



News Highlights in This Issue:

Laws to Stop Illegal Online Gambling Urged by 49 AGs	5
Major ISPs Unite to Create Database With NCMEC	17
Hawaii Legislature Approves Wiretapping Law	23
Maryland Commercial Electronic Mail Act Upheld	10
Online Child Pornography Publication Available	26
Windows to Have Free Child Monitoring Software	18
Indiana's Data Security Law Becomes Effective	24
Search Warrant Required to Get Cell Site Data	9
Supreme Court Denies Review of Yahoo! Case	16
GPS Monitoring of Predator Law Effective in Virginia	24
Pornography Subscription Provides Probable Cause	10
Reports Finds Cyber Blackmailing Attempts Increasing	21
Powerpoint Slides on Identity Theft Available	26
Use of Decoy Sufficient in Child Predator Probe	13
Pennsylvania Initiates First E-Notarization Program	21
Colorado Enacts Online Predator Legislation	24
Sponsored Links Most Likely to Contain Spyware	22
Florida Legislature Mandates AG Cyber Crime Unit	24
Subpoena of Investigated Company's Customers OK	9
Virginia Bans Web Sties Facilitating Child Pornography	24
Research Paper Outlines Why Phising Scams Work	21

Table of Contents

<u>Features:</u> Search Warrant Language for Cell Phones	2
<u>AGs Fighting Cyber Crimes</u>	
AG Suthers Attends Spring of Child Solicitation Bill	
Florida AG Announces Child Predator Sentenced	
AG Madigan's Task Force Apprehends Child Predator	
Massachusetts AG Sues Online Gun Dealers	
AG Cox Announces Arrest of Child Predator	
Mississippi AG Announces Sentencing of Child Predator	
AG Chanos Announces Arrest of Online ID Thief	
New Jersey AG Visits Schools on Internet Safety Day	
AG Madrid's ICAC Unit Arrests Child Predator	
New York AG Sues Firm for Installing Spyware	
AG Petro Unveils Internet Safety Web Page	
Pennsylvania AG's Unit Makes Child Sex Ring Arrests	
AG Myers Files AVC in Unauthorized Web Use Case	
South Carolina AG Announces Child Predator Arrest	
AG Abbott's Unit Obtains Guilty Plea From Predator	
Virginia AG Announces Child Pornography Arrest	
AG McKenna Settles First Can-Spam Suit	
<u>In the Courts</u>	9
Iowa AG's Subpoena of Customer Disk Relevant	
Employee Using Trace Remover Tools Can Be Sued	
Subpoena Required to Obtain Cell Phone Tracking Data	
Maryland Spam Law Upheld as Constitutional	
ISP Has Standing to Enforce CAN-SPAM Act	
Membership in Pornography Sites Gives Probable Cause	
Digitally Altered Pornography Clause Overbroad	
Using Internet Satisfies Interstate Commerce Element	
Arizona Law Requires Solicitation of Minor or Officer	
Use of Police Decoy Sufficient to Convict Predator	
Negligence Claim for Failure to Encrypt Dismissed	
Being Offended by Web Site Insufficient for Standing	
ISP Archiving Doesn't Give Rise to Infringement	
Using DC-Based ISP Conveyed Personal Jurisdiction	
Placing Identifying Data Online is Not Surveillance	
Financial Supporters of a Web Site Can Be Anonymous	
<u>U.S. Supreme Court Watch</u>	15
Courts Must Use Equity Test in Infringement Cases	
Cert Denied in Falwell Trademark Infringement Suit	
Court Denies Review of Yahoo! Jurisdiction Case	
<u>News You Can Use</u>	17
FTC Tells ICANN That Whois Databases Essential	
ISPs Unite to Build Database With NCMEC	
Survey: Cyber, Not Physical, Crime Greatest Threat	
Attacks on Desktop and Web Applications Rising	
Microsoft to Include Free Child Monitoring Software	
AOL to Offer Free E-Mail Options to Nonprofits	
ICANN Plans to Test Non-English Domain Names	
Spyware Watchdog Group Names Kazaa as Violator	
DC Seeks Wireless System That Gives Access to Poor	
Paper Claims Chips in RDID Tags Can Carry Virus	
Majority Wants Banks to Monitor Online Banking	
US Ranked First in Global IT Study	
Government CIOs Say Security is Top Priority	
Report: Most Americans Are Anti-Surveillance	
Researchers Tell Why Phising Scams Still Work	
Cyber Blackmail Attempts Increasing in 2006	
Pennsylvania Becomes First E-Notarization State	
Number of Americans Gambling Online Doubles	
Hate Groups Prefer Using U.S. Servers	
Sponsored Links Most Likely to Contain Spyware	
<u>Publications You Can Use</u>	23
<u>Legislation Update</u>	23
<u>Tools You Can Use</u>	26
<u>Hold The Date</u>	26

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

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

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

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

SEARCH WARRANT LANGUAGE FOR CELLULAR PHONES

**by Robert Morgester, Deputy Attorney
General, Special Crimes Unit Office of the
California Attorney General**

Cellular phones have become the virtual biographer of our daily activities. It tracks who we talk to and where we are. It will log calls, take pictures, and keep our contact list close at hand. In short, it has become an indispensable piece of evidence in a criminal investigation.

Want to know where your suspect was last Saturday? The cellular service provider can provide you with the location information of the cellular phone as it relates to the provider's network. What about the last person your victim called? Both the cellular phone and the cellular provider will keep a record of this. How about finding gang member photos associated with their gang moniker? It will be located within their cellular phones.

Information relating to a cellular phone will be found in two places –in the phone itself and in the records possessed by the cellular service provider. The following is offered to provide guidance on drafting a search warrant for the production of records maintained by the cellular provider.

The first step in obtaining records from a cellular service provider is to identify the provider. A cellular phone carrier can be queried directly to ascertain if they provide service to a known number. The North American Numbering Plan Administration also tracks the numbers that have been assigned to service providers (<http://www.nationalnanpa.com>). Since a cellular phone number may now be ported (transferred) by a consumer to another cellular service provider, law enforcement should make a number porting check. Law enforcement may sign up for the service at (<http://www.nationalpooling.com/forms/law/index.htm>).

The second step in obtaining records from a cellular service provider is a preservation request to "freeze" stored records and communications pursuant to 18 U.S.C. § 2703(f). Many cellular service providers maintain records for only a short period of time. This request can be used as a directive to third-party providers to preserve records and not disclose the investigation to the suspect. This is an important tool to use to prevent third-party providers from writing over or deleting data you need while you obtain a warrant. Currently there are no laws that govern how long a third-party provider must retain logs or other information. Sample preservation orders can be found on cdaa.org.

It is also recommended that you contact the cellular service provider to ascertain the type and nature of records kept and any special terms or definitions that the carrier uses to describe those records. Any request for records should be limited to only the records that are needed. Do not request all of the categories of records listed unless it is truly needed for your case. Cellular phone records can be described in the warrant as follows:

A) Subscriber information

Note: This should give you the name, address, phone numbers, and other personal identifying information relating to the subscriber.

B) Account comments

Note: Anytime the provider has contact with the customer or modifies the customer's account, a notation will be made by a service representative on the account.

C) Credit information

Note: Most providers run a credit report on a customer prior to activating the account.

D) Billing records

Note: Do not ask for toll information; that is a landline term for long distance. Specify period desired.

E) Outbound and inbound call detail

Note: This is the real time, current activity that is not yet on the customer's bill. "Inbound" is usually available for only a limited time (45 days).

F) Call origination / termination location

Note: Available for a limited time (45 days) and gives location information on cell sites used, length of call, date, time, numbers dialed. With a GPS enabled phone, it gives location of phone.

G) Physical address of cell sites and RF coverage map

Note: Needed to determine where cell site is located when you receive inbound & outbound or call origination & termination location. The RF coverage map models the theoretical radio frequency coverage of the towers in the system. You will want to limit this request to a specified geographical area.

H) Any other cellular telephone numbers that dial the same numbers as (xxx) xxx-xxxx

Note: If you want to know who calls the same number the target calls (for example a pager or landline number). Available for only a limited time (45 days).

I) Subscriber information on any cellular numbers that (xxx) xxx-xxxx dials

Note: Subscriber information on the carrier's network that is dialing the target.

J) All of the above records whether possessed by cellular service provider [target of warrant] or any other cellular service provider

Note: If you anticipate the suspect may be roaming or if the number is roaming in the provider's market, you may be able to obtain information from other cellular carriers if you include this language in your description of records.

K) All stored communications or files, including voice mail, email, digital images, buddy lists, and any other files associated with user accounts identified as: account(s) xxxxxx, mobile numbers (xxx) xxx-xxxx, or e-mail account roe1234@sprint.net.

Note: Cellular service providers now offer similar services to an internet service provider (ISP) and maintain the same type of records such as text messaging, e-mail, and file storage for the transfer of data including digital pictures. Limit your request to what you need.

L) All connection logs and records of user activity for each such account including:

1. Connection dates and times.
2. Disconnect dates and times.
3. Method of connection (e.g., telnet, ftp, http)
4. Data transfer volume.
5. User name associated with the connections.
6. Telephone caller identification records.
7. Any other connection information, such as the Internet Protocol address of the source of the connection.
8. Connection information for the other computer to which the user of the above-referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, and all other information related to the connection from cellular service provider.

Note: The above is a standard request made to ISP to track connection information. Remember with the type of cellular service offered today the user can send a message from the phone or from the associated account via a computer or other access device.

M) Any other records or accounts, including archived records related or associated to the above-referenced names, user names, or accounts and any data field name definitions that describe these records.

Note: This is the catch all to use when you want everything. This request also includes "archived" information. Many companies now "archive" records thus allowing for the preservation of subscriber records for a significant time. Archived records are usually stored in a spread sheet format encompassing a variety of data fields. You must request the data field name definitions in order to understand the spreadsheet.

N) PUK for SIM card # _____

Subscriber Identity Module (SIM) is a smart card inside of a GSM cellular phone that encrypts voice and data transmissions and stores data about the specific user so that the user can be identified and authenticated to the network supplying the service. The SIM also stores data such as personal phone settings specific to the user and phone numbers.

SIM cards can be password protected by the user. Even with this protection SIM cards may still be unlocked with a personal unlock key (PUK) that is available from the service provider. Note that after ten wrong PUK codes, the SIM card locks forever.

A search warrant for the production of records held by a cellular service provider should always include an order for non-disclosure. The cellular service provider will notify the customer of the search warrant unless there is a non-disclosure order. This order will delay notification for 90 days and can be extended for an additional 90 days. (See California Public Utilities Commission decision No. 93361 (7/21/1981).) A non-disclosure order may be phrased as follows:

ORDER FOR NON-DISCLOSURE OF SEARCH WARRANT

It is further ordered that cellular service provider not notify any person (including the subscriber or customer to which the materials relate) of the existence of this order for 90 days in that such a disclosure could give the subscriber an opportunity to destroy evidence, notify confederates, or flee or continue his flight from prosecution.

Now that we have listed what records we are seeking, probable cause must be shown in the affidavit for each of the listed items. The following is sample language justifying the need for the production of specified records that can be used as a starting point for drafting the search warrant affidavit:

A) Through experience and training, your affiant knows cellular service providers maintain records related to subscriber information, account registration, credit information, billing and airtime records, outbound and inbound call detail, connection time and dates, Internet routing information (Internet Protocol numbers), and message content that may assist in the identification of person(s) accessing and utilizing the account.

B) Through experience and training, your affiant knows that the cellular service provider maintains records that include cell site information and GPS location. Cell site information shows which cell site a particular cellular telephone was within at the time of the cellular phone's usage. Some model cellular phones are GPS enabled which allows the provider and user to determine the exact geographic position of the phone. Further, the cellular service provider maintains cell site maps that show the geographical location of all cell sites within its service area. Using the cell site geographical information or GPS information, officers would be able to determine the physical location of the individual using the cell phone number (xxx) xxx-xxxx, which according to corroborating sources listed above was/is in use by the suspect.

It is also recommended that you include within the affidavit the authority that allows a search warrant to be served by facsimile (fax) for the production of records maintained outside of California.

A) Your affiant is aware that cellular service provider is located within the State of _____. Pursuant to Penal Code section 1524.2 and Corporations Code section 2105 a California search warrant may be served upon them and they have requested that this warrant be served by facsimile to the attention of _____ at (xxx) xxx-xxxx.

Finally, a word of caution. If you use the cellular subscriber records to attempt to determine the physical location of an individual's position, there are a couple of questions that must be answered.

The question is call overloading. When the maximum call processing capacity of a specified cell tower is reached it may be designed to hand off calls to other cell towers. Thus, a tower that the records reflect handled a call may have off-loaded the call to another cellular tower. The cellular provider will be able to check the cellular traffic on a specified cellular tower to determine whether or not any calls were off loaded.

Second question is whether the records reflecting the placement of a specified cellular tower's directional antenna is accurate. Occasionally the cellular provider may make adjustments to the cellular towers directional antenna that are not reflected in the records. Since the physical location of an individual's position will be based upon this directional antenna, its placement should be confirmed prior to trial.



AG INITIATIVES

ATTORNEYS GENERAL FIGHTING CYBER CRIME

COLORADO

Attorney General John Suthers joined Governor Bill Owens on June 7, 2006 when the Governor signed HB 1011, which makes online child solicitation a felony. The bill was drafted by Attorney General Suthers' office and is the cornerstone of his Safe Surfing Initiative.

FLORIDA

Attorney General Charlie Crist announced that Daniel Zankman received the maximum sentence of 15 years in prison following his conviction for lewd and lascivious battery on a child under 16 years of age. A joint investigation by Attorney General Crist's Office of Statewide Prosecution, the Polk County Sheriff's Office and the Orange County Sheriff's Office found that Zankman seduced a 14-year-old girl that he met on the Internet. Investigators then posed as a second 14-year-old girl whom Zankman tried to seduce, telling the "girl" details of his encounter with the first girl in order to establish his experience with girls her age. Authorities then executed a search warrant on Zankman's home and found numerous child pornography images, resulting in additional charges still pending. The case was prosecuted by the Office of Statewide Prosecution and the Ninth Circuit State Attorney's Office.

ILLINOIS

Attorney General Lisa Madigan's Internet Crimes Against Children (ICAC) task force assisted the Winfield Police Department in apprehending William Murphy, who allegedly traveled to a park to have sex with a minor after meeting her online in a chat room. Murphy was charged with one count

of Indecent Solicitation of a Child, a Class three felony, punishable by a maximum of five years in the state Department of Corrections. Following the arrest, the ICAC task force and the Winfield police executed a search warrant at Murphy's home and seized his computer.

MASSACHUSETTS

Attorney General Tom Reilly sued three Internet dealers, accusing them of selling stun guns, which are prohibited in Massachusetts. The dealers, Personal Protection Outlet of North Port, Florida; Unique Wholesale, Inc. of Kissimmee, Florida; and We Care Company of Coppell, Texas sold their products through auction site eBay. As a result of the suit, eBay implemented more extensive warnings to sellers and buyers of stun guns, and will void auctions where the seller is in Massachusetts.

MICHIGAN

Attorney General Mike Cox announced that Scott Dykstra was arrested for using the Internet to attempt to accost and solicit a minor for immoral purposes. Dykstra was charged with four counts of using a computer to commit this crime, which is a 10-year felony.

MISSISSIPPI

Attorney General Jim Hood announced that Paul Valentine, a former church youth minister, will serve 20 years in prison after pleading guilty to two counts of sexual battery and touching a teenager for lustful purposes by a person in a position of trust. Attorney General Hood's cyber crimes unit strengthened the case against Valentine by gathering the e-mail dialogues between Valentine and the child, which began one year before any sexual encounters occurred.

NEVADA

Attorney General George Chanos announced that Monesha Carter was arrested on charges of theft and identity theft in connection with the fraudulent sale of items via the Internet. An investigation by Attorney General Chanos' Bureau of Consumer Protection found that Carter allegedly obtained money from purchasers responding to her advertisements on the Internet that offered items for sale. The victims sent money to Carter and received nothing in return. The state alleges that Carter defrauded her victims out of \$3,379. Carter is also charged with one count of felony Identity Theft.

NEW JERSEY

Attorney General Zulima V. Farber joined Acting Education Commissioner Lucille E. Davy in visiting several schools on Internet Safety Day to help draw attention to the risks posed to young people on the Internet and to offer tips to students, teachers and parents on safe use of the Internet.

NEW MEXICO

Attorney General Patricia Madrid's Internet Crimes Against Children (ICAC) Unit arrested Jeramie Dante, who is charged with one count of fourth degree Child Solicitation by Computer. An ICAC agent posing as a 12-year-old girl received a series of sexually explicit messages during an online chat on the Yahoo! Instant messaging service from Dante using the screen name of "wiccanprince1982." Dante disclosed his age and the area where he lived and sent photographs of himself. When Dante failed to keep scheduled appointments with the "girl," ICAC agents confirmed his identity and address by matching the photographs he sent to motor vehicle records. Special agents from the ICAC Unit served a search warrant on his home where they were able to match items in his apartment to items in the photographs he sent. He was arrested, taken into custody and is being held on \$50,000 bond.

NEW YORK

Attorney General Eliot Spitzer sued Direct Revenue LLC, an Internet pop-up advertising company, accusing the firm of secretly installing malicious programs on personal computers and sending ads through "spyware" that is already installed. The civil lawsuit alleges that Direct Revenue or its distributors offered free games, browsers or software without mentioning that they would come with VX2, Aurora, OfferOptimizer and other adware downloads that thwarted consumers' removal attempts and often reinstalled themselves.

OHIO

Attorney General Jim Petro unveiled a new "Internet Safety and Cyber Predator" page on his web site to help parents and educators learn what they can do to protect children from Internet safety threats. The page includes tips and detailed advice, as well as a resource page with links to tools such as i-SAFE and NetSmartz.

PENNSYLVANIA

Attorney General Tom Corbett's Child Predator Unit arrested Donald Unkefer, Brian Gostic, Brian Nolt and Bradley Doyle during an Internet "child sex sting" operation. In separate incidents, each man used Yahoo.com chat rooms to contact and sexually proposition an undercover agent from the Unit. The agent was using the undercover online identity of a minor-aged girl.

OREGON

Attorney General Hardy Myers filed an Assurance of Voluntary Compliance with westcoastwagers.net over the site's unauthorized use of the Oregon Food Bank's name in text message solicitations. The messages claimed a \$5 contribution would be made to the Oregon Food Bank for each new player to register with westcoastwagers.net. Domain name owner Iosif Skorohodov paid Attorney General Myer's office \$5,000 in restitution and investigative costs and

agreed to abide by Oregon laws governing charitable solicitations in the future.

SOUTH CAROLINA

Attorney General Henry McMaster announced that agents of the State Law Enforcement Division (SLED) arrested Bradley Coen for Criminal Solicitation of a Minor, a felony offense punishable by up to 10 years imprisonment. SLED is a member of Attorney General McMaster's Internet Crimes Against Children Task Force. According to the arrest warrant, Coen solicited sex over the Internet from a person he believed to be a 14-year-old girl but who in reality was a SLED agent. A search warrant executed at Coen's home resulted in the seizure of a computer and related items. His bond has been set at \$100,000. Members of the U.S. Secret Service, the FBI, the Lexington County Sheriff's Office and the West Columbia Police Department took part in the operation. Attorney General McMaster's office will prosecute the case.

TEXAS

Attorney General Greg Abbott's Cyber Crimes Unit obtained a guilty plea and a three-year prison sentence for Rodney Harris, a former restaurant manager, who attempted to meet a child for sex. Harris pled guilty to online solicitation of a minor, a third degree felony that carries a possible punishment of two to 20 years in state prison and a fine of up to \$10,000. He will also be required to register with the state as a sex offender. Prosecutors from Attorney General Abbott's office assisted Gregg County District Attorney Bill Jennings in the case. Harris was arrested after he arranged a meeting for sex with a person who he thought was a 13-year-old girl but actually was an undercover investigator for Attorney General Abbott's Unit. His arrest was part of an undercover sweep of two counties by Unit investigators.

VIRGINIA

Attorney General Bob McDonnell announced the arrest of Thomas Taveggia for violations of his suspended sentence for 10 counts of reproducing child pornography. The court suspended his sentence on the condition that he not "access a computer with Internet access." Attorney General McDonnell's Computer Crime Unit filed a motion to revoke his suspended sentence, alleging that he accessed a computer with Internet access and viewed pornography on that same computer. The Richmond Police Department and Richmond City Sheriff's Office participated in the arrest.

WASHINGTON

Attorney General Rob McKenna announced a settlement with the owners of two California companies in the state's first anti-spam lawsuit filed under a 2004 federal law. The suit against AvTech Direct, a marketing firm, charged the company with sending more than 1,500 unsolicited e-mail messages marketing desktop computers to Seattle Public Schools employees. AvTech, which also operates under the name Educational Publishing Services, advertised the computers for MD&I, which then assembled and shipped them to consumers. AvTech owner Gary Hunziker agreed to pay \$500,000 in civil penalties and \$10,000 in restitution to the School District. Arlene Sediqzad, an AvTech manager, also agreed to pay \$10,000 in attorney's costs, as well as a judgment of \$180,000 that was suspended on condition that she comply with the terms of the settlement. MD&I and its owner, Min Hui Zhao agreed to pay \$10,000 to resolve claims.



IN THE COURTS

SEARCH AND SEIZURE: INVESTIGATIVE SUBPOENAS

State of Iowa v. dotNow.com, Inc., No. 5-977/04-0708 (Iowa Ct. App. March 1, 2006). In an unpublished opinion, the court affirmed a district court ruling granting the Attorney General's application for an order enforcing an investigative subpoena issued pursuant to the state Consumer Fraud Act. The defendant ISP had argued that the state unreasonably sought a disk containing its customers in order to run its own randomization program and "go fishing," but the state contended that identifying customers who have had contact with an investigated business is key to an investigative inquiry. The court agreed with the state, finding that the randomness of a sampling of dotNow customers was relevant to the investigation.

COMPUTER FRAUD AND ABUSE ACT: FILE DELETION

International Airports Centers v. Citrin, 440 F.3d 418 (7th Cir. 2006). In one of the few appellate interpretations of the Computer Fraud and Abuse Act, the 7th Circuit reversed the district court and adopted an expansive view of the law by applying it to employees' use of trace remover tools on the laptops assigned to them by their employers. In a unanimous ruling, the court held that an employee of a company who is provided a laptop computer by that company, and who uses a trace remover tool on that laptop, may be sued civilly, or prosecuted criminally, for that act, even

if there is no employment contract or company policy that prohibits the use of trace remover programs. Citrin, an employee of IAC who decided to leave the company, deleted files on his company laptop and then used a special program to scrub the files, rendering them impossible to recover. The company sued under the anti-hacking statute, but the district court dismissed the case, holding that deleting material from a computer did not constitute "transmission" under the law.

FOURTH AMENDMENT: CELL PHONE TRACKING

In re Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information, 2006 WL 41229 (D.D.C. 2006). The magistrate denied an application by the U.S. Attorney's office for an order authorizing a cellular telephone company to provide "cell-site data" revealing the location of a suspected narcotics trafficker when his phone was turned on. Since no statute directly addresses the standards for a court's issuance of such an order, prosecutors argued that the court had authority through a combination of the pen register statute, which governs the ability to obtain the numbers dialed from a telephone, and the Stored Communications Act, which permits the government to obtain computerized records from the provider about a telephone's usage, including subscriber information. They contended that location information did not constitute the content of a communication, which

by statute would require a warrant, but was equivalent to identifying information, analogous to telephone numbers and subscriber information. The court did not buy the analogy, finding that existing statutes did not cover locating information, and therefore the government would have to obtain a search warrant and demonstrate probable cause before locating a target through cellular telephone signals.

SPAM LAWS: DORMANT COMMERCE CLAUSE

Beyond Systems, Inc. v. Keynetics, Inc., 2006 WL 687156 (D. Md. 2006). The district court upheld the Maryland Commercial Electronic Mail Act. The statute was challenged by Beyond Systems, an out-of-state advertising network, which argued that the statute violated the dormant commerce clause of the U.S. Constitution. Plaintiff Keynetics was an ISP who sued web site operators claiming they were generating unsolicited commercial e-mails in violation of the Maryland Anti-Spam statute. The court held that the benefits to ISPs and users in reducing strains on systems and irritation from clutter created by unwanted messages clearly outweighed any burdens on interstate commerce, and that in enacting the CAN-SPAM, Congress expressly accorded states the right to regulate false and misleading e-mail transmissions. The court relied on *Washington v. Heckel*, 24 P.3d 404 (Wash. 2001), in which the Washington Supreme Court upheld that state's nearly identical anti-spam statute against a dormant commerce clause challenge.

CAN-SPAM ACT: STANDING AND KNOWLEDGE

Hypertouch, Inc. v. Kennedy-Western University, No. 3:04-cv-05203-SI (N.D. Cal. March 8, 2006). The district court granted summary judgment on behalf of Kennedy-Western (KWU), an unaccredited online educational institution, in a lawsuit brought by Hypertouch, a small California ISP and frequent CAN-SPAM plaintiff, which claimed that e-mails promoting KWU violated the CAN-SPAM Act. The first issue was whether Hypertouch qualified as an "Internet access provider" to have standing to privately enforce CAN-SPAM. The court found that Hypertouch qualified because it maintains its own e-mail servers and provides accounts to users, even though those accounts are free of charge. Additionally, since KWU had argued that the e-mails were sent by third party e-mail marketers and that KWU didn't know they were spamming, the second issue was whether KWU had the requisite scienter to be liable. Although Hypertouch had argued that KWU directly monitored the e-mail campaign, the court accepted KWU's argument denying knowledge of the spamming.

SEARCH AND SEIZURE: PROBABLE CAUSE

U.S. v. Gourde, No. 03-30262 (9th Cir. March 9, 2006). An en banc panel concluded that police officers may search computer hard drives for child pornography if the computer owners subscribe to web sites selling those images. FBI agents became aware of "Lolitagurls.com," a web site selling Internet access to child pornography, with credit card payment to be made through a company called Lancelot

Security. Agents subpoenaed Lancelot's records and learned that Micah Gourde was an active member. An agent then obtained a warrant to search Gourde's residence and computer for child pornography. The affidavit alleged that Gourde was a collector of child pornography based upon his membership in a subscription-only web site that featured child pornography. It further explained that, according to the FBI's Behavioral Analysis Unit, most collectors of child pornography rarely dispose of their collections, and even if Gourde had "deleted" some files, they were not actually erased but kept in "slack space" until randomly overwritten. Agents executed the warrant and found more than 100 images of child pornography on Gourde's computer. Gourde contended that the warrant was invalid because the affidavit failed to show that he had actually downloaded or possessed child pornography. However, the court ruled the circumstantial evidence satisfied the test for probable cause because it demonstrated a "fair probability" that child pornography would be found on Gourde's computer.

**PROTECT ACT: DIGITALLY
ALTERED CHILD
PORNOGRAPHY**

U.S. v. Michael Williams, No. 04-15128 (11th Cir. April 6, 2006). An 11th Circuit panel unanimously struck down as too broad or vague part of the PROTECT Act, a federal law prohibiting the offering or advertising of material presented as child pornography. The section that the court struck down was Section 2252A(a)(3)(B), which expands child pornography to include images that are not necessarily sexual images of children but either are innocuous images

of children or digitally altered images of adults to make them look like children. As part of an undercover operation aimed at combating online child exploitation, Secret Service Agent Timothy Devine entered an Internet "chat" room and engaged Williams in a private Internet chat, during which Williams sent Devine a computer hyperlink containing child pornography. Agents subsequently executed a search warrant of Williams' home, finding child pornography on the computer hard drives. Williams was charged with one count of promoting or "pandering" material intended to cause another to believe it contains child pornography, as well as one count of possession of child pornography. Williams filed a motion to dismiss the pandering charge on the grounds that this provision of the PROTECT Act was unconstitutionally overbroad and vague. While the motion was pending, a plea agreement was reached whereby Williams would plead guilty to both counts but reserve his right to appeal the pandering charge. He was sentenced to sixty months' imprisonment for each charge to be served concurrently. The appeals court found that the pandering provision abridges the freedom to engage in a substantial amount of lawful speech and was thus unconstitutionally overbroad. It also found that the provision failed to outline its restrictions with sufficient clarity to enable compliance. Williams' sentence on the pandering count was reversed. The court's ruling also rendered that provision of the PROTECT Act unenforceable in the 11th Circuit, which covers Florida, Georgia and Alabama.

**CHILD PORNOGRAPHY:
STATUTORY CONSTRUCTION**

U.S. v. MacEwan, No. 05-1421 (3rd Cir. April 5, 2006). The Third Circuit found that the use of the Internet satisfies the interstate commerce element of the federal law prohibiting the receipt of child pornography, 18 U.S.C. §2252A(a)(2)(B). MacEwan was charged with three counts of receiving material containing child pornography in violation of the above statute, two of which involved the Internet. MacEwan pled guilty to the count that did not involve the Internet and went to trial on the remaining counts. At trial, although admitting that he downloaded pornographic images, he argued that the government could not establish that, in compliance with the interstate commerce jurisdictional element of the statute, there was an interstate transmission of the pornographic images. He contended that the images could have traveled interstate and thus were beyond the reach of Congress under the Commerce Clause. MacEwan was acquitted of one count on different grounds and found guilty on the other. On appeal, the Third Circuit affirmed MacEwan's conviction on two counts of violating 18 U.S.C. §2252A(a)(2)(B). The court concluded that the Internet is "a channel and instrumentality of interstate commerce" and that Congress can regulate the downloading of child pornography under §2252A(a)(2)(B), even if the transmission never crossed state lines. Because the defendant had admitted that he downloaded images from the Internet, there was sufficient evidence for the trier of fact to find the interstate-commerce-jurisdiction element under the statute.

**ONLINE CHILD ENTICEMENT:
REPORTER POSING AS MINOR**

Mejak v. State, No. CV-05-0299-PR (Ariz. May 24, 2006). The Arizona Supreme Court unanimously decided that state law requires a person charged with the crime of soliciting sex from a juvenile to have solicited either a juvenile or a police officer. Television reporter Lisa Fletcher, pretending to be a 13-year-old girl, engaged in an online conversation in a chat room with Jeremy Mejak of New York as part of a news investigation to show how the Internet can be used to solicit minors for sex. Mejak, believing her to be a teen, set up a meeting to have sex with her and was instead met by video cameras. Phoenix police subpoenaed the video tapes and Fletcher's laptop, and the county attorney took the case to the grand jury, securing an indictment on a charge of luring a minor for sexual exploitation. Mejak pled guilty and was sentenced to lifetime probation to be served in New York. However, the New York state probation system would not accept the terms of the probation, and the plea agreement was set aside. Mejak filed a motion to dismiss, which was denied by the trial court. He appealed, first to the Arizona Court of Appeals and then to the state Supreme Court. Prosecutors argued it was sufficient that Mejak believed the person solicited was a minor, but Mejak successfully argued that no minor was involved and the supposed juvenile was a reporter, not a police officer.

**ONLINE CHILD ENTICEMENT:
USE OF GOVERNMENT DECOY**

U.S. v. Tykarsky, No. 04-4092 (3rd Circ. May 10, 2006). The court determined that when a government agent poses as a

minor online in an attempt to catch offenders who participate in “actual or attempted persuasion of a minor to engage in illicit sexual activity” (18 U.S.C. § 2422(b)) or in “traveling for the purpose of engaging in illicit sexual activity (18 U.S.C. § 2423(b)), involvement of a minor is unnecessary, so long as the offender believes the victim to be a minor. Tykarsky engaged in explicit sexual discussions with a government decoy through Internet chat rooms and instant messaging, requesting pictures and setting up a sexual encounter with the undercover agent, who posed as a 14-year-old girl. When Tykarsky arrived at the planned meeting, he was arrested and later convicted. On appeal, Tykarsky argued that he could not be convicted of either statute because no minor was involved. The court, looking at legislative intent in § 2422(b), determined that the inclusion of the “attempt” provision indicated that the involvement of a minor was unnecessary. The court reached the same conclusion regarding § 2423(b), but based its decision on the plain language of the statute, noting that involvement of a minor was not an element. Consequently, the court affirmed Tykarsky’s convictions; however, his sentence was vacated due to an ex post facto error.

DATA SECURITY: NEGLIGENCE

Forbes v. Wells Fargo Bank, N.A., No. 05-2409 (D.Minn. March 13, 2006). The district court granted the bank’s motion for summary judgment because plaintiffs failed to show damages supporting their negligence claim arising from the bank’s alleged failure to encrypt customer’s personal data. Computers loaded with unencrypted customer information were stolen from a

third party hired by the bank to print mortgage statements. Two customers whose information was on the stolen computers filed suit, alleging breach of contract, breach of fiduciary duty and negligence. To date there had been no indication that the stolen information had been accessed or misused. The court found no present injury or reasonably certain future injury.

ESTABLISHMENT CLAUSE: STANDING

Caldwell v. Caldwell, No. C 05-4166 (ND Cal. March 13, 2006). The court granted defendant’s motion to dismiss, finding that being “offended” by a web site is insufficient to give rise to injury for purposes of standing. Plaintiff had sued two University of California officials, alleging that a web site maintained by the University’s Museum of Paleontology includes statements that show the University’s preference for religions whose views do not conflict with evolution, in violation of the First Amendment’s Establishment Clause. Thus, the court did not reach the merits of the Establishment Cause claim.

COPYRIGHT INFRINGEMENT: ISP ARCHIVING

Parker v. Google, Inc., 2006 WL 680916, (ED Pa., March 10, 2006). The court dismissed a lawsuit filed by a writer who claimed the search engine infringed upon his copyright by automatically archiving his posting on USENET and providing excerpts from his web site in their search results. The court disagreed, finding that under case law, Google’s activities are akin to an ISP, and when an ISP automatically and temporarily stores data so that the system can operate and transmit data to

its users, the necessary element of volition is absent.

COPYRIGHT INFRINGEMENT:
PERSONAL JURISDICTION

Virgin Records America, Inc. v. Does 1-35, Slip Copy, 2006 WL 1028956 (D.D.C. April 18, 2006). The district court ruled that it had personal jurisdiction over an out-of-state file sharer because the defendant offered sound recordings to the public and was able to download recordings made available by others. Virgin Records America sued 35 John Doe defendants for copyright infringement relating to music traded over P2P networks. Defendant #18, who was identified by his ISP Verizon, filed a motion to dismiss the case for lack of personal jurisdiction, arguing he did not have sufficient contacts with the District of Columbia. The court held that, by simply contracting with Verizon, a “District of Columbia-based ISP,” and using a Verizon facility to trade files, defendant #18 was “transacting business” in the District.

FREEDOM OF SPEECH:
INTERNET POSTINGS

Trummel v. Mitchell, 131 P. 3d 305 (Wash. March 30, 2006). The state Supreme Court reversed the appeals court, finding that the trial court’s order prohibiting Trummel from posting information on his web site was invalid. Paul Trummel began feuding with Council House, the low-income residence where he lived. He posted his complaints on his web site, as well as the names and home addresses and phone numbers of the administrators. Trummel petitioned the trial court for an anti-harassment order against Stephen

Mitchell, Council’s administrator, which was denied, and a cross-petition was filed. A series of orders and contempt orders ensued, with the trial court finding that Trummel’s continual posting of activities at Council House constituted “surveillance,” and Trummel was restricted from posting the information about Council House personnel on the Internet. Trummel appealed, claiming that his Internet activity was constitutionally protected. The appeals court upheld the order, but the state high court found that the trial court abused its discretion because the term “surveillance” is not broad enough to encompass the activity of placing identifying information under the facts of the case.

FREEDOM TO ASSOCIATE: WEB
SITE FINANCIAL DISCLOSURE

Matthews v. City of Maitland, 2006 WL 733966 (Fla. App. 5 Dist. March 24, 2006). The appeals court reversed a trial court order and found that financial supporters of a web site are entitled to remain anonymous. Michael and Joan Matthews believed that the city of Maitland did not follow proper procedures when it approved the development of a high rise structure. They filed a lawsuit challenging the development, and started a web site through which supporters could donate funds. During discovery, neither Michael nor Joan would disclose the names of contributors to the site. The city filed a motion to compel them to turn over the names, which was granted by the trial court. The appellate court, however, noted the chilling effect that could occur if supporters of political causes who wished to remain anonymous risked being revealed in litigation, particularly in the instant case,

where the names of supporters were not relevant to the underlying dispute. Citing the Supreme Court decision in *NAACP v. Alabama*, 357 U.S. 449 (1959) which held that the NAACP did not have to disclose the names of its members because to do so would violate the members' right to freedom of assembly, the appeals court found on similar grounds that supporters of the litigation against the city could remain anonymous.

U.S. SUPREME COURT WATCH

OPINION ISSUED:

eBay, Inc. v. MercExchange, LLC, No. 05-130 (May 15, 2006)

The Court unanimously held that when deciding whether to grant a permanent injunction in a patent infringement case, courts must utilize the four-part test traditionally applied by courts of equity to evaluate the appropriateness of injunctive relief generally. Petitioners eBay and Half.com operate Internet web sites whereby private sellers can sell merchandise by auction or at a fixed price. MercExchange, a patent holding company, holds a patent for a "buy-it-now" feature that would facilitate the online sale of goods. After unsuccessful attempts to license its patent to eBay and Half.com, MercExchange filed suit in the U.S. District Court for the Eastern District of Virginia, alleging patent infringement. A jury found that MercExchange had a valid patent and that eBay and Half.com had infringed the patent. The jury awarded damages, and MercExchange then moved for permanent injunctive relief, which the court denied. The Federal Circuit reversed, using the "general rule"

binding courts to issue permanent injunctions against patent infringement "absent exceptional circumstances."

The Supreme Court reversed. In an opinion written by Justice Clarence Thomas, the Court noted that injunctive relief is equitable in nature and that the historical four-factor test for granting an injunction requires a showing that (1) the moving party has suffered an irreparable injury; (2) remedies available at law are inadequate to compensate for that injury; (3) considering the balance of hardships between the parties, a remedy in equity is warranted; and (4) the public interest would not be disserved by a permanent injunction. The Court concluded that those principles also apply to patent infringement cases, and the district court must determine whether to grant or deny relief.

According to the Court, both the district court and the Federal Circuit failed to correctly apply those principles. The district court erred in finding that a plaintiff who was willing to license its patents, but did not use its own patents commercially, was not entitled to injunctive relief. The Federal Circuit erred in granting injunctive relief in all cases where infringement was a factor. The Court did not decide whether MercExchange was entitled to an injunction, but remanded the case to the district court to apply the four factor test.

CERTIORARI DENIED:

Lamparello v. Falwell, No. 04-2011 (4th Cir. August 24, 2005)

The Court denied without comment to hear a dispute over a web site criticizing televangelist Jerry Falwell

for his anti-gay views. Christopher Lamparello, identified in the pleadings as a gay man in his 30s, registered Falwell.com in 1999 to show his aversion to Falwell's stance. After several years of demanding in writing that Lamparello take the site down, Falwell, who operated the site falwell.com, filed suit in U.S. District Court for the Eastern District of Virginia claiming trademark infringement. That court ruled in favor of Falwell, barring Lamparello from using the intentionally misspelled site and ordering him to transfer it to Falwell. On appeal, a three-judge panel of the Fourth Circuit reversed, finding that Lamparello's site was completely different from that of Falwell's and did not create enough "likelihood of confusion" to give rise to trademark infringement.

Yanaki v. Parr, Waddoups, Brown, Gee & Loveless, No. 05-940 (10th Cir., July 26, 2005)

The Court declined to review the Tenth Circuit's opinion that an employer did not act "under color of law" and thus did not violate the Constitution when it obtained an order to search a former employee's home and computer. Iomed, Inc. filed a complaint in Utah state court against Yanaki, a former employee, alleging misappropriation of trade secrets and breach of a confidentiality agreement. Iomed obtained an ex parte order directing local police to execute a search warrant of Yanaki's home and seize all hard drives and electronic storage media. Yanaki filed a civil rights suit in the U.S. District Court for the District of Utah under 42 U.S.C. § 1983, alleging that the search violated his Fourth Amendment right to be free from unreasonable search and seizure and his procedural and substantive due

process rights under the Fifth and Fourteenth Amendments. The court granted the defendant's motion to dismiss, concluding that Yanaki's pleadings did not support the element of state action required in a § 1983 claim. On appeal, the Tenth Circuit affirmed, finding that the plaintiff did not meet the "color of law" test because the conduct complained of could only be attributed to private defendants.

La Ligue Contre Le Racisme Et L'Antisemitisme v. Yahoo! Inc., No. 05-1302 (9th Cir. January 12, 2006)

The Court declined consideration of whether Yahoo! Inc. could use U.S. courts to resolve an international dispute over its display of Nazi memorabilia. A French judge had ordered Yahoo to remove Nazi paraphernalia from its site, yahoo.com, and had proposed a fine of approximately \$15 million for running an auction site in which users could buy and sell items banned in France. Yahoo contested the decision in the U.S. District Court for the Northern District of California, seeking declaratory judgment that the French court's order was unenforceable. That court found the order unenforceable in the United States because it would violate Yahoo's free speech rights under the First Amendment. On appeal, the Tenth Circuit dismissed the case in a 99-page opinion for lack of ripeness. Although it lost, Yahoo did not appeal. Instead, two French associations filed a petition for certiorari, arguing that the ruling would allow Yahoo to try to use U.S. courts to avoid foreign judgments. Yahoo, which was not forced to pay the fine, filed no arguments in the Supreme Court.



NEWS YOU CAN USE

FTC RESPONDS TO PROPOSED WHOIS LIMITS

The Federal Trade Commission (FTC) issued a statement saying that access to the Whois databases was critical to law enforcement agencies around the world. Whois databases are online information directories that contain contact information about web site operators. The statement was in response to a recommendation by one of the advisory boards of the Internet Corporation for Assigned Names and Numbers (ICANN) that access to Whois data be limited to use for “technical purposes only.” That ICANN report can be accessed at <http://gns0.icann.org/issues/whois-privacy/tf-report-15mar06.htm>.

ISP GROUP TO BUILD DATABASE TO COMBAT CHILD PORN

Five major Internet service providers (ISPs) joined forces to jointly build a database of child pornography images, as well as develop other tools to help law enforcement prevent distribution of the images. The participants are Time Warner Inc.’s AOL, Yahoo Inc., Microsoft Corp., EarthLink Inc. and United Online Inc., the company behind NetZero and Juno. They pledged a total of one million dollars to set up a technology coalition as part of the National Center for Missing and Exploited Children (NCMEC). Plans call for NCMEC to collect known images and create a unique mathematical signature for each one based on a

common formula. Each participating ISP would scan its users’ images for matches. Although each ISP will set its own procedures on how it uses the database, the partnership will allow them to exchange their best ideas and ultimately develop preventive tools.

SURVEY: CYBER CRIME GREATER THREAT THAN PHYSICAL CRIME

Chief information officers see cyber crime as a greater threat than physical crime, according to an International Business Machines (IBM) survey of 600 U.S. manufacturing, financial, health care and retail businesses. Of those surveyed, 57 percent said they are losing more money due to cyber crime than from conventional crime, through lost income, loss of current and potential customers and decreased employee productivity. The survey also found that 84 percent believed that criminal hacker groups are increasingly replacing lone hackers as cyber crime perpetrators. However, 83 percent of respondents said they were well prepared to combat organized cyber crime, with 73 percent reporting they had upgraded their antivirus software and 69 percent having upgraded their firewalls. Two thirds were implementing intrusion detection or prevention technologies, while 53 percent were implementing patch management systems on their networks. In addition to the U.S. survey, businesses from 16 foreign countries, including the United Kingdom, were surveyed with similar results.

THREAT REPORT: MORE DESKTOP AND WEB ATTACKS

Cyber attackers are continuing to move away from broad attacks on firewalls and routers and are now targeting desktop and web applications, according to the ninth volume of Symantec Corporation's semiannual Internet Security Report, one of the world's most comprehensive sources of Internet threat data. The report, which covers the period from July 1, 2005 to December 31, 2005, also said that viruses, worms and Trojans that can unearth information from a user's computer rose six percent up to 80 percent of the top 50 malicious software code threats in the last half of 2005. Additionally, phishing threats continued to increase, and a phishing attempt was made in every 119 processed e-mail messages, translating into an average 7.92 phishing attempts per day. The report also cited a growing threat from robot, or "bot," networks used to launch attacks on computer systems, now up to 1,402 denial of service attacks per day utilizing bots. The full report is available on www.symantec.com.

MICROSOFT TO OFFER FREE CHILD MONITORING SOFTWARE

Microsoft Corp. plans to include free software to help parents monitor the online activities of their children in its upcoming Windows Live offering of web services. Windows Live Family Safety Settings is currently scheduled to launch in the summer of 2006, and will allow parents to filter web sites and receive reports of what their children are doing online. Microsoft already offers a similar service under its subscription-based MSN premium. The company

also plans to eventually allow parents to control who communicates with their children through e-mail, messaging and in their blogs.

AOL TO PAY COSTS FOR NONPROFITS' E-MAIL

America Online (AOL) will offer nonprofit organizations that want to send e-mail to AOL members two new free e-mail options that have many of the features, including images and web links, of the company's premium service designed for commercial mass e-mail. The first new service, the Enhanced White List, is for nonprofits that meet AOL's anti-spam and e-mail requirements, and AOL expects to complete tests of the service within 30 days. Unlike certified e-mail, messages sent via the Enhanced White list will not be marked as "certified." The second offering, to be ready in 30 days, will allow nonprofits to use a third party e-mail service to authenticate their messages. Such services charge a flat, nonrecurring fee, which AOL has promised to pay.

Ed. Note: In our March-April 2006 issue, we reported that a consortium of non-profit and public interest groups, including Move.On.org, the AFL-CIO, Gun Owners of America and the Electronic Frontier Foundation, had protested the plan by AOL and Yahoo to charge a fee for guaranteed delivery of bulk e-mails.

ICANN TO TEST NON-ENGLISH DOMAIN NAMES

The Internet Corporation for Assigned Names and Numbers (ICANN) outlined a plan for testing domain names in non-English characters in response to a

change sought by Asian and Arabic Internet users. The tentative timetable calls for tests to begin in the second half of 2006 which would seek to ensure that non-English suffixes would not affect the current global addressing system. The Internet's current directories use only the 26 letters of the English language, the 10 numerals and the hyphen.

WATCHDOG GROUP NAMES KAZAA AS VIOLATOR

StopBadware.org, a corporate-backed watchdog group that monitors software for deceptive and abusive practices, named Kazaa, a widely used file-sharing program, as a violator of its guidelines in its first report. The report said that Kazaa misleadingly advertises itself as spyware-free, does not completely remove all components from the uninstall process, interferes with computer use and makes undisclosed modifications to other software. The group, which was started by researchers from Harvard and Oxford universities, also named a video download manager distributed by Movieland.com, a spyware removal program from SpyAxe.com and Waterfalls 3 by Screensaver.com. StopBadware.org receives funding from Google Inc., Sun Microsystems Inc. and Chinese computer manufacturer Lenovo Group Ltd.

DC TO FIND WIRELESS INTERNET THAT HELPS POOR

The District of Columbia government plans to ask companies to bid on building a wireless Internet system that will also provide low income residents with free Internet access and possibly free computers and training. The

winning company will receive an exclusive, eight-year franchise to attach wireless devices to District-owned street lights and buildings. It will also get some access to the District's private fiber optic network free of charge to carry wireless traffic toward the Internet. According to government officials, no tax dollars will be involved. Bidding companies may submit plans for where they would build the network, how they would charge paying customers and what speeds will be offered. The District will not mandate the technology bidders must propose and will give bidders the option of serving low income residents with landline Internet access rather than a wireless system. However, the District plans to require that low income residents receive a minimum speed of 500 kilobits per second downstream.

PAPER: CHIPS IN ID TAGS CAN CARRY VIRUS

A group of European researchers affiliated with the computer science department at Vrije Universiteit in Amsterdam have demonstrated how it is possible to insert a software virus into radio frequency identification (RFID) tags. The tags are part of a microchip-based technology used in commercial and security applications. The researchers, led by Andrew Tanenbaum, an American computer scientist, presented a paper entitled "Is Your Cat Infected With a Computer Virus?" at the annual Pervasive Computing and Communications Conference sponsored by the Institute of Electrical and Electronic Engineers. The paper also describes how this vulnerability could be used to undermine tracking systems; however, the group has published a set of steps to help protect RFID chips from

such attacks. The paper, as well as related materials on security issues related to RFID systems, is posted online at www.rfidvirus.org.

SURVEY: BANKS SHOULD MONITOR ONLINE BANKING SESSIONS

The annual Financial Institution Consumer Online Fraud Survey by RSA Security found that 89 percent of account-holders would like their bank to monitor online banking sessions for signs of irregular activity or behavior, and 59 percent would like their bank to contact them if something suspicious is detected. The survey, which asked 402 U.S. adults their opinions about online banking authentication and e-mail fraud, also found that 73 percent of account holders believe that financial institutions should replace username and password log-in with stronger authentication. Another finding was that, as a direct result of scams such as phishing, 79 percent of account holders are less likely to respond to an e-mail from their bank. The survey also shows that many account holders are looking to their banks and their Internet service providers (ISPs) to protect them from phishing. Forty-five percent feel that an ISP blocking service for phishing would be effective, and 68 percent would like their ISP to offer such a service. The survey was conducted by Infoserv, an online market research company.

U.S. RANKED FIRST IN WORLD INFORMATION TECHNOLOGY STUDY

The U.S. rose to first position from fifth place in the World Economic Forum's (WEF's) Global Information Technology rankings, an annual study

designed to assess the impact of information technology on the competitiveness of nations. The study covers 115 economies worldwide and includes a Networked Readiness Index designed to measure the ability of countries to make the most of information technologies. The study also noted that 17 of the 36 companies named in the separate WEF's technology pioneers report are based in the U.S. The WEF is a nonprofit organization that promotes economic development and is best known for its annual forum for business leaders and government policy makers.

GOVERNMENT CIOs: SECURITY IS PRIORITY

Government chief information officers (CIOs) say they have made progress in establishing information technology (IT) security as a priority and expanding security awareness among staff, according to the 16th annual survey by the Information Technology Association of America (ITAA) of U.S. government CIOs. However, most CIOs felt that they were not moving forward on privacy issues. The survey included interviews with 36 CIOs or assistant CIOs and three government oversight officers. As in the past, it focused on general trends rather than hard data points. In addition to security concerns, the CIOs identified as key priorities standardizing and consolidating their IT infrastructure, improving project management and examining ways to use managed services from outside vendors.

REPORT: MOST AMERICANS ARE ANTI-SURVEILLANCE

More than 85 percent of Americans are against or unsure about spyware that monitors Internet shopping or behavior being placed on their personal computers, according to a report entitled “Americans: Perceptions About Surveillance,” by the Pokemon Institute, a privacy think tank. Nearly 90 percent of the respondents to Pokemon’s survey reported that they are not in favor of or are unsure about government wiretaps. The survey also found that nearly all of the respondents rejected the idea of the government implanting chips in people for identification, and 72 percent were also not in favor of electronic tags, such as RFIDs, that are embedded in products that could be used to track identities from short distances. However, more than 57 percent of respondents said they would not mind if law enforcement authorities used hidden cameras to monitor traffic or speeding. The report may be accessed at: http://i.n.com/pdf/ne/2006/surveillance_study.pdf.

RESEARCH: WHY PHISHING SCAMS STILL WORK

Three U.S. academics published research into why, after years of public warnings, phishing scams still work. For their paper, “Why Phishing Works,” Rachna Dhamija of Harvard University and Marti Hearst and J.D. Tygar of the University of California at Berkeley conducted tests on a small sample of users. They found that 90 percent of their subjects were unable to pick out a highly effective phishing e-mail. The researchers put together a spoofed Bank of the West e-mail that directed recipients to the phishing web site,

www.bankofthevest.com (note the double “v” instead of the “w”). Presented with this, 91 percent of participants guessed it was legitimate. When the participants were presented with a genuine E*Trade e-mail that directed them to a legitimate site, 77 percent of participants guessed it to be fake. Nearly a quarter of the participants did not look at the address bar, status bar or security indicators on the phishing sites. The paper may be accessed at http://people.deas.harvard.edu/~rachna/papers/why_phishing_works.pdf.

CYBER BLACKMAIL ATTEMPTS ON RISE

Cyber blackmail attempts rose during the first three months of 2006, according to a new study by the Kaspersky Lab, an anti-virus provider. The study, “Malware Evolution: January to March 2006,” finds that hackers are moving away from stealing personal data to direct blackmailing of victims. The report cites cases where virus writers have either encrypted data or corrupted system information before demanding a ransom for safe return of data, with demands ranging between \$50 and \$2,500. The report also finds that hackers are adopting more sophisticated encryption schemes, and advises users to avoid downloading files from untrusted sources, run up to date anti-virus protection and make regular backups. The report is available at <http://www.viruslist.com/en/analysis?pubid=184012401>.

PENNSYLVANIA FIRST E- NOTARIZATION STATE

Pennsylvania has become the first state that allows notaries to digitally sign electronic documents. The first phase of

their e-notarization program is limited to four counties, but it is anticipated that it will expand to the rest of the state after the first year. State and local officials worked with the National Notary Association (NNA) in its development, and NNA maintains the registry for the program. The e-notary seals must be issued by a qualified certificate authority with the ability to suspend and revoke the seals. Notaries would have to appear in person before a county official to prove identity. Recordors in participating counties will monitor the program for one year.

NUMBER OF ONLINE GAMBLERS DOUBLES

The number of Americans who gambled online doubled to about four percent of the population last year, according to a survey by the American Gaming Association, a trade group that represents casinos and suppliers. The survey found that almost half of the people who gambled online said they did so primarily because of the convenience, with fewer than 10 percent saying it was for the chance to win money. Despite the U.S. Justice Department's position that the law forbidding interstate telephone betting also applies to the Internet, the survey found that only 19 percent of the 552 Internet gamblers polled thought it was illegal. Internet gambling worldwide generated about \$12 billion in revenue last year, with about half of the sales coming from U.S. residents.

HATE GROUPS FAVOR U.S. SERVERS

Hate groups around the world often use Internet servers based in the U.S. to send propaganda and instructions to

followers, according to the eighth annual report on Internet hate speech by the Simon Wiesenthal Center, an international Jewish human rights organization. The center had logged about 6,000 web sites in the past year used by racists and bigots to incite violence. The report said that while much of the material originates overseas, the extremists find it easier and cheaper to use a site hosted in the U.S. The center said it has recently been intercepting an increased number of online terrorism tutorials and how-to manuals aimed at sympathizers who might actually be recruited to carry out attacks. The center passes most of the material on to law enforcement officials.

SPONSORED LINKS MOST LIKELY TO HARBOR SPYWARE

Web sites that pay for sponsored links are nearly three times more likely to harbor spyware or adware, or to generate spam, than URLs generated by the search engine's algorithms, according to anti-virus software maker McAfee's SiteAdvisor service. The study, which evaluated Google, Yahoo, MSN, AOL and Ask.com search engines using 1,300 different keyword searches, found that about five percent of the links served up in the first five pages can infect computers or plague users with spam. That figure, which is about one link per search page, is more than double SiteAdvisor's web average of two percent. SiteAdvisor's research showed that MSN had the lowest percentage of risky sites at 3.9 percent, while Ask.com's percentage was almost double at 6.1 percent. Google, Yahoo and AOL were in the middle, with 5.3, 4.3 and 5.3 percent, respectively. Sponsored links, however, are a big income source for search engines, as

SiteAdvisor reported that the search industry made \$1.1 billion from sponsored sites last year. SiteAdvisor, which was recently acquired by McAfee,

offers free plug-ins for Internet Explorer and Firefox that overlay Google, Yahoo and MSN search results with color coded labels that reveal risky sites.



PUBLICATIONS YOU CAN USE

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

This report addresses the need 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

WIRETAPPING

On May 8, 2006, the Hawaii Legislature approved SB 965, which conforms the state’s electronic surveillance laws to federal statutes. The bill authorizes interception of communications if the interception might provide evidence of a crime and sets procedures for surveillance and interception. It also authorizes

emergency surveillance without a prior court order in certain specified circumstances. Currently, investigators seeking to wiretap a suspect must petition a judge with the suspect’s defense attorney present, potentially putting undercover agents, informants and other people involved in the investigation in danger. The bill also establishes a surveillance review unit in the Office of the Attorney General, which would be

responsible for reviewing all applications for interception of communications.

ESTABLISHMENT OF A CYBER CRIME UNIT

The Florida Legislature passed SB 2322/HB 1593, statutorily establishing the Cyber Crime Unit in the Office of the Attorney General and making the unit a responsibility of that office. The bill also mandates the unit's responsibility to investigate crimes associated with the sexual exploitation of children. The bill would become effective on July 1, 2006.

ONLINE SEXUAL PREDATORS

On June 7, 2006, Colorado Governor Bill Owens signed signed H.R. 1011, making it a felony to use the Internet to set up a meeting with a child younger than 15 years of age without the parents' permission, It also makes it a felony to expose oneself or ask a child to expose him or herself over the Internet. The bill also makes possession of child pornography a felony. The bill was supported by Attorney General John Suthers.

GPS MONITORING OF CHILD SEXUAL PREDATORS

Virginia's H.B. 846, which mandates three years of supervised probation as part of the sentence for offenders convicted of a serious sex offense, in addition to mandatory GPS monitoring, will become effective on July 1, 2006. The legislation was supported by Attorney General Bob McDonnell.

Wisconsin Governor Jim Doyle signed Assembly Bill 591 on May 22, 2006, which extends lifetime global positioning system (GPS) monitoring to serious and repeat child sex predators. The measure requires tracking of anyone on parole, probation or supervised release for first or second degree child sexual assault that involved violence or the threat of violence.

CHILD PORNOGRAPHY

Virginia's H.B. 1014, which prohibits intentionally operating a web site to facilitate the payment for accessing child pornography over the Internet, becomes effective on July 1, 2006. The legislation is intended to penalize third party billing companies that intentionally assist in processing payments for those consumers who want to purchase access to child pornography. The bill was supported by Attorney General Bob McDonnell.

DATA SECURITY

On July 1, 2006, Indiana's new data security law will go into effect, requiring businesses and database owners to notify affected state residents of data security breaches. If more than 1,000 people are affected, the company must also notify the three major credit bureaus. If a company or database owner fails to comply, the Attorney General can sue and seek penalties of up to \$150,000. If more than 500,000 people are affected, or if the cost of notifying victims exceeds \$250,000, the database owner can make its official notification by a posting on its web site or by a news release to the media.

INTERNET GAMBLING

On May 25, 2006, the U.S. House Judiciary Committee approved 25-11, H.R. 4777, a bill that would ban much online gambling, including bets on sporting events and games of chance, such as poker. The bill, sponsored by Representative Bob Goodlatte (R-VA), would update the Federal Wire Wager Act, which prohibits gambling over telephone lines, but currently may not apply to Internet gambling because not all web traffic travels over telephone lines. The bill would also require banks to block transactions related to online gambling and would empower state and federal law enforcement agencies to compel Internet service providers to remove or disable

links to gambling sites. The bill effectively would prevent state lotteries from taking their games online, as no current technology exists that would keep gambling within a state. Fantasy sports leagues would be exempt. The bill is backed by the administration, as well as certain religious groups such as the Southern Baptists Convention, professional sports leagues such as the National Football League and online auction company eBay. It is opposed by casinos, the Poker Players Alliance, which argues that poker is a game of skill and should be exempt and the Independent Community Bankers of America, a group of about 5,000 small banks, says its members do not have the manpower to block all gambling transactions.

NET NEUTRALITY

The House Judiciary Committee also approved H.R. 5417, a bill requiring broadband providers to abide by strict Internet neutrality principles. The bill, sponsored by Representative James Sensenbrenner, Jr. (WI-R), which was approved along party lines by a vote of 20-13, means that broadband networks would have to be operated in a non-discriminatory manner. It is supported by Internet companies such as Amazon.com, Google, Microsoft and Yahoo. A competing bill, H.R. 5252, sponsored by Representative Joe Barton (R-TX), passed the House Committee on Energy and Commerce on May 17, 2006 and gives the Federal Communications Commission (FCC) exclusive authority to investigate violations of Internet neutrality principles, but does not include strict Internet neutrality mandates. An amendment to H.R. 5252, which would have codified net neutrality regulations into federal law and prevented broadband providers from discriminating among Internet sites, was defeated in the House by a vote of 269-152. The House leadership could try to meld both bills together before a floor vote, or they could permit both bills to go to the floor for votes.

DIGITAL COPYRIGHTS

On June 8, 2006, the House Judiciary Committee's Subcommittee on Courts, the Internet and Intellectual Property approved HR 5553, which seeks to amend Section 115 of title 17, U.S. Code, the complex system of royalties governing the music industry by providing for digital delivery of musical works. Currently, separate licenses exist for the "performance" of a song and the reproduction or distribution of it, so companies wishing to sell music have to negotiate separate licenses for each song's recording. The bill would establish a "blanket licensing" system in which those entities would apply for and receive licenses through a "one-stop shop."

SECURITY FOR WIRELESS NETWORKS

Westchester County, New York became the first in the country to enact a law requiring local businesses to implement "minimum security measures," such as installing a network firewall, changing the systems SSID or network name and disabling SSID broadcasting, to protect their wireless networks. Enacted on April 21, 2006, the new law applies to all commercial businesses that collect customer information, as well as businesses that offer public Internet access. Businesses that collect, store and use personal information have 180 days to comply with the law. In addition, Internet cafes and other organizations that offer wireless access need to prominently post signs advising customers to implement security measures on their systems when accessing the Internet. Those who fail to comply will receive a warning giving them 30 days to remedy the situation. A second violation will result in a \$250 fine, and further violations will result in a \$500 fine.



TOOLS YOU CAN USE

“Avoid Identity Theft: Deter, Detect, Defend”

This educational package by the Federal Trade Commission contains presentation powerpoint slides and brochures. It can be viewed by accessing www.consumer.gov/idtheft, and the kit can be obtained by e-mailing idtheftkit@ftc.gov.

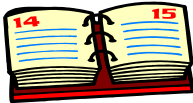
“Child Pornography on the Internet”

This 102-page publication describes the problem and reviews the factors that increase the risks of Internet child pornography. It then identifies a series of questions that may assist in the analysis of the problem and reviews responses based on evaluative research and police practice. It can be accessed at www.cops.usdoj.gov/mime/open.pdf?Item=1729

Child Abuse Training & Technical Assistance Center (CATTa) Newsletter

The summer 2006 CATTa newsletter features an article on protecting children from Internet perpetrators. The article provides information from the National Juvenile Online Victimization Study, which collected data from Internet-related arrests between July 1, 2000 and June 30, 2001. The newsletter is published by the California Institute on Human Services at Sonoma State University and can be accessed at www.cattacenter.org/pdf/Summer2006Web.pdf

Note: The Editor thanks Teena Watkins, Assistant Attorney General in the Office of the Arkansas Attorney General, for information on the newsletter.



HOLD THE DATE!

INTERNET CRIMES AGAINST CHILDREN TRAINING THIS FALL

Don't miss the in-depth training conference on **Prosecution and Innovative Approaches to Internet Crimes Against Children**, 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. Topics to be covered will include social networking sites, ISP record retention issues and legal issues in child pornography investigations. More information will be available in August 2006 so please contact Hedda Litwin, NAAG Cyber Crime Counsel, at 202-326-6022 or hlitwin@naag.org to receive conference updates.