



National Association
of Attorneys General

CYBERCRIME NEWSLETTER

Issue 3

May/June

News Highlights in this Issue

Oklahoma, Virginia Enact Anti-Spam Laws

Oklahoma Senate Bill 660 makes putting deceptive information in e-mail illegal. Virginia's new law establishes criminal penalties for large scale offenders. **Page 10**

Two Government Studies Say Online Pornography is Widespread

The General Accounting Office reports that 76% of test sites had pornography. The House Government Reform Committee finds blocking technology has limited preventive use. **Page 12**

Legislation Providing Tough Penalties Against Child Pornography Enacted

President Bush has signed the PROTECT Act, which ends a distinction under previous law that allowed defendants in child pornography cases to claim sexually explicit information did not involve real children, but rather computer-simulated ones. **Page 10**

Thirteen Attorneys General File Fraud Suits Against Pop-Up Software Provider

The Attorneys General took legal action against Alyon Technologies, Inc. for illegally charging consumers for viewing pornographic websites the consumers had never visited nor agreed to visit. **Page 6**

Internet Fraud Complaints Tripled in 2002

The Internet Fraud Complaint Center has announced that it had referred three times the number of complaints to law enforcement in 2002 than the previous year, with total monetary loss tripling to \$54 million. **Page 13**

Government Study Finds Federal Agencies Lax in Protecting Social Security Numbers

A report by the Social Security Administration's Inspector General finds that 14 out of 15 federal agencies examined had inadequate controls to protect citizens' social security numbers. **Page 12**

Four Attorneys General File Actions Against Scammers and Spammers

The actions represent a wide array of deceptive schemes and illegal scams including auction fraud, the illegal sale of controlled substances, bogus business opportunities and deceptive money-making scams. **Page 5**

Table of Contents

AG Initiatives.....	5
AG Reilly Prosecutes Campus Identity Fraud.....	5
Michigan AG Charges Child Abuse Using Internet.....	5
AG Moore Announces School Officer Pled Guilty to Child Pornography.....	5
AG Spitzer Arrests "Buffalo Spammer".....	5
Four AGs Sue Internet Scammers & Spammers.....	5
13 AGs File Fraud Suits Against Pop-Up Software Provider.....	6
In the Courts.....	7
Employer Must Pay Cost of Electronic Discovery.....	7
Under ECPA, Consent to Interception Cannot be Inferred.....	8
Anonymous Hacker's Search Did Not Implicate 4 th Amendment.....	8
Legislation.....	10
Oklahoma, Virginia Enact Anti-Spam Laws.....	10
New Law Has Tough Penalties For Child Pornography.....	10
California Senate Pass Tough Anti-Spam Bill.....	11
Ohio Legislature Sends Anti-Cyberstalking Bill to Governor.....	11
Identity Theft Protection Bill Passes Texas Senate.....	11
House Subcommittee Votes to Extend Internet Tax Moratorium.....	12
Internet Gambling Bill Scheduled for House Debate.....	12
News.....	12
Congress Establishes Cybersecurity Panel.....	12
Two Federal Agencies Find Online Pornography is Widespread.....	12
SSA: Federal Agencies Lax in Protecting Social Security Numbers.....	12
NET Standards Task Force to Fight Spam.....	12
FTC: 2/3 of Spam Messages Are False.....	12
Internet Fraud Complaints Tripled in 2002.....	13
Executive Order Allows Infrastructure Data to Be Classified.....	13
Features	
Geeks With Guns.....	2
Free School Curriculum for Cyberspace Responsibility.....	6

Geeks with Guns, or How to Have Your Forensic Examiner Explain Computer Evidence

Richard L. Hardy & Susan S. Kreston

Introduction. When testifying about computer forensic evidence, it is often necessary for the forensic examiner to explain technical terms and concepts to the judge or jury, or to rebut technical testimony and evidence offered by the defense. As is so often the case with a “battle of the experts,” what the jury chooses to believe depends upon who they accept as their teacher. The difficulties in testifying about highly technical evidence encompass a need to be technically accurate while also being clear. To accomplish this, complex concepts must be explained in easily understood terms while conveying a true picture of the underlying technical information. Over time, experienced forensic examiners have developed analogies that assist with understanding several of the most commonly addressed issues. The best of these analogies have been developed in concert with prosecutors, investigators and other examiners, and have been refined and extended over time. Following are some concepts that need to be addressed in court, and analogies that could prove useful in their explanation.

File Allocation Table. The File Allocation Table (FAT) can be likened to a library card catalog that discloses the location of books within a library. The title of the book is contained in the Allocation Table, and the book is the File itself. To find a book, one looks up the name in the card catalog, which then points to the book’s location.

Deleted Files. Deleted files are files whose reference has been removed from the file system, and the area of the electronic media they occupy is released for reuse. Until overwritten with new characters, these files may be recovered.

The use of the term “deleted” is, in many ways, misleading. Deleting a file can be analogized to putting household garbage in a garbage bag, but keeping the bag in the house. While the garbage has, technically, been thrown away, it can still be

readily retrieved. Therefore, finding a deleted file is simply a matter of finding the file that remains in the FAT, but with a different first character.

Using the library card analogy discussed above, when a book (file) is deleted, the library card referring to that book is replaced with one containing the book’s name, minus the first character, and no reference information to the location of the book. On the FAT, the first character of the file’s name is replaced with a *sigma* or “s”. For example, a file named “Criminalevidencehere” would become “criminalevidencehere.” This effectively makes it impossible to find the file simply by searching for it under its title. However, the book itself is not touched until the space it occupies on the shelf is reused by another book. Prior to that, recovering the deleted book is a matter of finding the replaced card, and re-referencing it to the location of the original book, which can then be read in its entirety.

Wiping. “Wiping” a file entails not only deleting the reference to the file in the FAT, but also overwriting its contents, usually with “0s”, preventing later recovery of its contents. Unallocated space and file slack are also common targets of this practice. This process requires specialized software. An analogy for this procedure could be the act of wiping fingerprints from surfaces at a crime scene.

Unallocated Space. This is area on the media that is not currently referred to by the file system. If this area has been previously used, and not “wiped,” it will contain remnants from that prior use. Deleted files are one type of unallocated space. The other type of unallocated space would be space that has never been allocated (made part of any file). Returning to the library card analogy, unallocated space would be those areas of the library with no corresponding library card. If

books or parts of books are still on the shelves (not wiped), however, they may still be read, even though they are not recognized by the card catalog system.

File Slack. File slack is the area allocated to a file that the file does not actually use. File slack may or may not contain data, depending on whether it has been previously used by other files. A useful analogy for file slack is videotape. If you record a half hour show to a fresh hour long videotape, the remaining thirty minutes is analogous to file slack, even though it will be empty. If you had previously recorded a one hour program to that tape, once you finished watching the half hour show, you would see thirty minutes of the originally recorded one hour program. This would be analogous to file slack containing the contents of a previously deleted file.

Sectors and Clusters. A sector is 512 bytes of information. Sectors are then grouped into clusters. A cluster will contain several sectors, commonly eight or 16. A cluster is the smallest area that can be written to by a file, although the file need not fill the entire cluster. An analogy for this would be sectors as pages in a manila file folder, with the file folder itself being the cluster. This analogy can be extended to include a filing cabinet that holds the folder representing the hard drive.¹

RAM Slack. RAM slack is the area in the last sector used by a file that contains information taken from whatever is in the computer's memory at the time that the file is written. Using the videotape analogy again, RAM slack could be likened to the commercial at the end of a recorded program, filling out the final portion of the recording time programmed into the VCR.

Internet Protocol Addresses and Domain Name Servers. Internet Protocol (IP) addresses are numbers used to locate computers on a network.

Every computer has an IP address when it is in use. Phone numbers are analogous to IP addresses in that for one phone to communicate with another, both must have unique numbers in the phone system.

This analogy can be expanded to explain Domain Name Servers (DNS) by using the analogy of a phone book, where the DNS uses a typed in name to find the IP address number, just as a phone book uses a name to find a phone number. Domain Name Servers (DNS) are computers that translate plain text names into Internet Protocol (IP) addresses by using a table cross-referencing the two. For instance, typing "www.cnn.com" into a browser, such as Internet Explorer or Netscape, will cause a check to a DNS that will return the IP address "64.236.24.20," pointing the browser to the computer that contains the requested web page.

E-mail headers and "Spoofing."

E-mail headers contain routing information from the e-mail programs used to forward the message through to its final destination. These are assembled by the servers and are attached at the top of the e-mail. They can be used to trace the origin of the e-mail being examined. IP addresses would be one type of information found in the e-mail header. Two analogies for e-mail headers could be stamps placed on a passport as an individual passes through countries, or forwarding addresses placed on a piece of mail by each post office as the letter passes through the postal system to its final destination. Spoofing e-mail is the act of forging information contained within the header of the e-mail to attempt to mask its origin. One possible analogy for e-mail spoofing would be check fraud, in which the name and address information on the check is changed prior to the check being passed.

Encryption and Steganography. Encrypting a file or image is the deliberate scrambling of information, so that the original information may only be unscrambled with a key. It is an attempt to hide the content of the message and may be

¹The authors would like to thank Mark Menz of My Key Technology for this analogy.

likened to a secret code that needs the “decoder ring” to discover the meaning of the message.² Steganography differs from encryption in that it is an attempt to hide the very existence of a file. Steganography hides one file inside another, so that the second file is completely concealed. Steganography can best be summarized as “hide in plain sight.”³ The hidden file will usually be encrypted and/or password protected. An analogy for steganography could be a book with a hollow area, used to hide something within it. A slightly more apt analogy might be a picture created from very small words that only reveals its text content upon close inspection. Another might be a hide-a-key rock. A final analogy is the hidden stairway behind the wall in murder mystery movies.

MD5 hash values. These are extremely exact measures of the size and structure of an object, such as a disk, a file, or a folder. An analogy for this value would be an electronic fingerprint for the object. The slightest alteration in an object, such as minutely cropping an image, or changing the shading on even one pixel, will result in a completely different hash value. Hiding an image or a file within an object, i.e., steganography, will cause a drastic change in hash value. The scientific possibility of two different objects having the same MD5 hash value is more than 1 in 340 undecillion.

⁴ This is a higher level of certainty than even DNA enjoys.

Conclusion. The development of analogies for computer forensic topics is an ongoing collaborative process. Sharing and discussion of these analogies and explanations can help prosecutors and forensic examiners in their quest to find methods to explain complex technical concepts in an understandable and accurate manner.

Rick Hardy is a Detective/Computer Forensic Examiner at the Regional Computer Forensic Laboratory in San Diego, California. Susan Kreston is a Counsel at the National Center for Justice and the Rule of Law at the University of Mississippi School of Law.

² The mathematical probabilities of breaking an encrypted file are daunting. Odds of winning the state lottery today = approximately 2^{28} . Chances of being struck by lightning today = approximately 2^{33} . Chances of being struck by lightning and winning the top lottery prize = approximately 2^{61} . Possible permutations of a modern encryption key = approximately 2^{1024} – (there are fewer atoms in the known universe).

³ See Brad Astrowsky, STEGANOGRAPHY: Hidden Images, A New Challenge in the Fight Against Child Porn, UPDATE, Vol. 13, No. 2 (2000). This publication is also available on-line at http://www.ndaa-apri.org/publications/newsletters/update_volume_13_number_2_2000.html

⁴ Undecillion would be written as a 1 followed by 36 zeros.

AG INITIATIVES

Massachusetts Attorney General Tom Reilly's office prosecuted a former Boston College student for allegedly installing keystroke-recording software on more than 100 campus computers and accessing databases containing personal information on other students, staff and faculty. Douglas Boudreau of Warwick, Rhode Island, a senior studying computer science, was accused of using the intercepted information to add money to a stored-value card which he used in the campus dining room, laundry room and bookstore system, stealing about \$2,000 in goods and services. Boudreau pled guilty to interception of wire communications, unauthorized access to a computer system, larceny, identity fraud and other charges. He was sentenced to five years of probation and was also ordered to go into counseling, reimburse the College and agree to computer monitoring.

Michigan Attorney General Mike Cox, together with the Livingston County Prosecuting Attorney and the Michigan State Police, announced that criminal charges have been filed against a Canton man who used the Internet to solicit, meet and abuse a 15-year-old just days before being arrested for attempting the same conduct with an undercover officer posing as a minor. Leo Fennelly was first arrested in August 2002 after soliciting an undercover member of General Cox's High Tech Crime Unit (HTCU) who was conducting an investigation through the Michigan Crimes Against Children Task Force. After the arrest, Fennelly admitted, and the HTCU confirmed, that he had used the Internet to meet the teen. Fennelly is currently serving a prison term for felony counts arising from the 2002 case.

Mississippi Attorney General Mike Moore, together with the Hancock County District Attorney, announced that Frank Perniciaro, a former school attendance officer for Gulfview Elementary School of Hancock County, pled guilty to Possession of Child Pornography. Perniciaro had used his school computer to download child pornography and save the images to diskettes which were later found in his school office. Perniciaro was sentenced to three years, two years of which will be supervised probation.

New York Attorney General Eliot Spitzer announced that the man known as the "Buffalo Spammer," who has allegedly sent 825 unwanted e-mails, has been arrested and arraigned. Howard Carmack of Buffalo, New York, was charged with stealing the identity of two residents to open Internet access accounts with EarthLink, Inc., falsifying EarthLink's business records, forging the headers of e-mail sent from EarthLink accounts, and possessing a software program designed to create the forged e-mails. Carmack entered not guilty pleas, and bail was set at \$20,000. The prosecution is the first by General Spitzer under New York's identity theft statute, which was enacted in November 2002. His office worked with the FBI and EarthLink during the investigation.

Attorneys General Mike Beebe of Arkansas, Richard Ieyoub of Louisiana, Drew Edmondson of Oklahoma and Greg Abbott of Texas, together with the Federal Trade Commission, U.S. Postal Inspection Service, Securities and Exchange Commission, three U.S. Attorneys and two state regulatory agencies, announced that they have filed 45 criminal and civil law enforcement actions against Internet scammers and deceptive spammers.

The actions represent a wide array of deceptive schemes and illegal scams including auction fraud, the illegal sale of controlled substances, bogus business opportunities, deceptive money-making scams, illegal advance-fee credit card offers and identity theft. A summary of the specific actions can be accessed at <http://www.ftc.gov/os/2003/05/swnetforcepresschart.pdf>

Attorneys General Mike Beebe of Arkansas, Bill Lockyer of California, Lawrence Wasden of Idaho, Lisa Madigan of Illinois, Ben Chandler of Kentucky, Jay Nixon of Missouri, Jon Bruning of Nebraska, Peter Harvey of New Jersey, Roy Cooper of North Carolina, Jim Petro of Ohio, Hardy Myers of Oregon, Greg Abbott of Texas and Peg Lautenschlager of Wisconsin took legal action against Alyon Technologies Inc. of Secaucus, New Jersey to stop them from illegally charging consumers for viewing pornographic websites the consumers had never visited nor agreed to visit. Consumers who misspelled the popular children's website, spongebob.com, were automatically directed to one of the adult-oriented websites for which Alyon handles billing and were billed by Alyon. The suits seek refunds for consumers in addition to civil penalties.

CyberSmart! Curriculum Teaches Kids Computer Literacy and Security Skills



An innovative new school curriculum has been developed to foster civic responsibility in cyberspace and promote technological literacy. The free CyberSmart! Curriculum, co-published by The

CyberSmart! School program with Macmillan/McGraw-Hill, aims to empower students to use the Internet safely, responsibly and effectively. The curriculum provides K-8 teachers with 65 original, step-by-step teacher lesson plans and student activity sheets. Each lesson is aligned with current technology standards and is non-sequential, flexibly integrated to support any school subject.

CyberSmart! teaches the ground rules for online behaviors that are acceptable, appropriate and effective. Because student research is the most common use of the Internet in schools - and Web sites espousing various forms of extremism may be accessed by children both at school and at home - CyberSmart! also develops skills for effective research including how to critically evaluate online content, and how to responsibly handle the unacceptable behavior of others in cyberspace. Students are taught how to stay secure online, protect their privacy, as well as the importance of safeguarding their family computer and its content from harm. The free CyberSmart! Curriculum is available at www.cybersmartcurriculum.org. For more information, contact Jim Teicher, Executive Director at 908-221-1516.



IN THE COURTS

Defendant Employer Must Pay Cost of Electronic Discovery

Zubulake v. UBS Warburg LLC, No. 02 Civ. 1234 (S.D.N.Y. May 13, 2003)

UBS employee Zubulake, alleging that her new manager discriminated against her because she was female, filed a charge of gender discrimination with the EEOC and three months later, she has terminated. Zubulake then filed suit in U.S. District Court for the Southern District of New York, alleging sex discrimination and retaliation under Title VII, the New York State Human Rights Law and the Administrative Code of the City of New York. Discovery commenced, and Zubulake requested all e-mails exchanged among UBS employees concerning her employment. UBS, after producing approximately 350 pages of e-mails, informed Zubulake that the cost of producing additional e-mails from the backup tapes was estimated at \$300,000 and would be prohibitive. A UBS system representative testified that all e-mails sent or received by any employee are automatically stored on backup tapes. Snapshots of all e-mails on a given server were also taken at time of backup, and non-internal e-mails were also stored on optical disks. The system representative added that the restoration process for the tapes is lengthy, with each backup tape taking about five days to restore. He determined that the e-mail files requested were contained on 94 backup tapes.

The court noted that under the discovery rules, the presumption is that the responding party bears the expense of complying with the request, but it may invoke the court's discretion to protect it from undue burden or expense. However, when

electronic data is requested, it is often only available on backup media that is expensive to restore, so the solution has often been to consider cost-shifting – forcing the requesting party to bear the expense. The court noted that the eight-factor Rowe test (outlined in *Rowe Entertainment v. The William Morris Agency*, 205 F.R.D. at 430) is widely used to determine whether costs should be shifted. However, the court felt that the Rowe test was incomplete and generally favored cost-shifting. The court stated that deciding disputes regarding the cost of electronic discovery requires a three-step process. First, the court should thoroughly understand the responding party's computer system, because cost-shifting should only be considered when electronic data is relatively inaccessible, such as backup tapes. Second, the court must determine what data is contained on the media, for in many cases documents from a small sample might suffice. Third, the court proposed a new seven-factor test as follows, with the factors weighted in the following order: (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of the information from other sources; (3) the total cost of production, compared to the amount in controversy; (4) the total cost of production, compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake; and (7) the relative benefits to the parties of obtaining the information.

Applying these rules, the court ordered UBS to produce, at its own expense, all e-mails existing on its optical disks or active servers, in addition to responsive e-mails from any five backup tapes selected by Zubulake. UBS was also

ordered to prepare an affidavit detailing the search results, as well as the time and money spent, and the court would then conduct the appropriate cost-shifting analysis.

Under ECPA, Consent to Interception Cannot Be Inferred From Mere Purchase of Service

In Re Pharmatrak, Inc. Privacy Litigation, No. 02-2138 (1st Cir. May 9, 2003)

Pharmatrak, a now-defunct company that collected internet information, contracted with several pharmaceutical companies to monitor their website traffic and compare it to other intra-industry websites. According to the original contracts, the pharmaceutical companies specifically stated that they did not want any personal or identifiable information about their website visitors collected. Despite those instructions, Pharmatrak collected personal information that could identify some individuals who had visited the website. Those individuals subsequently filed a class action suit against Pharmatrak and several pharmaceutical companies in U.S. District Court for the District of Massachusetts for violating the privacy protections under the Electronic Communications Privacy Act (ECPA). The District Court granted summary judgment for Pharmatrak, finding that the pharmaceutical companies had consented to the placement of code on their websites. Plaintiffs dismissed the suit as to the pharmaceutical companies and appealed the ruling as to Pharmatrak.

The First Circuit Court of Appeals, noting that although the ECPA requires that a plaintiff show the following five elements: the defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device, the Act does have a statutory exception for the giving

of consent. However, the court found that the district court incorrectly interpreted that consent exception in the instant case. Relying on *Griggs-Ryan v. Smith*, 904 F.2d 117 (1st Cir. 1990), the court stated that consent can only be implied when the surrounding circumstances convincingly show that the other party knew about and consented to the exception. Knowledge of the capability alone cannot be considered implied consent. The court noted that the pharmaceutical companies had sought assurances from Pharmatrak that they would not collect personal information from site visitors; when they discovered that Pharmatrak had not complied, they severed the relationship. Additionally, the court found that that Pharmatrak did intercept communications that were protected under the ECPA without consent because Pharmatrak's collection of personal information had occurred simultaneously with the users' communication with the pharmaceutical website. The case was reversed and remanded for further proceedings, particularly on the issue of whether Pharmatrak's interceptions were intentional as defined by the ECPA.

Anonymous Hacker's Search of Defendant's Computer Files Did Not Implicate Fourth Amendment Because Hacker Was Not Agent of Government

United States v. Steiger, 318 F.3d 1039 (2003)

The Montgomery, Alabama Police Department received an e-mail from an anonymous source about a child molester the source had found on the Internet with an electronic image attachment containing a picture of a male sexually abusing a female child. In his second e-mail, the source, who disclosed that he was in Turkey, identified the molester as Brad Steiger and provided Steiger's Internet service account information with AT&T WorldNet, a possible home address, the telephone number used to connect to the Internet and a fax number, along with more images of sexual abuse.

A third e-mail from the source contained some IP addresses used by Steiger on specific dates. The police referred the case to an FBI agent, who verified the details the source provided in the first two e-mails and then issued a subpoena to AT&T WorldNet, who advised that the Internet account was registered to a Brad Steiger at the same home address the source provided. The agent then obtained a photo of Steiger from an Alabama driver's license check and concluded that it was identical to the male depicted in the images sexually abusing young girls. A security officer at Steiger's place of work also identified the photo as Steiger. The agent next prepared an affidavit in support of a search warrant, stating that an anonymous source had located the child molester on the Internet, describing the pictures the source had sent and detailing the steps taken to corroborate the information. The affidavit did not mention that the source had obtained the evidence by hacking into Steiger's computer. The warrant issued, and law enforcement seized Steiger's computer and related equipment, as well as leg restraints, clamps and a blindfold. A federal grand jury returned an indictment against Steiger, charging violation of federal statutes involving sexual exploitation of minors.

Steiger filed several motions to suppress, claiming that the evidence asserted in support of the warrant was obtained in violation of the Fourth Amendment; that the FBI agent intentionally omitted material evidence from the affidavit by not mentioning that the source obtained the evidence by hacking; and that the information obtained by the source was inadmissible under the Wiretap Act. The U.S. District Court for the Middle District of Alabama denied the motions to suppress, reasoning that there was no proof that the source was a government agent and, therefore, his acts did not implicate the Fourth Amendment. Further, the Wiretap Act does not include suppression as a remedy because the suppression provisions do not refer to electronic

communications. A jury found Steiger guilty on several of the charges, and the court sentenced him to 210 months in prison and three years of supervised release. Steiger appealed.

The U.S. Court of Appeals for the Eleventh Circuit agreed with the district court that the Fourth Amendment was not implicated because there was no evidence that the government had any pre-knowledge of the search. The court also rejected Steiger's argument based on the FBI agent's failure to include the method in which the source obtained the information. The court noted that to justify suppression of evidence seized under a warrant, the alleged deliberate or reckless failure to include material information in the affidavit must conceal information that would defeat probable cause, as was not true in the instant case. Furthermore, because information obtained by a private person is not subject to the Fourth Amendment's exclusionary rule, a statement that the anonymous source had hacked into Steiger's computer would not have affected the finding of probable cause. As to the Wiretap Act, which applies to private conduct as well as to government agents, the court held that the anonymous source did not intercept electronic communications in violation of the Act because Steiger's computer did not contain any electronic communication service; only stored communications were accessed. The court also agreed with the district court that the Wiretap Act provides no basis for moving to suppress the intercepted electronic communications. The judgment of the district court was affirmed.

Note: The Cybercrime Project thanks AAG Vince Carroll of the Alabama Attorney General's Office for providing us with the cite to this case

LEGISLATIVE NEWS

STATES CRACK DOWN ON SPAM

Oklahoma Governor Brad Henry has signed Senate bill 660 into law, making it illegal to put false or misleading information in the subject line of an e-mail or to use a third party's Internet address or domain name without their consent for the purpose of making it appear that the third party sent the e-mail. The law also requires the sender to include a return e-mail address or a toll-free telephone number so that individuals could request that they not receive further communication from that sender. Additionally, e-mail containing sexually explicit material will be required to include "ADV-Adult" in the first 10 characters of the subject line. Violators will be subject to a misdemeanor offense, plus court costs and damages.

Virginia Governor Mark Warner signed into law an anti-spam bill that establishes five-year prison terms and other criminal penalties against chronic, large-scale e-mailers. Under the statute, penalties against spammers become felonies if the e-mail volume exceeds 10,000 messages in a 24-hour period or 100,000 messages over a 30-day span. The law also makes it a felony if revenue raised from a single transmission exceeds \$1,000, total revenue exceeds \$50,000 or if a minor is hired to assist in sending spam.

The **U.S. House Financial Services Committee** has favorably reported H.R. 2143, the Unlawful Internet Gambling Act, which prohibits financial institutions from processing transactions from Internet casinos. However, it purposefully does not contain any enforcement provisions that would require the bill to go through the Judiciary Committee. Under the measure, federal regulators

and the Federal Trade Commission would have six months from enactment to develop policies that would identify financial institutions that were processing Internet wagers and prevent those actions. The legislation is scheduled to come to the full House floor for debate.

PROTECT ACT SIGNED BY PRESIDENT

President Bush signed S.151, the Prosecutorial Remedies and Other Tools to end Exploitation of Children Today (PROTECT) Act, which deals with crimes against children, on April 30, 2003. In addition to authorizing a nationally coordinated system to replace the AMBER alert systems, the bill, now Public Law 108-21, also ends a distinction under previous law that allowed defendants in child pornography cases to claim sexually explicit information did not involve real children, but rather computer-simulated ones. The new law makes it a crime to pander or solicit images that are "virtually indistinguishable" from those of actual minors. However, it does allow defendants to introduce evidence that the alleged child pornography was not produced using actual minors, but either through computer technology or by using adults.

The new law also expands law enforcement's wiretap and electronic surveillance capabilities in investigations of child pornography, in addition to boosting the maximum penalty from 15 to 20 years for shipping, receiving or distributing child pornography or any visual depictions of minors engaged in sexually explicit activity.

LEGISLATION TO WATCH

The **California** Senate approved legislation which, if enacted, would be one of the strictest **anti-spam** measures in the country. The bill would make it illegal to send unsolicited e-mail advertising by requiring Internet marketers to get advance approval from e-mail recipients if they do not already have a business relationship with them. Currently, California law requires spammers to stop sending e-mails upon the recipient's request or face a \$1,000 fine. This new "opt-in" measure puts the burden on Internet marketers to get approval to spam customers rather than forcing people to ask to be removed from the spam list after the fact. The bill would also allow consumers to sue spammers for \$500 per unwanted message, and a judge could triple the fine if it is determined that the sender willfully and knowingly violated the law. The bill now goes to the State Assembly. Governor Gray Davis has taken no position on the bill to date.

The **Ohio** Senate has given final approval to an **anti-cyberstalking** bill that prohibits stalking or harassing someone repeatedly through electronic means, including e-mail or message boards. In most cases, the bill would make cyberstalking a first-degree misdemeanor, punishable by up to 180 days in jail and a maximum \$1,000 fine. However, if the victim is a minor or was threatened with physical harm or if the stalker has a history of violence, the crime would be a fourth-degree felony, punishable by six to 18 months in jail and a fine of up to \$5,000. Posting false information on the Internet, causing another person to stalk an individual, would also be illegal. The bill now goes to Governor Bob Taft.

The **Texas** Senate has passed S.B. 405, a comprehensive bill designed to protect consumers against **identity theft**. The measure gives the state attorney general authority to assess civil penalties for individuals convicted, and would also allow a

victim of identity theft to recover attorney's fees. Additionally, cases could be prosecuted in the county where the victim resides or in any county where the theft was committed. Under the measure, businesses would be required to maintain procedures to protect and safeguard personal identification information received, and receipts for merchandise cannot contain more than the last four digits of the customer's debit or credit card number. The legislation, titled the Identity Theft Enforcement and Protection Act, now goes for consideration to the State House.

The **U.S. House Judiciary Subcommittee on Commercial and Administrative Law** has approved H.R. 49 which would permanently extend a **moratorium on certain Internet-related taxes** that expires on November 1 of this year. The bill would permanently ban taxes on Internet access, prohibit taxes that treat Internet purchases differently from other sales and ban the double taxation of online purchases. Those restrictions have been in place under a moratorium enacted by Congress in 1998. The bill would also eliminate a "grandfather" clause in the existing law that exempted nine states that taxed Internet access before the moratorium was enacted. The White House has pressed for speedy passage of the legislation, and a full committee mark-up is expected in June. A Senate companion bill S. 52 and S. 150, a similar measure, are pending in the Senate Commerce, Science and Transportation Committee.

CYBERCRIME NEWS

CONGRESS SETS UP CYBERSECURITY PANEL

The U.S. House of Representatives has established its first panel devoted to cybersecurity.. The new 50-member House Homeland Security Committee, chaired by Chris Cox (R-CA) voted at its kickoff meeting to create five subcommittees: border security, emergency preparedness, counterterrorism (led by Jim Gibbons (R-NV), internal committee rules and a fifth that will oversee the federal government's efforts relating to cybersecurity (led by Mac Thornberry (R-TX). Former CIA Deputy Director John Gannon will serve as the committee's staff director. The U.S. Senate does not have a parallel effort, although its subcommittee on technology, terrorism and government information has similar duties.

GOVERNMENT REPORTS: ONLINE PORNOGRAPHY WIDESPREAD

Two government reports warn that pornography is rampant on file-swapping networks. The General Accounting Office (GAO) study, based on Internet searches using such words as "preteen," "underage" and "incest," found that about 42% of the sites were associated with child pornography images, with an additional 34% classified as adult pornography. Only 24% of the results could be classified as non-pornographic. The second report, prepared by staff from the House Government Reform Committee concluded that blocking technology has limited ability to block access to pornography via file-sharing programs.

STUDY: FEDERAL AGENCIES LAX IN PROTECTING SOCIAL SECURITY NOS.

The Social Security Administration's Inspector General has released a report finding that federal agencies have been lax in ensuring that citizens' Social Security numbers are kept confidential from private firms providing government services. The Inspector General's study found that 14 of the 15 agencies examined had inadequate controls over their access and use. In one case, private contractors were keeping personal identification information in unlocked cabinets, storage rooms and on desktops. The study was requested by Clay Shaw (R-FL), head of the House Ways and Means subcommittee on Social Security and Susan Collins (R-ME), head of the Senate Governmental Affairs Committee.

STANDARDS BODY TO FIGHT SPAM

The Internet Engineering Task Force (IETF), the influential NET standards body, has formed an Anti-Spam Research Group (ASRG) which will first develop a consistent definition for spam, to be followed by development of a mechanism whereby users can express consent or lack of consent for certain communications and have the architecture support that intent. The ASRG will not look into the legal aspects of fighting spam, except when these issues affect the technical approaches. Additional information about the effort can be accessed at <http://www.irtf.org/charters/asrg.html>

FTC: 2/3 OF SPAM IS FALSE

The Federal Trade Commission, studying a random sample of 1,000 unsolicited e-mails for deceptive claims in the text, "from" or "subject" lines, has concluded that two-thirds of the "spam" messages probably are false in some way. Of the

e-mails studied, one-third contain false information in the “from” line, obscuring the true identity of the sender. Spam involving business opportunities, such as work-at-home or franchise offers, accounted for 20 percent of the spam studied; offers for pornography or dating services accounted for another 18 percent, and spam involving pitches for credit cards, mortgages and insurance was the third largest category at 17 percent.

INTERNET FRAUD COMPLAINTS TRIPLED IN 2002

The FBI’s Internet Fraud Complaint Center (IFCC),* which was launched in May 2000 and is managed in part by the National White Collar Crime Center, announced that it had referred 48,252 complaints to law enforcement authorities last year, which is nearly three times the number of complaints referred in 2001. The monetary loss associated with the fraud more than tripled from \$17 million to \$54 million. Auction fraud accounted for the most complaints, as it has for the past two years, with 46%; nondelivered merchandise and nonpayment accounted for 31% of referred complaints, and credit or debit card fraud was third at about 12%. The highest median monetary loss was \$3,864 for those complaining about the Nigerian letter fraud. People who claimed to be victims of identity theft lost an average of \$2,000, and those suffering check fraud lost a median of \$1,100.

*The responsibilities of the IFCC were presented by Tom Sadaka, Special Counsel for Computer Crimes and Identity Theft Prosecutions in the Office of the Attorney General of Florida, at the Basic Cybercrime Training given by NAAG and the National Center for Justice and the Rule of Law in May.

EXECUTIVE ORDER ALLOWS INFRASTRUCTURE DATA TO BE CLASSIFIED

President Bush has signed an executive order that changes the definition of what the government may classify as confidential, secret and top-secret to include details about “infrastructures” and weapons of mass destruction. The order also makes clear that information related to “defense against transnational terrorism” is classifiable. The order, which replaces a 1995 directive signed by President Bill Clinton, allows information that already has been declassified and released to the public to be reclassified by a federal agency. The 1995 order did not allow such reclassification.

Written and Edited by Hedda Litwin, Cybercrime & Violence Against Women Project Counsel, (202) 326-6022, hlitwin@naag.org

Formatted by Arika Pierce, Project Assistant, (202) 326-6262, apierce@naag.org

The Cybercrime Newsletter is developed under the Cybercrime Training Partnership between the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL) at the University of Mississippi School of Law.

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.

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.

