

**Issue 19**

**News Highlights in This Issue:**

AGs of 33 States Stop Illegal Tobacco E-Sales	5
Police May Search Roommate's Computer	9
Losses From Software Piracy Increasing	16
Illinois Bans ID Theft Pretexting	21
Cyber Crime Training Application Available	24
ISP Cannot Disclose E-Mails Sent to Blog	10
Nebraska Sex Offender Law Now Effective	21
Sentence for Failed Hacking Attempt Upheld	15
One in Five Companies Hit By Keyloggers	17
South Dakota Online Offender Registry Available	21
Polygraph Exams of Sex Offenders Can Be Used	10
Adam Walsh Online Child Safety Law Enacted	22
Online Transactions Subject Firm to Jurisdiction	12
Virus Writers Now Using Open Source Code	20
U.S. House Passes Internet Gambling Ban	22
Auction Sites Not Subject to Fair Credit Act	15
Majority of Child Abuse Web Sites Are in U.S.	20
U.S. House Passes Social Networking Site Bill	22
Most Computers Sending Spam Are in Taiwan	18
Bloggers Are Not Publishers Under the CDA	12
National Strategy for ID Theft Paper Available	23

**Table of Contents**

<b><u>Features:</u></b> Data Breaches and Laws	2
<b><u>AGs Fighting Cyber Crimes</u></b>	5
Losses From Illegal Software Increasing	
AG Crist: Child Pornography Sentenced	
Illinois AG's Team Arrests Sex Offender	
AG Carter Publicizes Security Breach Law	
Louisiana AG Arrests Child Pornographer	
AG Cox's Unit Arrests Child Predator	
Mississippi AG Releases Cyber Statistics	
AG Bruning Urges Online Gambling Action	
New Mexico AG: Child Predator Indicted	
AG Spitzer Urges Net Neutrality Passage	
North Carolina AG Part of Cyber Sting	
AG Stenejem Updates Sex Offender Site	
Ohio AG: Child Pornographer Sentenced	
AG Corbett's Unit Charges Child Predator	
South Carolina AG: Child Predator Arrested	
AG Abbott: Child Pornographer Sentenced	
Virginia AG: Guilty Plea in ID Theft Case	
AG McKenna Files Spyware Lawsuit	
West Virginia AG Stops Online Loan Scheme	
AG Lautenschlager Awards Cyber Grant	
<b><u>In the Courts</u></b>	9
Police May Search Roommate's Computer	
Polygraph Exams for Offenders May Be Used	
ISP Cannot Disclose E-Mails to Blog	
NSL Requests Under SCA Are Unconstitutional	
SCA Inapplicable to Public Password Sites	
Bloggers Are Not Publishers Under CDA	
Lack of Jurisdiction for Out-of-State Torts	
E-Transactions Confer Personal Jurisdiction	
Jurisdiction Over Foreign Web Site Conferred	
Contacts With Foreign Web Site Insufficient	
Part of Maine E-Tobacco Law Struck Down	
Firing for Online Pornography is Constitutional	
Estimate of Stolen Goods Sold on eBay is Sound	
FCRA Not Applicable to Internet Auction Sites	
Sentence for Failed Hacking Crime Upheld	
<b><u>News You Can Use</u></b>	16
Losses From Illegal Software Increasing	
Security Concerns Stop Internet Usage	
New Orleans Approves Wireless Network Firm	
Number of Online Users Reaches New High	
One in Five Companies Hit by Keybloggers	
Microsoft Finds Three Million Bots in PCs	
Taiwan Hosts Majority of Spam Servers	
Survey Finds Business Cybercrime Losses Down	
AT&T Changes Account Disclosure Policy	
Federal Agency Sets Laptop Security Rules	
Public-Private Alliance to Study ID Theft	
Click Fraud Costs \$800 Million/Year	
Online Records for Florida Courts Approved	
Virus Writers Using More Open Source Code	
U.S. Has Majority of Online Child Abuse Sites	
Task Force Finds Flaws in E-Voting Systems	
<b><u>Legislation Update</u></b>	21
Illinois Ban ID Theft Pretexting	
U.S. House Committee Approves ID Theft Bill	
Nebraska Sex Offender Law is Effective	
South Dakota Offender Registry Available	
Federal Online Child Safety Law Enacted	
U.S. House Passes Social Networking Bill	
House Committee Passes Net Restriction Bill	
House Approves Online Gambling Ban Bill	
<b><u>Tools You Can Use</u></b>	22
<b><u>Cyber Crimes Against Children Training</u></b>	23

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](mailto: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.

---

## **Security Breaches and State and Federal Data Protection Laws**

**By Mary Ann Percy\***

Since February 2005, nearly 90 million data records of U.S. residents have been exposed because of security breaches, according to the consumer advocacy group Privacy Rights Clearing House (PRC).<sup>1</sup> Of these breaches, 31 percent were of educational institutions, 27 percent were of governmental or military agencies, 19 percent were of general business organizations; 12 percent were of banking, credit or financial services; and 11 percent were of healthcare facilities or companies.<sup>2</sup> These statistics include only breaches of personal information, such as Social Security numbers, account numbers and driver's license numbers.

PRC began chronicling breaches after the February 15, 2005 ChoicePoint breach. ChoicePoint is one of the largest data aggregators and resellers in the country. Identity thieves opened 50 accounts to access ChoicePoint's databases of personal information, resulting in a watershed moment in data security, both in terms of how public and private agencies should protect digital information and in defining what their duty to citizens and consumers once a breach of information has occurred. Consequently, agencies

and lawmakers are currently focusing on these issues in their attempt to protect digital information for millions of consumers and taxpayers.

### **State Legislation**

Several state legislatures have passed notification and credit freeze laws aimed at protecting citizens affected by a security breach. The catalyst for reporting data breaches to the affected individuals has been California Civil Code Sections 1798.29 and 1798.82, which comprise California's 2003 Security Breach Notification Law. California was the first state to pass a law requiring businesses, non-profits and public agencies, regardless of geographical location, to notify California residents if their personal information is compromised because of a security breach. Because of this law, ChoicePoint was required to notify residents of California who might have been affected by that breach.<sup>3</sup>

Since the ChoicePoint breach, state and federal lawmakers across the country have followed the lead of California and recognized the compelling need for these laws that attempt to combat security breaches. For instance, lawmakers have passed legislation that impose requirements on businesses to safeguard customer information, notify consumers when their

information has been compromised and enable consumers to take affirmative steps to prevent unlawful use of their compromised information by thieves.<sup>4</sup> Specifically, at least 32 states now have laws requiring private companies to safeguard consumers' personal information and to notify consumers when this information has been compromised. Of these 32 states, 21 have passed breach-notification laws also requiring government agencies to disclose data-security problems that could possibly lead to identity theft.

For instance, on July 1, 2006 Indiana's new data security law went into effect. The law requires businesses and database owners to notify affected state residents of data security breaches.<sup>5</sup> Also, New York recently amended former laws to create the Information Security Breach and Notification Act. This Act imposes a duty on state entities and persons or businesses conducting business in New York who own or license computerized data that includes private information to disclose any breach of the data to New York residents.<sup>6</sup> In addition, the 2005 Illinois General Assembly passed legislation requiring all companies and organizations, regardless of where they are based, to notify Illinois residents in the event of a security breach.<sup>7</sup>

Furthermore, at least half of the states have enacted legislation that either already grants or will soon give all or some consumers the right to prevent identity theft by placing a security "freeze" on their credit reports. This provision allows consumers to freeze their reports so that when a credit reporting agency receives a request for the consumer's credit report, the requester will be told that the report is unavailable for viewing. Twenty states have enacted laws that already give or will give all their residents the right to a security freeze. An additional five states currently provide this option only to ID theft victims.<sup>8</sup>

### **Federal Legislation**

Not only are states passing laws aimed at protecting individuals from identity theft, but Congress is also considering legislation to address topics such as consumer notice, reimbursement,

preemption of state laws, regulatory burden and credit freeze provisions. Six congressional committees are moving at varying speeds and with varying proposals to determine the best policy to protect consumers. For example, a bill pending in the U.S. House of Representatives is H.R. 3997, The Financial Data Protection Act. This bill would require consumer notice if the compromised information is reasonably likely to be misused in a manner that would cause harm or inconvenience to any affected consumer. H.R. 3997 would only enable identity theft victims to freeze their credit reports, which means that consumers could not freeze their credit reports to prevent identity theft. The bill could weaken existing state laws that require consumers to be notified when a company experiences a security breach.

Pending in the U.S. Senate is S. 1408, The Identity Theft Protection Act, which would require consumer notice when there is a reasonable risk of identity theft. This bill does not provide for reimbursement for losses incurred by financial institutions and/or consumers. The bill would preempt several state law provisions such as those on freeze provisions, information security programs, notice of security breaches, and liability for failure to notify of a security breach.<sup>9</sup>

### **Veterans Affairs and other Security Breaches**

While ChoicePoint and California's legislation may have served as the initial force behind state notification and freeze laws, the recent security breach affecting millions of U.S. veterans could be considered the impetus behind current proposed federal legislation. On May 3, 2006, a laptop computer and external hard drive were stolen from the Maryland home of a Veterans Affairs analyst. This equipment held as many as 26.5 million names, birthdates and, in about 17.5 million cases, Social Security numbers of U.S. former service members. Although the laptop was stolen on May 3, the Secretary of Veterans Affairs (VA) was not informed until May 16, and the VA did not disclose this security breach to veterans or Congress until May 22, exactly 19 days after the theft occurred. The

computer and data were recovered on June 28, 2006, and Veterans Affairs is “highly confident” that the information was not compromised.<sup>10</sup> None of the data was encrypted or password protected. Because of this high level of confidence, the VA has decided not to provide free credit monitoring to the affected individuals.

Although the VA breach has received the most recent attention, many more examples of breaches and subsequent delays in notification exist. For instance, hackers entered the student services system network of Western Illinois University on June 5, 2006. This security breach put at risk the personal data of 180,000 alumni and students, customers of the online bookstore, and guests of the university’s hotel. The university did not notify those affected for 10 days. Insurance organization American International Group (AIG) lost personal identifying information on about 970,000 consumers through a March 31, 2006 burglary at one of its Midwest offices. AIG did not notify those persons affected for more than 10 weeks. When a laptop containing personal information from thousands of blood donors was taken from a Texas office of the American Red Cross in May 2006, the Red Cross made the decision to not notify affected individuals because the information on the computer was encrypted. Therefore, the Red Cross maintained it had no duty to notify.

## Conclusion

From stolen laptops to infiltrated computer systems, security breaches at public and private organizations are becoming increasingly frequent. In response to this problem, public and private organizations and lawmakers are being called upon to find solutions. These organizations and lawmakers are working to answer questions such as what needs to be done to improve data security; to ensure that policies, practices, and procedures discourage the potential compromise of sensitive data; to prevent another security breach; and to more efficiently report a breach in a timely manner. Suggested answers to these questions have been increased legislation and

appropriations, more strictly enforced protection and notification policies, education about those policies and increased utilization of data encryption and passwords.<sup>11</sup>

## Sidebar

For more information on data security breaches and laws on this topic, please see the following sources.

- State Public Interest Research Groups (PIRGs) for a listing of states with notification and freeze laws, found at <http://www.pirg.org/consumer/credit/statelaws.htm>.
- ConsumersUnion.org: A nonprofit publisher of Consumer Reports, for an alphabetical listing by state security breach laws, found at [www.consumersunion.org/campaigns/Breach\\_laws\\_May05.pdf](http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf).
- Attrition.org for information on examples of recent security breaches, found at [www.attrition.org/dataloss](http://www.attrition.org/dataloss).
- Privacy Rights Clearing House for information on security breaches and related laws, found at <http://www.privacyrights.org/index.htm>.
- California Legislative Information for information on the California security breach law, found at <http://www.leginfo.ca.gov/>.
- Credit Union National Association for information on data protection bills pending in Congress, found at [http://www.cuna.org/gov\\_affairs/legislative/issues/2006/data\\_sec\\_legcomp.html](http://www.cuna.org/gov_affairs/legislative/issues/2006/data_sec_legcomp.html).
- Stateline.org for a map depicting states with various data protection laws, found at <http://www.stateline.org/live/ViewPage.action?siteNodeId=137&languageId=1&contentId=126215#map>.

\*Mary Ann Percy is currently a third-year law student at the University of Mississippi School of Law. This article was written during her internship with the NAAG Cyber Crime Project during the summer of 2006.

---

<sup>1</sup> <http://www.privacyrights.org/ar/ChronDataBreaches.htm>.

<sup>2</sup> <http://www.idtheftcenter.org/breaches.pdf>.

<sup>3</sup> For more information on the California law, see <http://www.leginfo.ca.gov/>.

<sup>4</sup> Comments of the Attorneys General of the Undersigned States before the Federal Communications Commission, in the matter of Implementation of the Telecommunication Act of 1996, April 28, 2006.

<sup>5</sup> Crystal Garcia, *Official: New law protects Hoosiers from identity theft*, TribStar.com, [http://www.tribstar.com/news/local\\_story\\_184225945.html/resources\\_printstory](http://www.tribstar.com/news/local_story_184225945.html/resources_printstory).

<sup>6</sup> <http://www.cscis.state.ny.us/securitybreach/>.

<sup>7</sup> *Madigan Urges General Assembly to Pass Legislation to Ensure Illinoisans are Alerted to Breaches of Personal, Financial Information*, press release from the office of the Illinois Attorney General, April 12, 2005.

---

<sup>8</sup> For a summary of state breach and freeze laws, see <http://www.pirg.org/consumer/credit/statelaws.htm>

<sup>9</sup> For more information on these and other federal data breach bills pending in the 109<sup>th</sup> Congress, see [http://www.cuna.org/gov\\_affairs/legislative/issues/2006/dat\\_a\\_sec\\_legcomp.html](http://www.cuna.org/gov_affairs/legislative/issues/2006/dat_a_sec_legcomp.html).

<sup>10</sup> Letter from James H. Burrus, Jr., Acting Assistant Director, Criminal Investigative Division of the U.S. Department of Justice to Senator Larry E. Craig, Chairman, Committee on Veterans Affairs, dated July 18, 2006.

<sup>11</sup> Opening Statement of Chairman Larry Craig, at the hearing of the U.S. Senate Committee on Veterans Affairs titled, VA Data Privacy Breach: Twenty-Six Million People Deserve Assurance of Future Security, held July 20, 2006.



## AG INITIATIVES

---

### ATTORNEYS GENERAL FIGHTING CYBER CRIME

#### MULTI-STATE

Attorneys General of 33 states reached an agreement with Lorillard Tobacco Co, under which Lorillard agreed to implement new measures to prevent the illegal sale of its cigarettes over the Internet and by mail. The new protocols provide for (a) termination of shipments to any of Lorillard's direct customers that the Attorneys General have found to be engaging in illegal Internet and mail order sales; (b) reduction in the amount of product made available to direct customers who engage in illegal resale of cigarettes to Internet vendors; and (c) suspension from Lorillard's incentive programs for any retailer found to be engaging in illegal sales. The negotiations with Lorillard were led by the Office of the Attorney General of New York. The Attorneys General of the following jurisdictions joined the agreement: Alabama, Arkansas, California, Connecticut, Delaware, District of Columbia, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Montana, Nebraska, Nevada, New

Hampshire, New Mexico, Northern Mariana Islands, Oklahoma, Oregon, South Carolina, South Dakota, Tennessee, Utah, Vermont, Washington, West Virginia and Wyoming. A copy of the Protocol may be accessed at <http://www.naag.org/news/pdf/20060710-LorillardProtocol.pdf>.

#### FLORIDA

**Attorney General Charlie Crist** announced that Lynn Carico was sentenced to five years in prison after pleading guilty to one count of promotion of child pornography, a second-degree felony, and one count of compiling/possessing child pornography. Carico was also sentenced to 10 years of sex offender probation and must register with the state as a sex offender. He was arrested after talking online with and transmitting pornography images to a person he believed was a pedophile but was actually an undercover investigator with the Jacksonville Sheriff's Office. A search warrant was subsequently executed on Carico's home, and authorities seized his computer, which contained multiple images and videos of

child pornography. The Marion County Sheriff's Office also participated in the investigation. The case was prosecuted by attorneys from Attorney General Crist's Child Predator Cybercrime Unit. A copy of the criminal charges filed can be accessed at [http://myfloridalegal.com/webfiles.nsf/WF/JFAO-6QWM83/\\$file/Carico\\_Information.pdf](http://myfloridalegal.com/webfiles.nsf/WF/JFAO-6QWM83/$file/Carico_Information.pdf).

## ILLINOIS

**Attorney General Lisa Madigan's** investigators coordinated with the Chicago Police Department and the U.S. Marshals Service to arrest George Zollicoffer, a registered sex offender, based on a tip from a Colorado probation officer received on the Illinois Sex Offender Registry Team (I-SORT) Hotline. The tip reported that Zollicoffer had "deregistered" with the Fort Collins, Colorado Police Department and was moving to Illinois. A check of the Illinois State Police Sex Offender Registry revealed he had not registered. Zollicoffer was subsequently charged by the Cook County State's Attorney's office with Failure to Register as a Sex Offender, punishable by two to five years in the Illinois Department of Corrections.

## INDIANA

**Attorney General Steve Carter** visited Terre Haute to publicize the state's new security breach disclosure law. The law requires companies to notify state customers if there is a breach in their security system that compromises their personal identification information. The law applies to all companies, regardless of where they are based, if the breach concerns Indiana residents. Failure to obey the law could result in fines of up to \$150,000.

## LOUISIANA

**Attorney General Charles Foti's** agents arrested Nicholas Carver for trying to arrange to make a pornographic video involving two 16-year-

old girls. He was charged with one count of computer-aided solicitation of a minor and one count of attempted pornography involving juveniles. If convicted on the first count, he faces up to 10 years in jail and a fine of up to \$10,000. If convicted on the second charge, he faces up to 10 years in prison.

## MICHIGAN

**Attorney General Mike Cox's** Child and Public Protection Unit arrested Robert Vanderwall, a self-employed cab driver, for using the Internet to sexually solicit what he believed to be a teen-ager but was actually an undercover officer. Vanderwall was arraigned on one count of child sexually abusive activity, and one count of using the Internet to commit child sexually abusive activity. Michigan State Police from the Cadillac Post assisted in the arrest.

## MISSISSIPPI

**Attorney General Jim Hood's** Cyber Crime Unit released its statistics for year-to-date 2006. The Unit opened 69 new cases, 25 of which have been closed. Of those cases, 15 search warrants were executed, 29 subpoenas were issued, 62 computers were seized and 20 computers were imaged. In addition, 10 persons were indicted and five persons have been convicted. A total of 51 forensic examinations were conducted, and the Unit responded to 72 requests for technical assistance from other law enforcement agencies in the state. Finally, Unit members trained 254 law enforcement agencies. They also provided Internet safety information to 1,837 students and information on social networks and electronic stalking to an additional 618 people.

## NEBRASKA

**Attorney General Jon Bruning** sent a letter to the president of the National Automated Clearing House Association (NACHA), an electronic

payments association, urging that its members cease service to online gambling web sites. Attorney General Bruning asked that NACHA adopt and issue an Operations Bulletin with suggested business practices to assist members in protection themselves from becoming a party to illegal online gambling.

## **NEW MEXICO**

**Attorney General Patricia Madrid** announced that a grand jury indicted three suspected Internet child predators who were captured in a sting by her Internet Crimes Against Children (ICAC) Unit and other law enforcement agencies. Gavin Frazier and Tyrone Wiggins were each indicted on one count of Child Solicitation by Computer, a fourth degree felony, for sexually soliciting undercover detectives posing as a 13-year-old girl. The third suspect, Roy Gallea, was charged with two counts of Child Solicitation by Computer for twice soliciting an undercover detective posing as a 14-year-old girl. Each count of Child Solicitation by Computer is subject to a basic sentence of up to 18 months imprisonment and a \$5,000 fine. The sting operation was conducted by the ICAC Unit and officers and investigators from the Albuquerque, Santa Fe, Rio Rancho and New Mexico State Police Departments, the Bernalillo County Sheriff's Department, the New Mexico Taxation and Revenue Tax Fraud Investigations Unit and Immigration and Customs Enforcement.

## **NEW YORK**

**Attorney General Eliot Spitzer** sent a letter to the leaders of the U.S. Senate Commerce Committee urging the adoption of the Internet Freedom Preservation Act, a net neutrality bill that would generally bar all network operators from making special deals with content providers to ensure speedier delivery or improved quality of service and would require them to offer all Internet material on an "equivalent" basis. Attorney General Spitzer also encouraged the committee to add a

provision that would allow state Attorneys General and private parties to sue companies that fail to adhere to net neutrality regulations.

## **NORTH CAROLINA**

**Attorney General Roy Cooper's** State Bureau of Investigation (SBI) agents participated in an undercover operation that led to the arrest of Charles Childers, former Chief of Police of Landis, North Carolina, on felony charges of child solicitation and child pornography. Childers had sexually graphic conversations with an undercover SBI agent posing as a teenage girl and sent child pornography to the "girl." The undercover operation was carried out by the North Carolina Internet Crimes Against Children (ICAC) Task Force, which is led by the SBI, the Michigan ICAC Task Force and the U.S. Postal Service. The case is being prosecuted by the U.S. Attorney's Office for the Middle District of North Carolina.

## **NORTH DAKOTA**

**Attorney General Wayne Stenehjem** announced a new mapping feature on the state sex offender web site that allows citizens to access detailed maps to see if a high risk or registered offender lives near their home or their child's school. Recent improvements to the site also allow users to search for sex offenders by address, age and physical description. Users may also review a list of all of the state's registered sex offenders, now consisting of almost 1,000 names. Since its inception in November 2001, the site has handled 918,000 individual inquiries with millions of page views.

## **OHIO**

**Attorney General Jim Petro** announced that former Wapakoneta Police Chief David Harrison was sentenced to six years in prison following his conviction on charges related to accessing child pornography on his work computer.

Harrison was also labeled a sexually-oriented offender and will be required to register his home and work addresses with the sheriff upon release. A jury convicted him on 15 counts of illegal use of a minor in nudity-related material, two counts of unauthorized use of property and one count of theft in office. Scott Longo and Erin Rosen of Attorney General Petro's Child and Elder Protection Section served as special prosecutors in the case.

### PENNSYLVANIA

**Attorney General Tom Corbett's** child predator unit agents charged Kurt Huettner with criminal attempted unlawful contact with a minor and criminal use of a computer. Huettner allegedly began sexual conversations in an Internet chat room with an undercover agent who was posing as a 13-year-old girl. He was arrested when he showed up to meet the "girl" at a planned location. Attorney General Corbett's agents, together with the Upper St. Clair police, then executed a search warrant on Huettner's home and seized computer equipment and disks.

### SOUTH CAROLINA

**Attorney General Henry McMaster** announced that Karim Gulamhusein, a graduate assistant at Clemson University, was arrested in an undercover sting conducted by the City of Westminster Police Department, a partner in Attorney General McMaster's Internet Crimes Against Children (ICAC) Task Force. Gulamhusein was charged with Criminal Solicitation of a Minor, a felony punishable by up to 10 years imprisonment, and Attempted Criminal Sexual Conduct With a Minor, a felony punishable by up to 20 years in prison. Arrest warrants allege that Gulamhusein solicited sex online from a person he believed to be a 13-year-old girl but was actually a police officer. He was arrested at a meeting location he arranged with the "girl." Computers and computer-related equipment were seized during the execution of search warrants at both his

residence and at the University. The case will be prosecuted by Attorney General McMaster's office.

### TEXAS

**Attorney General Greg Abbott** announced that Ron Guzman, who admitted to keeping sexually explicit images and videos of children on his iPod digital music player, was sentenced to 40 years in prison. Guzman pleaded guilty to nine counts of child pornography possession and six counts of child pornography promotion. He also pleaded guilty to four counts of aggravated sexual assault of a child and one count of indecency with a child in a plea deal in a separate case. Sentences in both cases will run concurrently. This was the first case investigated by Attorney General Abbott's office in which the offender used an iPod to store child pornography.

### VIRGINIA

**Attorney General Bob McDonnell**, together with Louisa Commonwealth's Attorney R. Don Short, announced that Dawn Rumsey pled guilty to three counts of felony identity theft and three counts of committing computer fraud with the identities. By employing several illegal means, Rumsey obtained the personal identifying information of several people and then went on an online "fishing" expedition, using their information to apply for credit cards over the Internet. Once she received the cards in the victims' names, she went on a shopping spree for nearly \$30,000. Rumsey will serve the maximum sentence of 45 years, 40 years of which will be suspended on condition that she make restitution to the victims and does not have access to the Internet or personal identifying information of others. The Sheriff's Offices of Greensville and Louisa Counties, the Henrico Police Department and the U.S. Postal Service also participated in the investigation. Rusty McGuire of Attorney General McDonnell's Computer Crime Unit argued the case.

## WASHINGTON

**Attorney General Rob McKenna** filed his second lawsuit under the state's Computer Spyware Act, accusing four California-based corporations of installing software that takes control of a computer by launching aggressive and persistent pop-ups that demand payment for a movie download service. The suit names as defendants Digital Enterprises, d/b/a Movieland.com; Alchemy Communications; AccessMedia Networks; and Innovative Networks. Two company officials, Easton Herd of Digital Enterprises and Andrew Garroni of Alchemy, are also charged. If found liable, each defendant could be fined \$100,000 per violation of the Computer Spyware Act and \$2,000 per violation under the state Consumer Protection Act. They may also be required to pay restitution to affected consumers. The suit was filed after a seven-month investigation by Attorney General McKenna's Consumer Protection High-Tech Unit. A copy of the complaint may be accessed at <http://www.atg.wa.gov/releases/2006/Documents/MovielandComplaint8-14-06.pdf>.

## WEST VIRGINIA

**Attorney General Darrell McGraw's** office worked with Canadian police and Internet service providers to shut down Global Capitol Solutions and New Balance Express, two online loan companies who tried to defraud out-of-state consumers. The companies promised on their web sites to approve consumers for fast loans, charging large advance fees. When consumers paid, they were either sent fake loan checks or real checks that bounced. Both companies listed fake West Virginia addresses on their sites, but were actually based in Canada.

## WISCONSIN

**Attorney General Peg Lautenschlager** awarded a grant of \$2,550 to the Wausau Police Department to assist in the investigation of Internet crimes against children. The funds will be used to purchase hardware and software to analyze hard drives police suspect contain evidence of these crimes. The new equipment will allow police to get the results of a search in a few days, instead of waiting months for results from the state crime laboratory.



# IN THE COURTS

---

## SEARCH AND SEIZURE: SCOPE OF WARRANT

*United States v. Adjani*, 2006 WL 1889946 (9<sup>th</sup> Cir. July 11, 2006). Overturning a lower court ruling, the Ninth Circuit ruled that police may seize and search the computer of a suspect's roommate, even though the roommate has not been identified as a suspect and is not named as a target in the investigation. Christopher Adjani was suspected of trying to extort three million dollars from his former

employer. Agents obtained a warrant for his arrest and a search warrant covering his residence which specifically authorized seizure of computers and various computer storage devices. When executing the search warrant, agents seized a computer belonging to Jana Reinhold, Adjani's roommate, which contained e-mails between the roommates implicating Reinhold in the extortion. Adjani and Reinhold were arrested and charged with conspiracy to commit extortion. Adjani and Reinhold moved to suppress the incriminating e-

mails, and the U.S. District Court for the Central District of California granted the motion, finding that the agents lacked sufficient probable cause to search Reinhold's computer and should have obtained an additional warrant once they found the e-mails. The Ninth Circuit reversed, finding that the warrant was supported by probable cause because the affidavit established a fair probability that evidence of a crime would be found in computers at Adjani's residence.

### **SEX OFFENDERS: POST-RELEASE USE OF POLYGRAPHS**

*United States v. Johnson*, No. 04-4992 (2<sup>nd</sup> Cir. May 1, 2006). In a case of first impression, the 2<sup>nd</sup> Circuit found that polygraph examinations for convicted sex offenders being monitored on probation can be used to determine compliance with the terms of their supervised release, and their use does not violate the Fifth Amendment right against self-incrimination. The appeal was filed by Jeffrey Johnson, a convicted sex offender, who challenged the terms of his supervised release issued by a judge of the U.S. District Court for the Northern District of New York. That judge had allowed the polygraph testing proposed by probation officials, but limited the scope of questioning to "information necessary for supervision, case monitoring and treatment." Johnson argued that the testing would violate his Fifth Amendment rights and force him to choose between making an admission or staying silent, which would violate the terms of his supervised release. His argument failed, however, with the court noting that 2<sup>nd</sup> Circuit precedent clearly allows for supervised release to be revoked where an offender "fails to answer questions even if they are incriminating."

### **STORED COMMUNICATIONS ACT: CIVIL SUBPOENAS**

*O'Grady v. Superior Court*, 2006 WL 1452685 (Cal. App. 6<sup>th</sup> Dist. May 26, 2006). Reversing the court below, the court of appeals held that the Stored Communications Act prohibits an ISP that hosted a blog's e-mail account from disclosing e-mails sent to the blog in response to a subpoena issued during civil litigation. The subpoena asked for the production of e-mails that would allow Apple Computer to identify the person(s) who sent trade secrets about an unreleased Apple product to the blog Power Page, and resulted in articles Power Page published on its blog. Apple filed suit against several John Does and served the subpoena on Nfox, which provides e-mail service to the Power Page blog. Jason O'Grady, the publisher of the Power Page blog, moved for a protective order to quash the subpoenas issued to Nfox and prohibit Apple from serving a subpoena on Power Page. The Superior Court of Santa Clara County denied the motion, holding that Power Page was not entitled to quash Nfox's subpoena and since a subpoena had not yet been served on Power Page, the issue was not ripe for adjudication. The appellate court reversed, noting that the Stored Communications Act outlines five exceptions to its prohibition of the disclosure of stored communications, and none of them authorized production in response to a civil subpoena.

### **STORED COMMUNICATIONS ACT: DISCOVERY**

*Doe v. Gonzalez*, 2006 WL 1409351 (2<sup>nd</sup> Cir., May 23, 2006). In a consolidated appeal of two cases, the 2<sup>nd</sup> Circuit found that the compulsory, secret

and unreviewable production of information required by the FBI's application of 18 U.S.C. § 2709 violates the Fourth Amendment, and the non-disclosure provision of 18 U.S.C. § 2709 (c) violates the First Amendment.

§ 2709 (a) of the Stored Communications Act imposes a duty on wire and electronic communications providers to comply with FBI requests for "subscriber information and toll billing records information or electronic communication transactional records." § 2709 (b) makes these written requests in the form of a National Security Letter (NSL). The first case, *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), involved an ISP that received a NSL requesting information on a subscriber and was told that no one could be informed of the request under § 2709 (c). The plaintiff challenged § 2709 (c) on First Amendment grounds, arguing it was a prior restraint on speech that was not sufficiently narrow to achieve a compelling government interest. The U.S. District Court for the Southern District of New York agreed with the plaintiff. The second case, *Doe v. Gonzalez*, 2005 WL 2179634 (D. Conn., Sept. 9, 2005), involved a broadly worded NSL requesting patron records sent to a library employee and prohibiting him or her from disclosing the request. Here, the plaintiff asked for a preliminary injunction against enforcement of the gag order, arguing it was a prohibition on constitutionally protected speech. The U.S. District Court for the District of Connecticut granted the injunction, finding that plaintiff showed irreparable harm from suppression of speech and that plaintiff's suit was likely to succeed on the merits. The Second Circuit vacated and remanded the *Ashcroft* case to the lower court. Since § 2709 (c)(3) now requires

NSL recipients to notify other parties assisting in compliance, *Gonzalez* was dismissed as moot.

### **STORED COMMUNICATIONS ACT: PASSWORD-PROTECTED SITES**

*Snow v. DirectTV*, 2006 WL 1493817 (11<sup>th</sup> Cir. June 1, 2006). Affirming the district court, the 11<sup>th</sup> Circuit held that the Stored Communications Act, 18 U.S.C. § 2701, does not apply to password-protected web sites accessible to the general public. Michael Snow operated a web site with an electronic bulletin board that stated it was for use by "individuals who have been, or will be, sued by any corporate entity." Access to the bulletin board required a password that could be obtained by registering, as well as agreement that the user was not DirectTV or its agents. Snow alleged that DirectTV accessed the site without authorization, presumably in an effort to stop theft of its encrypted satellite transmissions, and filed a complaint. The U.S. District Court for the Middle District of Florida dismissed the complaint for failure to state a claim upon which relief can be granted, reasoning that electronic bulletin boards are not "in electronic storage" within the meaning of the Act and therefore not protected. The Court of Appeals affirmed, although with different reasoning. Instead the court focused on subsection (2)(g) of the Act which provides in part that it is not unlawful to access an electronic communication made through an electronic communication system readily accessible to the general public. The court reasoned that any member of the general public could register to access the bulletin board and therefore dismissed the complaint.

**LIABILITY FOR WEB SITE  
POSTINGS: BLOGGERS**

*DiMeo v. Max*, No. 06-1544 (ED Pa. May 26, 2006). Effectively overriding the traditional treatment of publishers under statutory and common law, a district court judge has ruled that the pre-emption clause of Section 230 of the Communications Decency Act grants bloggers immunity from libel suits over anonymous postings on their web sites by stating that they cannot be treated as the “publisher” of such postings. Anthony DiMeo III, operator of a publicity firm, sued blogger Tucker Max over a series of anonymous postings on Max’s web site that described a party given by DiMeo’s firm in derogatory terms and that DiMeo claimed were libelous. Although DiMeo conceded that Max had not authored the postings, he argued that Max was liable because he had published them. The court disagreed, finding that Congress enacted Section 230 to provide immunity from libel suits for Internet providers, including bloggers, and dismissed the complaint.

**WEB SITE TAMPERING:  
PERSONAL JURISDICTION**

*Davidoff v. Davidoff*, No. 101728/06 (NY Sup. Ct. May 10, 2006). The court dismissed the case for lack of personal jurisdiction over defendants where defendants, who were not physically present in New York, allegedly committed tortuous acts on an Internet site created by the plaintiff who resided in New York. Plaintiff Jonathan Davidoff, a New York attorney, created a web site featuring his personal and professional information and encouraged clients to view it. His web site’s hosting service was located in Florida.

Defendants, his aunt and uncle, allegedly deleted the files on the web site from their home in Florida, replacing them with a picture of plaintiff with the phrase “Pig of the Year.” Plaintiff sued for destruction of personal property, defamation, intentional infliction of emotional distress, tortuous interference with a business, computer trespass and computer tampering. Defendants contended the court had no jurisdiction because they had no ties to New York and had not committed a tortuous act within the state. Plaintiff argued that personal jurisdiction would lie because their posting intended to target users in New York where the action was filed. While the court agreed with the plaintiff that the defendants’ physical presence in New York was not a prerequisite, it found a lack of jurisdiction in New York because the tortuous acts were committed in Florida. The property claims could not be sustained because the “property” was on the web site’s hosting server in Florida.

**ELECTRONIC TRANSACTIONS:  
PERSONAL JURISDICTION**

*Deutsche Bank Securities, Inc. v. Montana Board of Investments*, 2006 NY Slip Op 04338 (June 6, 2006). In a 6-1 decision, New York’s highest court has expanded personal jurisdiction by ruling that individuals and companies from out of state who conduct business within the state through electronic means of communication are considered to be engaged in commerce in New York and therefore subject to the reach of New York courts. The case involves a failed bond trade between Deutsche Bank, a New York-based bank, and the Montana Board of Investments, a state agency that manages Montana’s public retirement system. All of the failed loan

transactions were conducted through an instant messaging system. The bank brought an action for breach of contract in New York, but the Supreme Court dismissed the complaint for lack of jurisdiction over the Montana agency. The Appellate Division, 1<sup>st</sup> Department reversed, and the Supreme Court affirmed its decision, with the majority finding that the electronic communication established long arm jurisdiction.

### **FOREIGN ONLINE GAMBLING SITE: PERSONAL JURISDICTION**

*Uebler v. Boss Media AB*, 2006 U.S. Dist. LEXIS 34346 (E.D.N.Y. May 30, 2006). Under agency theory, a district court ruled that the agency activities of a foreign online gambling site operator's domestic subsidiary were sufficient to confer personal jurisdiction over the parent. Susanne Uebler, a New York resident, sued Boss Media AB, a Swedish operator of online gambling systems, for failure to pay prize money owed to her from winning one million dollars on an online gambling web site operated by a Boss Media subsidiary. Uebler received about 10 percent of the money by monthly payments, then was told there would be no more payments. Boss Media moved to dismiss for lack of personal jurisdiction. Uebler relied on New York's long arm statute, Civil Practice Law & Rules (CPLR) Sections 302 (a)(1) and (a)(3). CPLR Section 302 (a)(1) provides for personal jurisdiction over a non-domiciliary who, in person or through an agent, transacts business in New York. The court found that jurisdiction over Boss Media was proper based on the activities of its New York-based subsidiary, WebDollar, which managed its financial matters and was listed as a division in its annual report.

### **TRADEMARK INFRINGEMENT: PERSONAL JURISDICTION**

*Pebble Beach Co. v. Caddy*, 2006 WL 1897091 (9<sup>th</sup> Circ. July 12, 2006). The Ninth Circuit ruled that a bed-and-breakfast in England cannot be sued in the United States for infringing on the famous Pebble Beach Golf Club's trademark. Michael Caddy, a citizen of both the United States and the United Kingdom (UK), owns the Pebble Beach bed-and-breakfast in southern England as well as the web site [www.pebblebeach-uk.com](http://www.pebblebeach-uk.com). Pebble Beach Co., which owns the Pebble Beach Golf Club and its web site, [www.pebblebeach.com](http://www.pebblebeach.com), sued Caddy under the federal Lanham Act and the California Business and Professional Code for intentional infringement and dilution of its own web site. Caddy moved to dismiss for lack of personal jurisdiction. The U.S. District Court for the Northern District of California agreed, finding that Caddy's contacts with California were insufficient to confer long-arm jurisdiction, even under state law conferring personal jurisdiction over a party to the maximum extent permitted by federal due process requirement. On appeal, the Ninth Circuit affirmed the dismissal, finding that Caddy's actions were not expressly aimed at California and, regardless of the foreseeable effect, were insufficient to establish jurisdiction.

### **INTERNET TOBACCO SALES: PREEMPTION**

*New Hampshire Motor Transport Association v. Rowe*, 2006 WL 1360943 (1<sup>st</sup> Cir, May 19, 2006). The 1<sup>st</sup> Circuit invalidated part of Maine's Tobacco Delivery Law regulating the Internet sales and delivery of tobacco products,

finding it impermissibly affects the delivery procedures of air and motor carriers and is preempted by the Federal Aviation Administration Authorization Act (FAAAA). Among other things, the law, enacted in 2003 to curb cigarette sales to minors, requires retailers to use a carrier that will deliver a package only to the addressee and verify that the person receiving the package is old enough to buy tobacco. Additionally, Section 1555-D forbids anyone to knowingly deliver tobacco products to a Maine consumer if they came from an unlicensed dealer. Under the law, the person delivering the package is “deemed to know” that it contains tobacco products if the packaging indicates that tobacco products are contained or if the shipper appears on the Attorney General’s list of unlicensed tobacco retailers. The New Hampshire Motor Transport Association, representing air and motor carriers, sued Maine’s Attorney General, claiming the FAAAA, which preempts states from enacting laws related to a carrier’s prices, routes or services, preempted Maine’s law. The U.S. District Court for the District of Maine agreed, concluding that Maine’s law would force carriers to alter their delivery practices. The 1<sup>st</sup> Circuit agreed with the exception of the “deemed to know” section, finding that requiring carriers not to act as knowing accomplices does not cause them to modify their delivery practices.

**PARTICIPATION IN ONLINE PORNOGRAPHY: FIRST AMENDMENT**

*Thaeter v. Palm Beach County Sheriff’s Office*, 2006 US App. LEXIS 13308 (11<sup>th</sup> Cir. May 26, 2006). A three-judge panel of the 11<sup>th</sup> Circuit unanimously ruled that the Palm Beach County

Sheriff’s Office did not violate the First Amendment when it fired two deputies for appearing in Internet pornography. Deputies Ronald Thaeter and Timothy Moran participated in pornography that was available to the public on pay-per-view Internet sites. An anonymous tip led sheriff’s office officials to the sites, and the office filed ethics charges against the deputies, accusing them of failing to obtain authorization for off-duty employment and violating a pledge to set an example by conducting an unsullied private life. Both deputies were terminated after an investigation. Thaeter and Moran filed suit, claiming that their First and 14<sup>th</sup> Amendment rights were violated. The U.S. District Court for the Southern District of Florida granted the sheriff’s office’s motion to dismiss for failure to state a claim on which relief could be granted. On appeal, the 11<sup>th</sup> Circuit, citing *City of San Diego v. Roe*, 125 S. Ct. 521 (2004), found that the deputies’ speech was not protected because it did not involve matters of great public interest. However, the court in its opinion chastised the sheriff’s office for government over-reaching into personal lives.

**INTERNET AUCTION FRAUD: LOSS CALCULATION**

*US v. Wasz*, No. 05-1463 (7<sup>th</sup> Cir. June 14, 2006). The 7<sup>th</sup> Circuit affirmed defendants’ sentences for wire fraud, finding it was reasonable for the district court to use the total retail value of stolen items sold on eBay as an estimate of the actual loss for sentencing calculations. Laura and Bruce Wasz fenced and sold millions of dollars of stolen goods on eBay. They pled guilty to wire fraud in violation of 18 U.S.C. 1343. The U.S. Sentencing Guidelines

applicable to offenses involving stolen property specify a base offense level of six, but they also mandate an increase to that offense level commensurate with the extent of the loss. The U.S. District Court for the Northern District of Illinois calculated the loss at between one and two and a half million dollars based on the total retail value of the stolen goods, which called for a 16-level increase. The court accordingly sentenced them to serve prison terms of 70 and 83 months, respectively. The defendants appealed, contending the district court overestimated the loss results and should have calculated it by using the gain defendants realized on the sales or the actual loss suffered by the retailers of the stolen goods. The 7<sup>th</sup> Circuit found that the loss calculated by the district court corresponds to a conservative estimate of the retail value of the merchandise defendants sold on eBay and thus was a reasonable measure.

**INTERNET AUCTION SITES:  
FAIR CREDIT REPORTING ACT**

*McCready v. eBay*, No. 05-2450 (7<sup>th</sup> Cir. July 10, 2006). The 7<sup>th</sup> Circuit affirmed the district court's dismissal of a suit against eBay under the Fair Credit Reporting Act (FCRA) because eBay could not be considered a "consumer reporting agency." Kenneth McCready was a seller on eBay who had some dissatisfied customers who voiced their dissatisfaction by leaving negative feedback on eBay's Feedback Forum. Instead of trying to improve his sales image, McCready filed lawsuits against eBay in several Midwest courts, including the U.S. District Court for the Central District of Illinois. He alleged that eBay violated the FCRA, 15 U.S.C. §1681 et seq., by providing false and misleading information in the Feedback

Forum. The district court dismissed the case, finding that the Feedback Forum was not a "consumer report" as required under the statute. On appeal, the 7<sup>th</sup> Circuit affirmed, adding that the FCRA applies only to information that is used for consumer purposes, not commercial or business purposes.

**HACKING: LENGTH OF PRISON  
TERM**

*United States v. Salcedo*, No. 05-4147 (4<sup>th</sup> Cir. July 10, 2006). The Fourth Circuit upheld a nine-year prison term for a hacker who tried and failed to steal credit card numbers from the Lowe's home improvement chain. Brian Salcedo was caught breaking into several Lowe's networks over an unsecured Wi-Fi connection. The U.S. District Court for the Western District of North Carolina sentenced him to 108 months in prison and three years of supervised release, despite the fact that no damage was done and despite his cooperation with Lowe's to help boost their security. The sentence, one of the longest for a hacker, was largely based on the amount of harm that would have resulted had the plan succeeded. Salcedo appealed, arguing that the district court erred in using his intended conduct to enhance his sentence and in improperly calculating his base offense level. The Ninth Circuit affirmed, finding that the district court did not err in view of the harm intended and that Salcedo had completed all of the acts necessary to complete the offense so a reduction in sentence did not apply.



## NEWS YOU CAN USE

---

### **REPORT: SOFTWARE PIRACY LOSSES ON THE RISE**

Global losses from the use of illegal computer software rose to \$34 billion in 2005, an increase of \$1.6 billion from the previous year, according to an annual report by the Business Software Alliance. The study also found that 35 percent of the packaged software installed on personal computers worldwide in 2005 was illegal, the same as in 2004. Piracy rates in China, Russia, Ukraine and Morocco, while still high, declined slightly. Overall, piracy rates fell in 51 of the 97 countries surveyed while increasing in 19 countries. According to the study, the countries with the highest piracy rates were Vietnam and Zimbabwe at 90 percent, Indonesia at 87 percent and China and Pakistan at 86 percent. The countries with the lowest piracy rates were the United States at 21 percent, New Zealand at 23 percent and Austria and Finland at 26 percent. The data in the report was assembled by IDC, a global market research firm for the information technology industry.

### **POLL: AMERICANS FEAR INADEQUATE ONLINE SECURITY**

One-half of Americans do not shop or conduct other transactions online due to security concerns, a two percent increase over six months ago, according to a poll commissioned by the Cyber Security Industry Alliance, a computer industry lobby group. The poll also found that fewer than 20 percent of those

sampled believe existing laws are sufficient to protect them on the Internet. Additionally, 70 percent support strong federal data security legislation, even though it could lead to higher prices. The poll, which sampled 1,150 adults, more than 900 of whom were Internet users, was carried out by Pineda Consulting, a Pasadena, California-based strategic research and communication firm and had a 2.89 percent margin of error.

### **EARTHLINK TO BUILD WIRELESS NETWORK IN NEW ORLEANS**

Atlanta-based Internet service provider Earthlink Inc. won approval from the city council to build a wireless Internet network around a free city-owned system in New Orleans. Initially, Earthlink's system will cover about 15 square miles of the 181-mile city, including the downtown business district and the French Quarter. The company will offer two levels of service – a free service expected to operate at up to 300 kps, and a fee service that would operate three and one-half times faster. The city's current network operates at 512 kps – much faster than dial-up connections, but slower than high-speed service offered by private providers. Under state law, it will have to be slowed to 128 kbps when the city's post-Katrina state of emergency ends.

## **REPORT: U.S. ONLINE POPULATION IS AT NEW HIGH**

The U.S. online population reached a new high in 2006 with 73 percent of adults, or 147 million, now using the Internet, according to a new report released by the Pew Internet and American Life Project. The figures represent an increase from January 2005 of 66 percent, or 133 million. Internet use, however, still varies with age, with 88 percent of adults under 30 going online, compared with 32 percent for those aged 65 or older. It also varies by income, with only 53 percent of adults in households earning less than \$30,000 a year using the Internet, compared with 91 percent in households with annual income of over \$75,000. The report can be accessed at [http://www.pewinternet.org/pdfs/PIP\\_Internet\\_Impact.pdf](http://www.pewinternet.org/pdfs/PIP_Internet_Impact.pdf).

## **SURVEY: NEARLY 20 PERCENT OF COMPANIES HIT BY KEYLOGGERS**

Almost one in five organizations have had employees launch a hacking tool or a keylogger within their network in 2006, up from 12 percent in 2005, according to the seventh annual Web@Work study commissioned by Websense Inc., a web security and web filtering productivity software company. A keylogger is a form of spyware with the ability to record keystrokes and screen shots that could be replayed later to reconstruct a user session. It can be used by hackers to steal passwords and confidential information that can provide full access to corporate systems and files. The survey also highlighted bots (short for robots) as a new threat. Bots is software that can be unknowingly installed on an end-user's PC and

communicates with a command and control center. That center has unauthorized control of many bot-infested PCs from a single point, and can be used for launching distributed Denial of Service attacks, acting as a spam proxy or hosting malicious content and phishing exploits. Only 34 percent of information technology (IT) decision-makers said they are very confident that they can prevent bots from infecting employees' PCs when not connected to the corporate network, while 19 percent said they have had employees' work computers or laptops infected with a bot. The survey also found that 62 percent of IT decision-makers filter bot traffic in their network, while 14 percent do not and 24 percent were unsure. The survey, conducted by Harris Interactive, interviewed online 351 IT decision-makers who work for organizations with at least 100 employees and surveyed by telephone 500 U.S. employees who work for organizations with at least 100 employees. It can be accessed at <http://www.websense.com/global/en/PressRoom/MediaCenter/Research/webatwork>.

And more on bots...

## **MICROSOFT REMOVES BOTS IN THREE MILLION PCS**

Microsoft found and removed bots in more than three million home and small business PCs connected to the Internet, according to a report the company issued at the recent Tech Ed conference in Boston. The report was based on Microsoft's scanning of the PCs of 270 million consumers and small business owners who used its free scanning tool from January 2005 through March 2006. The company also found that about 20 percent of the PCs

checked in March had been cleaned once before, then re-infected, most often with a different kind of bot. About 30 percent of the bots were implanted when victims opened attachments sent via e-mail, instant messages or peer-to-peer web sites that share data files. Most of the rest of the bots were spread with no action by the victim.

### **MAJORITY OF SPAM SERVERS LOCATED IN TAIWAN**

According to research by CipherTrust, an e-mail security company, 64 percent of computers sending out junk e-mail are located in Taiwan. The United States was second with 23 percent, and China was third with three percent. The data was gathered using CipherTrust's network of fake "zombie" computers, which spammers usually use without their owners' knowledge to send out their junk messages. The company also noted a rise in spam, attributed in part to the growing use by spammers of image-only e-mails to defeat filters. The spammers place text into a message as an image, thus fooling some filters that use textual recognition to identify e-mails as spam. CipherTrust saw 7.4 million new zombies during their research, with 24 percent of them located in China, 9.4 percent in the U.S. and 7.5 percent in Germany.

### **SURVEY: BUSINESS LOSSES FROM CYBERCRIME DOWN**

Despite the rise in computer-facilitated crime, financial losses incurred by businesses due to cybercrime have decreased, according to the 2006 annual survey by the Computer Security Institute and the FBI. The 615 U.S. CSI members who responded to the

survey reported an average of \$168,000 in cybercrime losses, an 18 percent drop from the 2005 survey which found an average loss of \$204,000. About one-third of respondents said they had no losses due to insider threats, while another 29 percent said that less than one-fifth of overall losses came from insider threats. Although almost all of the respondents in both years stated that they use firewall and antivirus software, this year, eight out of 10 said they also use spyware protection, which might contribute to the decrease. A copy of the survey may be obtained at the web site, <http://www.gocsi.com>.

### **AT&T ALTERS INTERNET PRIVACY POLICY**

AT&T Inc. changed its privacy policy for Internet and television customers to specify that account information is a business record the company owns and can be disclosed to government and law enforcement, as well as to protect the company's "legitimate business interests." AT&T considers account information to include the customer's name, address, telephone number, e-mail address and information about the customer's services, but does not include usage information, such as how a person uses the Internet. Under the new policy, customers must agree to it before using AT&T broadband and TV service. AT&T notified its seven million customers of the new policy but told them it would continue its policy of not sharing customer information with advertisers for marketing purposes.

### **OMB SETS GUIDELINES FOR FEDERAL LAPTOP SECURITY**

The White House Office of Management and Budget (OMB) issued

new guidelines for federal employee laptop security. Federal agencies now have to encrypt all data on laptop or handheld computers unless the data is classified as “non-sensitive” by an agency’s deputy director. Agency employees will need a two-factor authentication, such as a password and a key card, to reach a work database through a remote connection, which must be automatically disconnected after 30 minutes of inactivity. Finally, agencies must begin keeping detailed records of any information downloaded from databases that hold sensitive information, as well as verify that those records are deleted within 90 days unless their use is still required. OMB will work with agency inspector generals on compliance with the guidelines.

#### **PUBLIC-PRIVATE ALLIANCE TO STUDY ID THEFT, FRAUD**

An alliance of businesses, colleges and federal agencies will combine their expertise at the new Center for Identity Management that will study the problems of identity theft and fraud. Founding partners of the Center include LexisNexis, IBM, the U.S. Secret Service, the FBI, Carnegie Mellon University, Indiana University and Syracuse University. The Center will be located at Utica College in upstate New York. Research will focus on critical issues in identity management, information sharing policy and data protection. One of its initial research projects will examine current and emerging criminal groups that perpetrate identity fraud and theft, with a focus on their methods of operation. The Center will also look at developing stronger identity authentication systems and will share its research through

training sessions, symposiums, publications and its web site.

#### **CLICK FRAUD COSTS \$800 MILLION/YEAR**

Online advertisers estimate that about 14.6 percent of the clicks on advertisements for which they are billed are fraudulent, costing them about \$800 million in 2005, according to a study by Outsell, a research and advisory firm. That \$800 million does not include the estimated \$500 million that advertisers say they no longer spend on pay-per-click advertising. The survey of 407 advertisers found that 27 percent had already slowed or stopped their pay-per-click advertising. In addition, 75 percent of those surveyed said they had experienced click fraud, and seven percent said they had requested refunds. Pay-per-click is the primary revenue source for Google and a big revenue contributor for Yahoo.

#### **FLORIDA MOVES TO ONLINE COURT RECORDS**

The Florida Supreme Court approved a controversial recommendation by the Committee on Privacy and Court Records that Florida courts should move to a statewide system of easily accessible online court records. The court also approved establishment of a pilot program, while extending the current online records moratorium for another year until more permanent procedures can be established. The court did allow Internet access to dockets, case schedules, verdicts and other basic case information and issued some guidelines outlining who is responsible for keeping private information out of public records. Under current law, there are about 1,000

exemptions to open records laws dealing with court cases. The court said that the party filing documents must seek confidentiality for situations that fall outside these exemptions.

### **VIRUS WRITERS USING MORE OPEN-SOURCE METHODS**

Malicious software writers are increasingly using open-source methodologies when developing their code, according to security company McAfee's Global Threat Report for 2006. McAfee also warned that more hackers are sharing source code and ideas, including distributing source code with documented explanations and annotations of how that code works, helping programmers to adapt it. The report claims that more virus writers, especially those involved in organized crime, are forming communities. It says that malicious software now has a long-term development cycle, with code being developed, bugs being fixed and betas and final versions being distributed among the malicious software community in ways similar to those used in legitimate open-source communities. McAfee reports that hacker tools are also created and distributed freely on an open-source model.

### **OVER HALF OF ONLINE CHILD ABUSE SITES ARE IN U.S.**

More than 50 percent of online images of child abuse can be traced to the U.S., according to a study by the Internet Watch Foundation (IWF), a watchdog group based in the United Kingdom. In the first six months of 2006, the IWF received more than

14,000 reports of suspected web sites, a 24 percent increase from the first six months of 2005. Of the reports, nearly 5,000 sites contained images of child abuse, with nearly 2,500 sites traced to the U.S. and more than 730 sites to Russia. A further eight percent of 287 web sites containing child abuse remained accessible for one to five years after being reported by the IWF to authorities. Japan, Spain, Thailand and South Korea are also among the worst offending countries for hosting child abuse content. The IWF is funded by the European Union and United Kingdom Internet industry.

### **STUDY SAYS E-VOTING SYSTEMS FLAWED**

The Task Force on Voting System Security convened by New York University's Brennan Center for Justice released a report that concluded that the most widely-used e-voting systems all have flaws that can be addressed relatively easily. However, it finds that few states and counties have implemented the recommended security measures. Even the printing of paper records, seen as a countermeasure to hacking and other attacks, does little good if audits are not routinely and automatically performed, according to the study. Recommendations include banning wireless components, which can create openings for attacks, and randomly testing selected machines on Election Day to uncover malicious software and other problems triggered only that day. The Task Force members were from government, universities, security companies and non-profit advocacy groups.

# LEGISLATION UPDATE

---

## **Identity Theft**

On July 5, 2006, Illinois Governor Rod Blagojevich signed SB 2554 into law, banning the practice of pretexting, or pretending to be an account holder, or to have authorization to access an account to obtain cell phone records and other personal records. The practice is often used by companies who then sell phone records online. A violation of the law, which was effective immediately, is a class two felony and is also subject to a civil suit brought by the victim(s).

The U.S. House of Representatives' Energy and Commerce Committee approved H.R. 1078, legislation criminalizing the sale of Social Security numbers and requiring the Federal Trade Commission (FTC) to issue and enforce regulations on the practice. The bill, sponsored by Representative Edward Markey (D-MA), also gives the FTC broad authority to grant exceptions to the law for the purpose of national security, law enforcement, national health, emergency or research purposes. The bill, as passed, incorporates an amendment made by Representative Markey that puts a cap on civil penalties, includes an exception for the use of partially redacted Social Security numbers for credit verification or other approved reasons and contains a state preemption provision. This amendment, which was approved by voice vote, was required by Committee Chairman Joe Barton (R-TX) for his support of the bill. The bill has also been referred to the Ways and Means Committee, which shares jurisdiction over it.

## **Sex Offenders**

Nebraska LB 1199, a comprehensive bill that strengthens penalties and post-release provisions for sex offenders, became effective on July 14, 2006. In addition to enhancing sentences for sexual assault of a child, the law provides for

court-ordered treatment of sex offenders who have completed their sentences but continue to pose a threat. It also provides for lifetime supervision of repeat sex offenders and those convicted of sexual assault of a child in the first degree or those using force or threat of serious harm in the commission of the assault. The new law establishes a working group to study sex offender treatment and management and make recommendations.

The South Dakota online registry of sex offenders became available on July 1, 2006 and provides the name, address, photograph and type of crime committed by each offender. The registry is available on the web site of the Attorney General of South Dakota. The legislation creating the registry, SB 150, was signed into law on February 17, 2006.

## **Online Child Safety**

The Adam Walsh Child Protection and Safety Act was signed into law on July 27, 2006, becoming Public Law 109-248. It provides that anyone using innocent or misleading words or images, such as "Barbie" or "Furby," that confuse a minor into viewing a harmful web site will face up to 20 years in prison in addition to fines. The law makes the intentional Internet sale or distribution of date rape drugs a new federal crime carrying a potential sentence of up to 20 years. It requires sex offenders to provide a DNA sample and creates a national sex offender registry to be run by the FBI. The law also funds pilot programs to monitor sex offenders with real time tracking devices such as a GPS downlink, a cellular uplink and two-way voice communications. Finally, it authorizes a study to evaluate the effectiveness of monitoring and restricting sex offender activities.

## **Social Networking Sites**

On July 26, 2006, the House passed by 2/3 majority H.R. 5319, a bill requiring recipients of universal support for schools and libraries to enforce a policy that prohibits access to a social networking site or chat room that might subject minors to obscene or indecent material or subject them to sexual advances or requests. It also directs the Federal Communications Commission to publish an annual list of social networking sites and chat rooms that have provided easy access for predators. The bill has been referred to the Senate Commerce, Science and Transportation Committee.

## **Operations in Internet-Restricted Countries**

The Global Online Freedom Act, or H.R. 4780, which would impose strict obligations on U.S. technology companies doing business with countries that restrict Internet usage, was unanimously approved by the U.S. House Subcommittee on Africa, Global Human Rights and International Operations and forwarded to the full Committee on International Relations. Under the bill, which was sponsored by Representative Christopher Smith (R-NJ), U.S. firms would be barred from keeping any electronic communication, such as e-mail, that contains

personally identifiable information on servers or other storage facilities in Internet-restricting companies. They would also be prohibited from turning over personal information about their subscribers to governments in those countries except for legitimate law enforcement purposes. Internet service providers could face fines of up to \$2,000,000 per offense and imprisonment for blocking access to any U.S. government-sponsored web site or content, such as Voice of America, in those countries.

## **Internet Gambling**

On July 11, 2006, the House, by a vote of 317-93 passed H.R. 4411, legislation that amends the 1961 Wire Act prohibiting gambling using telephone wires to include Internet gambling as a prohibited activity. The bill, sponsored by Representative James Leach (R-IA), would ban most forms of Internet gambling and require banks to develop systems to block their customers' transactions to gambling web sites. It allows states to continue to regulate gambling within their borders. The bill also increases criminal penalties for gambling businesses that settle Internet bets with credit cards, checks or fund transfers. It has now been placed on the Senate legislative calendar.

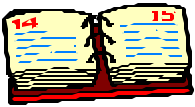


# **TOOLS YOU CAN USE**

---

## **A National Strategy to Combat Identity Theft**

This document describes the components of a national strategy and their interrelationships. It includes best practices or innovative responses that illustrate each component. It can be accessed at <http://www.cops.usdoj.gov/mime/open.pdf?Item=1732>.



# REGISTRATION NOW OPEN!!!

---

## **CYBER CRIMES AGAINST CHILDREN TRAINING THIS FALL**

Application forms are now available for prosecutors from state Attorneys General offices to attend the in-depth training conference on **Prosecution of and Innovative Approaches to Cyber 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) at the University of Mississippi. 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 include legal issues in child pornography and child predator investigations, social networking sites and ISP record retention issues. To apply, please complete and return the application form on the last page of this e-newsletter. For additional information or questions, please contact Hedda Litwin, Cyber Crime Counsel, at 202-326-6022 or [hlitwin@naag.org](mailto:hlitwin@naag.org).

**SEE APPLICATION FORM ON PAGE 24!!!!!!!**

