residents access the Internet, but HB 30 eliminates three of the five possible business models being studied.

SUPERCOMPUTING

A bill aimed at boosting U.S. leadership in high end computing became Public Law 108-423 on November 30, 2004. The Department of Energy High-End Computing Revitalization Act, HR 4516, authorizes \$165 million over three years (\$50 million for fiscal 2005, \$55 million for fiscal 2006, and \$60 million for fiscal 2007) for the U.S. Department of Energy (DOE) to build supercomputing facilities for academic and government researchers. With this funding, DOE will research high-end computing issues, develop and buy supercomputers, establish a center to develop and maintain software, and transfer technology to the private sector.

DIGITAL PIRACY

The U.S. Senate passed S. 3021, the Family Entertainment and Copyright Act, a scaled down version of a controversial copyright bill on November 20, 2004. The measure creates stiff penalties for unauthorized reproduction of works before their official release and outlaws the use of camcorders in movie theaters. It also insulates from copyright lawsuits technologies, such as ClearPlay, that filter sexually explicit and graphic material from DVDs. In addition, the bill toughens penalties for providing false contact information when registering a web site. If a fraudulent domain name is used in

connection with credit card fraud, copyright infringement or other federal offenses, the maximum penalty would increase by seven years. Finally, the bill makes it illegal to buy or sell "authentication" devices, such as special inks and holograms, that music and software makers attach to their products to identify them as genuine. Since its passage, the bill has been held at the Senate desk, and the House has been notified of the Senate action.

INTERNET ACCESS TAXES

A bill that renews a ban on Internet access taxes became Public Law 108-435 on December 3, 2004. The original ban, in place since 1998, expired over one year ago when Congress could not agree on whether to make the ban permanent or merely extend it. The bill as passed extends the ban until 2007, as well as extends it to cover broadband service. Existing broadband taxes will be phased out.

E-RATE PROGRAM

A telecommunications bill that frees hundreds of millions of dollars in subsidies for school Internet connections through the E-Rate program became Public Law 108-494 on December 23, 2004. H.R. 5419, cleared by voice vote, resolves an accounting problem at the Federal Communications Commission which finances Internet connections in schools and libraries. The legislation prevents a potential \$12 million increase in the "universal service" fees that consumers pay on their telephone bills. To date, the E-Rate Program, created by the 1996 Telecommunications Act (PL-104-104) has distributed about eight billion dollars to schools and libraries.

VIDEO VOYEURISM

A bill that makes it a crime to surreptitiously capture images of people in situations in which they have an expectation of privacy became Public Law 108-495 on December 23, 2004. Under the Video Voyeurism Act, video

voyeurism committed on federal lands would be punishable by a fine of not more than \$100,000 or imprisonment for up to one year, or both. The new law, formerly S. 1301,

applies only in federal jurisdictions, such as federal buildings, national parks or military bases, but it carves out exceptions for law enforcement, intelligence and prison work.



IN THE COURTS

Credit Card Companies Are Not Liable When Their Cards Are Used to Buy Stolen Pornography

Perfect 10, Inc. v. Visa International, No. 04-0371 (N.D.Cal., November 15, 2004)

Internet Matchmaking Service Liable in Client's Domestic Violence Relationship Because It Should Have Told Client About Battered Spouse Waiver

Nataliya Fox v. Encounters International, No. 02-1563 (D.Md, November 18, 2004)

Use of Keystroke Logger to Spy on Employer Does Not Violate Federal Wiretap Statute

United States v. Ropp, No. 04-3000 (C.D.Cal., October 8, 2004)

Alleged File Sharers Must Be Given a Notice Explaining Their Legal Rights Before ISPs Give Their Personal Information to Music Companies.

Elektra Entertainment v. Does 1-6, No. 04-1241 (E.D.Pa., October 12, 2004)

Videotapes Sold on Internet by Police Officer That Show Him Stripping Are Not Protected by the First Amendment

City of San Diego v. Roe, 125 S. Ct. 521 (2004)

Defendant is Not Liable to Plaintiff for Tortious Interference Because It Complied With the "Notice and Takedown" Provisions of the Digital Millennium Copyright Act

Michael Rossi v. Motion Picture Association of America, No. 03-16034 (9th Cir., December 1, 2004)

Defendant's Sentence in Child Pornography Case is Vacated Where Lower Court Had Discretion to Fine or Impose Imprisonment or Both, But Was Not Made Clear at Sentencing

US v. Pabon-Cruz, No. 03-1457 (2nd Cir., December 3, 2004)

Civil Procedure Code Shifts Expense of Translating a Data Compilation Into Usable Form to Discovering Party, But Factual Issues Such as Necessity are Left to Court's Discretion

Toshiba Am. Elec. V. Superior Court of Santa Clara County, No. H027029 (Ca.App.4th, December 3, 2004)

Defendant's Conviction for Knowingly Attempting to Induce a Minor to Engage in Unlawful Sexual Activity Was Proper Where There Was Ample Evidence That Defendant Used Internet to Arrange Sexual Abuse of Children

United States v. Hornaday, No. 03-13992 (11th Cir., December 13, 2004)

Sending One E-Mail to a Resident of the State is Sufficient “Contact” to Satisfy the Long Arm Statute and the Minimum Contacts Requirement of Due Process for a Statutory Claim Based on the Sending of That E-Mail

Fenn v. Mleads Enterprises, 2004 UT App. 412 (November 12, 2004)

Online Real Estate Company Can Use Property Appraiser Records for Profit Without Paying Royalties to the Government That Created Them

Microdecisions v. Skinner, No. 03-3346 (Fla Dist. Ct. App. 2nd, December 1, 2004)

The Digital Communications Copyright Act Does Not Permit Copyright Owners to Obtain and Serve Subpoenas on ISPs to Obtain Personal Information About an ISP’s Subscribers

In Re: Charter Communications, Inc., No. 03-3802 (8th Cir., January 4, 2005)

Police Only Need Employer’s Consent, Not a Search Warrant, to Examine an Employee’s Computer for Incriminating Files

State of Washington v. Jack Leck, No. 30714 (Wash. Ct. App., December 28, 2004)

Unsolicited Pop-Up Ads Do Not Violate a State Law Regulating Unsolicited “Electronic Messages”

Riddle v. Celebrity Cruises, 2004 UT App 487 (December 30, 2004)



NEWS YOU CAN USE

UN ESTABLISHES INTERNET GOVERNANCE WORKING GROUP

The United Nations established a Working Group on Internet Governance that will organize an open dialogue and make recommendations in preparation for a decision by the World Summit on the Information Society in November 2005. The group will develop a working definition of Internet Governance, identify the relevant public policy issues, and develop a common understanding of the respective roles and responsibilities of governments, international organizations, and the private sector. Secretary-General Kofi Annan named Nitin Desai, his Special Advisor for the World Summit, as chair of the Working Group, which will have 40 members representing all regions. The Working Group’s report is expected to be submitted to the Secretary-General in July 2005.

FILE-SHARING SURVEY FOCUSES ON ARTISTS, MUSICIANS

“Artists, Musicians and the Internet,” a survey recently released by the Pew Internet and American Life Project, compares the opinions of the general public, artists and musicians, and provides a snapshot of what the people who actually produce the goods that are often downloaded think about the Internet and file sharing. The survey finds that artists are divided but not deeply concerned about online file-sharing. Only about half thought that sharing unauthorized copies of music and movies online should be illegal, but nearly two-thirds of the rest thought that file-sharing software services should be held responsible for illegal file-swapping. However, the subset of 2,755 musicians, who were recruited for the survey through e-mail notices, web site announcements and flyers distributed at musicians’ conferences, had

different views. A full 37 percent said the file-sharing services and those who use them ought to share the responsibility for illegal trades.

GOOGLE TO SCAN BOOKS FROM MAJOR LIBRARIES

Material from the New York public library, as well as the libraries at four universities – Harvard, Stanford, Michigan and Oxford – will be indexed and scanned by Google under an ambitious initiative to bring more of the world’s collective knowledge online. The Michigan and Stanford libraries are the only two so far to agree to submit all their material to Google’s scanners. The New York library will allow Google to include a small portion of its books no longer covered by copyright, while Harvard is confining its participation to 40,000 volumes so it can gauge how the process works. Oxford wants Google to scan all of its books originally published before 1901. Scanning the library books is a monumental task, since Michigan’s library alone contains seven million volumes – about 132 miles of books. Google hopes to complete indexing their library within six years. Harvard’s library is even larger with 15 million volumes. As it does with new books already included in its search engine, Google will only allow its users to view the bibliographies of copyrighted books scanned from the libraries; it will provide unrestricted access to all material in the public domain. The books scanned from libraries will be included in the same Google index that spans the web.

FDIC STUDY RECOMMENDS ID THEFT PREVENTION METHODS

“Putting an End to Account-Hijacking Identity Theft,” a study by the Federal Deposit Insurance Corporation (FDIC), gives several recommendations that underscore growing concern about Internet theft. According to the study, financial institutions’ wider adoption of electronic payment systems, as well as the increasing number of customers using these services, has produced greater opportunity for electronic fraud. The unauthorized use of personal information to break into bank accounts, known as account hijacking, is one of the fastest growing forms of electronic fraud, with the FDIC reporting that almost

two million users experienced this type of fraud in the 12 months ending in April 2004. Bank regulators recommend that banks should use more than a single password to identify on-line customers and should rely upon multiple tests. They further recommend that banks should invest in software that scans web sites for indications that they are the targets of information thieves.

LAPD SEEKS TO EXPAND USE OF FACIAL RECOGNITION SOFTWARE

The Los Angeles Police Department (LAPD) is seeking about \$500,000 from the federal government to expand the use of facial recognition technology to identify suspects. The department is currently using two computers donated by their developer, Neven Vision, which wanted field testing for its technology. The computers are still considered experimental. LAPD’s Rampart Division has used the devices about 25 times in the two months officers have been testing them. The technology has resulted in 16 arrests for alleged criminal contempt of a permanent gang injunction and three arrests on outstanding felony warrants. On one occasion, the computer was used to clear a man the officers suspected of being someone else. The city attorney has filed seven injunction cases to date involving the technology. Other experiments with the technology have had mixed results. Officials in Tampa, Florida stopped using it last year because it didn’t result in arrests. In 2002, two systems at Logan International Airport in Boston failed 96 times to identify people who volunteered to test it, but correctly identified 153 other volunteers.

FTC ISSUES FINAL CAN SPAM REGULATIONS

The Federal Trade Commission (FTC) issued its final regulations governing what law enforcement authorities will consider spam subject to the terms of the Can-Spam Act. The regulations state that bulk e-mail is commercial if it includes advertising and promotion or if the subject line or beginning of the message would be reasonably considered to be advertising or promotion. The final rules are similar to the proposed rules that were published in August 2004. They cover e-mail messages that have both

commercial and transactional (such as information about a purchase) or relationship (such as information about a product update) content. They also require companies to clearly label sexually explicit e-mails. Further information about the rules can be accessed at <http://www.ftc.gov/opa/2004/12/canspamfrn.htm>.

REPORT: PHISHING ATTACKS HAVE ESCALATED

The Anti-Phishing Working Group released a report showing that phishing attacks increased by 29 percent in November 2004, with the number of phishing sites, or fake web sites set up to fool victims into handing over personal information, reaching 1,518 that month. According to the report, 51 brands were hijacked during the month as well. Financial services were the most targeted industry, averaging 75 percent of all hijacked brands. ISPs were next, and experienced 16 percent of the total scams. The United States remained the top host country for phishing web sites, accounting for 27 percent. The report may be accessed at

<http://www.antiphishing.org/APWG%20Phishing%20Activity%20Report%20November%202004.pdf>.

INDUSTRY, LAW ENFORCEMENT LAUNCH DIGITAL PHISHNET

Digital PhishNet, a collaborative enforcement operation that unites industry leaders in technology, banking, financial services and online auctioneering with law enforcement, was launched to confront “phishing.” While other industry groups have focused on identifying phishing web sites and sharing best practices and case information, Digital PhishNet is the first group to focus on aiding criminal law enforcement and assisting in apprehending and prosecuting perpetrators. Developing supporters include America Online Inc., Digital River Inc., EarthLink Inc., Lycos Inc., Microsoft Corp., Network Solutions, VeriSign Inc., the Federal Bureau of Investigation (FBI), the Federal Trade Commission (FTC), the U.S. Secret Service and the U.S. Postal Inspection Service. Additional information about Digital Phishnet can be accessed at <http://www.digitalphisnet.org>.

SURVEY: BLOG READERSHIP ROSE IN 2004

Readership of online journals known as blogs grew significantly in 2004, with 27 percent of online adults reporting they read them, according to a survey by the Pew Internet and American Life Project. However, the percentage of Americans who write blogs grew only slightly to seven percent. According to the survey, blog creators tend to be male, affluent, well-educated and young; 70 percent have high-speed connections at home, and 82 percent have been online at least six years. Despite the attention to blogging, only 38 percent of Internet users know what a blog is. Really Simple Syndication (RSS), new software that makes blogs easier to read by regularly pulling headlines from news sites and web journals and presenting them within e-mail, is used by five percent of online Americans. The survey was based on random telephone calls with 1,861 Internet users. The RSS question was based on a smaller sample of 537 Internet users.

FIVE COMPANIES TO COMPETE FOR .NET REGISTRY

VeriSign, the current operator of the .net registry, a position that controls more than five million .net domain names and three trillion annual page views, will for the first time face competition to retain its control. VeriSign will compete against NeuLevel, which oversees the .us and .biz domains; Afilias, which runs .info; DENIC, which handles Germany’s .de domain; and Core++, a global consortium of domain registrars, registry operators, and telecommunications and networking companies. The Internet Corporation for Assigned Names and Numbers (ICANN) has closed the bidding process and is expected to name the .net’s operator in March 2005. The .net contract between VeriSign and ICANN expires on June 30, 2005. As operator, VeriSign has spent \$150 million on its Internet infrastructure, and has met such service requirements as keeping its outage time below a certain level and resolving domain names disputes. However, VeriSign and ICANN are currently embroiled in a lawsuit in which VeriSign alleges that ICANN violated its contract and antitrust laws by preventing it from adding new features, such as the controversial

Site Finder utility that redirected all misspelled or unassigned .com and .net domain names to a search page owned by VeriSign. ICANN is using an independent party to review the .net bids.

MICROSOFT LAUNCHES ANTI-PIRACY AUTHENTICATION SYSTEM

Microsoft announced Windows Genuine Advantage, an authentication system that urges users to provide proof that their Windows copy is authentic before receiving software updates, and will limit the options for security fixes on pirated copies of Windows. David Lazar, director of the effort, said that the program will become mandatory for Windows users to get all updates, including security fixes available through Microsoft's Update Web site, by mid-year

2005. However, users of pirated copies will be able to continue to get security fixes if they sign up to automatically receive updates. Users who visit the manual Windows Update site will be asked to prove that their copies are legitimate by allowing Microsoft's system to automatically run a check or by providing a product identification number. Users who have lost that number will be asked three basic questions, and if they are deemed to be acting in good faith, will be given a free replacement key. Microsoft also will begin providing discounted versions of Windows to users in China, Norway and the Czech Republic who discover they have a counterfeit version of Windows XP.

TOOLS YOU CAN USE

Intellectual Property Cases Described

"Intellectual Property Theft, 2002" (10 pages) presents statistics on both criminal and civil enforcement of Federal intellectual property laws for 1994-2002 published by the Bureau of Justice Systems (BJS). You can access the text at:

<http://www.ojp.usdoj.gov/bjs/abstract/ipt02.htm>

Law Enforcement Intelligence

"Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies" (312 pages-COPS) aims to help law enforcement agencies develop or enhance their intelligence capacity and be instrumental in fighting terrorism and other crimes while preserving hard-won community policing relationships. You can access the text at:

<http://www.cops.usdoj.gov/default.asp?Item=1404>

Juvenile-Involved Pornography

The Office of Juvenile Justice Systems (OJJDP) has released "Child Pornography: Patterns From NIBRS" (8 pp.) (NCJ 204911). The Bulletin cites data the National Incident-Based Reporting System (NIBRS) has collected from law enforcement that provide a profile of the dissemination and sale of pornography involving juveniles. You can access the full text at:

<http://www.ojjdp.ncjrs.org/publications/PubAbstract.asp?pubi=11943>

The Cybercrime Newsletter is developed under the Cybercrime 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, Cybercrime and Violence Against Women Counsel (hlitwin@naag.org, 202-326-6022), and formatted by Valarie Gibson, Project Assistant (vgibson@naag.org, 202-326-6262).

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 author 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.