



National Association  
of Attorneys General

# CYBERCRIME NEWSLETTER

Issue 6

February/March 2004

## News Highlights in this Issue

Web Businesses Lobby Against Utah Spyware Bill .....	10
Search of Employee E-Mails does Not Violate ECPA .....	7
California E-Voters to Get Paper Receipt .....	13
“Internet Sex Crimes Against Minors” Report Available .....	9
Four States Enact Laws Against Digital Taping in Movies .....	10
Iowa Launches Citizens’ Web Site .....	13
Law Enforcement Cannot Eavesdrop on Onstar Cars .....	7
New York, California Seek Internet Sales Tax .....	12
Georgia Prisons Give Inmates Computers for Appeals .....	14
IBM Leads in Patents Granted in 2003 .....	17
Search of CD Violated Fourth Amendment .....	8
Over 50% of Federal Agencies Flunk Security Test .....	17
Microsoft Offers Reward for MyDoom.B Leads .....	15

## Table of Contents

<b>Features</b> .....	2
Main Task Force Fights Cybercrime	
<b>Counsel Position Available</b> .....	18
<b>AG Initiatives</b> .....	4
Arizona AG Presents Internet Safety Program	
Attorney General Salazar Creates ID Theft Web Site	
Illinois AG Sues Online License Plate Seller	
Attorney General Kline Charges Online Tractor Vendor	
Maryland AG Orders Web Site Seller to Stop Selling Adult Sites	
AG Cox Charges Deputy with Sending Porn	
Missouri AG Stops Fraudulent Online Sales	
Nevada AG Ends Sham Online Sale of Art	
Attorney General Spitzer Settles With PayPal	
AG Heed Unveils Online Safety Program	
AG Edmondson Halts Online Sales Fraud	
Oregon AG Files Against Online Tobacco Sales	
AG Abbott Gets Commitment to Children Award	
<b>In the Courts</b> .....	7
Eavesdropping on Onstar Cars Prohibited	
Search of Employee E-Mails Doesn’t Violate ECPA	
Bailee’s Consent Not Enough for CD Search	
<b>Legislation</b> .....	10
Four States Ban Digital Taping in Movies	
Web Publishers Lobby Against Utah Spyware Bill	
Nanotechnology Research Funding Bill Enacted	
Database Protection Bill Passes Judiciary Committee	
House Committee Asks Drug Cos. About Illicit Sales	
<b>News</b> .....	12
New York, California Seek Internet Sales Tax	
UN Urges Action Against Internet Drugs	
Iowa Launches Citizens’ Web Site	
FBI Announces “John Doe” Child Pornography Effort	
California E-Voters to Get Paper Receipt	
FCC Releases Net Phone Guidelines	
Georgia Prisons Give Inmates Computers for Appeals	
Four ISPs Sue Major Spammers	
ICANN Approves Domain “Wait-Listing”	
Six User Groups Accepted by ICANN	
Microsoft Offers Reward for MyDoom.B Leads	
President Urges Cybercrime Treaty Ratification	
FCC Expands Wireless Net Frequencies	
UN, Microsoft Partner to Help Poor Countries	
50% of Federal Agencies Flunk Security Test	
IBM Again Leads in Patents Granted	
<b>Publications Available</b> .....	9
“Internet Sex Crimes Against Children” Report	
“Test Results for Disk Imaging Tools”	
“ISTEP II Case Studies”	
“Test Results for Software Write Block Tools”	

---

## IFCC and the Maine Computer Crimes Task Force Partner to *Drop a Dime on Cyber Crime*

By Michael L. Webber

---

### **Partnerships**

In the field of law enforcement, partnerships are crucial in our efforts to fight crime. Since the formation of the Maine Computer Crimes Task Force in 1999, its members have recognized that no one agency can alone fight Internet crime or crimes involving computers. Partnerships are necessary, and resources need to be pooled.

### **The National White Collar Crime Center (NW3C) and the FBI recognize this as well.**

Since 2000, the two agencies have partnered and co-managed the Internet Fraud Complaint Center (IFCC), a Web-based initiative that receives citizen complaints regarding online crimes such as auction fraud, credit card fraud, identity theft, investment fraud and child pornography. Since 2001, the IFCC has received over 119,000 citizen complaints from around the globe. In the first nine months following the attacks of September 11, 2001, when the IFCC turned its Web site into a terrorist tip portal, over 303,000 tips on terrorism were submitted to the IFCC staff. This provided the FBI with significant leads that enabled it to preempt certain terrorist activities subsequent to September 11. The IFCC partnership has been so successful that the Royal Canadian Mounted Police is working with NW3C to duplicate the program in Canada.

### **A Local Approach to Internet Crime and Crimes Involving Computers**

The Maine Computer Crimes Task Force (MCCTF) is a partnership comprised of representatives of state, local and federal law enforcement. The Maine Office of the Attorney General is a key collaborator in the MCCTF providing legal guidance and investigative support. The MCCTF is a member of the Northern New England Internet Crimes Against Children Task Force, which is comprised of law

enforcement in Maine, New Hampshire and Vermont. The primary mission of the MCCTF is investigating and assisting those Maine law enforcement agencies that investigate crimes involving computers. It accomplishes this through law enforcement training, public outreach and investigations. The task force hosts two computer forensic labs located strategically in the state, and has been involved in virtually every computer crime investigation in Maine since 1999. Over 500 computers have been forensically examined since the unit's inception; more than 674 cases have been investigated ranging from homicide and extortion to drug trafficking, computer intrusion, identity theft, bank fraud and child exploitation; and over 506 calls for technical assistance have been answered by task force staff.

### **Drop a Dime on Cyber Crime**

About the same time the IFCC was launched, the Maine Computer Crimes Task Force initiated a similar program. The program, *Drop a Dime on Cyber Crime*, featured a Web-based reporting form that encouraged Maine residents to report Internet or computer crimes directly to staff at the task force. The program was somewhat cumbersome, though, in that it asked consumers to report Internet crimes against children directly to the National Center for Missing and Exploited Children and sometimes referred the complainants directly to the IFCC. Complaints were received by the unit supervisor via e-mail and were analyzed only as time allowed. The information submitted by the complainant was cross-checked only against task force or local police records, and referrals to other law enforcement agencies sometimes took weeks. Though hampered by these limitations, the program enjoyed some success.

### **Collaboration, the Key to Success**

In July of 2003, Maine's *Drop a Dime on Cyber*

---

*Crime* program underwent some major changes. Working with NW3C, the program was modified to allow the submission of citizen complaints directly to IFCC staff via the Maine Computer Crimes Task Force Web page. Instead of the complaint being forwarded to task force supervisors for analysis, the report goes directly to analysts at the IFCC. Once received, IFCC staff examines the report, compares it against citizen reports from all over the world, and then forwards it to the most appropriate law enforcement agency or agencies. Unlike the earlier version of *Drop a Dime on Cyber Crime*, visitors are no longer being re-directed if they wish to report crimes against children. A report may be filed directly through the task force Web site and, upon receipt by the IFCC, the report will be immediately forwarded to the National Center for Missing and Exploited Children. In all cases, staff at the Maine Computer Crimes Task Force will maintain copies of the report for local analysis and record keeping, and program statistics will be available in real time.

In Maine, our partnership with NW3C has been of great benefit. The NW3C, which is a non-profit, membership-affiliated organization comprising law enforcement agencies, state regulatory bodies with criminal investigative authority and state and local prosecution offices, offers its service and support efforts across state

boundaries, bringing agencies together to provide an effective response to combating economic and high-tech crime. Members benefit from several support services with their cost-free affiliation to NW3C, including financial investigations and cyber crime training, analytical services, case funding, database searches, Internet Fraud Complaint Center (IFCC) referrals and research and information resources. The Maine Office of the Attorney General has been a voting member of the NW3C for several years. Both investigators and prosecutorial staff have benefited tremendously from NW3C training on economic and cyber crimes. Law enforcement agencies can begin the process of membership by contacting NW3C at [www.nw3c.org](http://www.nw3c.org) or by calling (800) 221-4424, ext. 345.

---

***About the Author***

*Detective Michael L. Webber works for the Maine Office of the Attorney General. Prior to joining the Maine Office of the Attorney General, he worked full time with the Maine Computer Crimes Task Force coordinating its Internet Crimes Against Children Program. He is a certified forensic computer examiner and still remains a member of the task force policy board. You can reach him at [michael.l.webber@maine.gov](mailto:michael.l.webber@maine.gov). You can view the Maine Computer Crimes Task Force Web site at [www.mcctf.org](http://www.mcctf.org) and the Office of the Attorney General Web site at [www.maine.gov/ag](http://www.maine.gov/ag)*



# AG Initiatives

---

## ATTORNEY GENERAL INITIATIVES

### ARIZONA

**Attorney General Terry Goddard** presented an Internet safety program on February 7, 2004. The forum utilized information from NetSmartz and the National Center for Missing and Exploited Children. Hands-on activities were also provided for teens and younger children. Assistant Attorney General Gail Thackeray participated in the program.

### COLORADO

**Attorney General Ken Salazar's** office has created a new Web site page, found at [www.ago.state.co.us](http://www.ago.state.co.us), to provide comprehensive information on how to protect oneself from becoming a victim of identity theft and practical steps about what to do if one becomes a victim. A key feature of the *Colorado Attorney General's Identity Theft Website* is step-by-step guidance to victims, including a searchable database to help consumers locate the law enforcement agency in their community should they need to file an identity theft report. Other topics on the site include information for businesses, assistance for law enforcement, prevention tips, Colorado and federal statutes relating to identity theft and information on who can require social security numbers.

### ILLINOIS

**Attorney General Lisa Madigan** filed a lawsuit against Chan Briggs of Minnesota who allegedly sold non-expired Illinois license plates through various Web sites, including eBay. Briggs is charged with numerous violations of the Illinois Consumer Fraud Act and the Illinois Motor Vehicle Code. While most of the plates were expired and supposedly purchased by collectors, some of the

Illinois plates Briggs sold were valid at the time of sale, leading to concerns that they could be used to falsify or hide the identity of a person committing crimes. Because of these concerns, eBay prohibits the sale of plates less than five years old, but Briggs allegedly got around that ban by advertising the plates as 1996 or 1997 issues. In fact, they were newer Abraham Lincoln plates first distributed in 2000. The Chicago Police Department made several undercover purchases of the non-expired plates from Briggs and alerted General Madigan's office. Police investigators purchased 42 Illinois license plates, of which at least 14 were valid. General Madigan is seeking full restitution, a \$50,000 civil penalty, additional penalties of \$50,000 per violation of the Consumer Fraud Act and injunctive relief. Assistant Attorney General Adam Sokol is handling the case.

### KANSAS

**Attorney General Phil Kline** charged Greg Jackson with allegedly defrauding several individuals out of thousands of dollars over the Internet. Jackson was charged with ten counts of theft by deception and eight counts of computer crimes for allegedly receiving money for tractors offered for sale through online auction sites without delivering the items as agreed. Jackson has also been charged with one count of sale of a vehicle without transfer of certificate of title for allegedly selling a car without providing the title at the time of delivery or within the time allowed by law. Computer crime is a level eight felony punishable by a sentence of five to 17 months and fines of up to \$100,000 per violation. Theft by deception is a level nine felony punishable by a sentence of seven to 23 months and fines of up to \$100,000 per violation. Sale of a vehicle without transfer of certificate of title is a misdemeanor punishable by 30 days to six months imprisonment in county jail and/or a fine not to exceed \$2,500. Assistant Attorney General Lee Davidson will prosecute the case.

---

## MARYLAND

**Attorney General Joseph Curran's** Securities Division issued a Summary Order to Cease and Desist against Jean DeFague, charging him with violating the antifraud, registration and disclosure provisions of the Maryland Business Opportunity Sales Act by selling adult Web site "business opportunities" from his home computer. According to the order, DeFague advertised the adult website businesses on eBay, telling prospective buyers that he would sell them a website domain name, adult content, site support and ongoing assistance to allow them to operate the websites profitably. In some cases, DeFague guaranteed buyers that they could earn as much as \$500 per week through subscriptions. Some buyers paid DeFague \$3,000 or more, but never received what was promised and never heard from him again. The order charges DeFague with defrauding buyers, making misrepresentations about the website business opportunity, failing to register with the Securities Division and failing to provide disclosure to prospective buyers. According to the order, DeFague must immediately cease and desist offering or selling business opportunities in or from Maryland, pending a hearing.

## MICHIGAN

**Attorney General Mike Cox** announced that Matthew Guy, a sheriff's deputy, was charged with sending sexually explicit photos via a web cam to an online person he thought was a 14-year-old boy, as well as trying to entice the persona to meet him for sex. The "boy" was actually a New Jersey police officer. Guy was charged with two counts of using a computer to commit a crime; each count carries a maximum sentence of 10 years in prison. Guy was also charged with three counts of distributing obscene material to a child; each count is a four-year felony.

## MISSOURI

**Attorney General Jay Nixon** announced that Joseph Merkle pleaded guilty to five criminal counts of consumer fraud related to the sale of computer equipment over the Internet. General Nixon and Miller County Prosecuting Attorney Robert Seek had filed charges against Merkle last year. Merkle advertised computers and computer equipment for sale and instructed consumers to wire

money to him, but failed to send the merchandise or refund the money. Sentencing for Merkle is scheduled for April 15, 2004. He faces a maximum of four years in prison and a \$5,000 fine on each count.

## NEVADA

**Attorney General Brian Sandoval** announced that Susan Christine Thomas was sentenced to a term of not less than 24 months or more than 60 months in Nevada State Prison, such term to be suspended. The sentencing followed Thomas' guilty plea to felony theft by obtaining money under false pretenses. Thomas paid \$17,000 of the total ordered restitution of \$63,392 and was placed on probation subject to terms including monthly restitution payments and prohibition from conducting transactions over the Internet. General Sandoval's Bureau of Consumer Protection had filed a six-count felony complaint against Thomas, alleging that she placed high value art up for bid on the online auction site eBay. Although she told bidders that she would ship the art to them within seven to ten days after receiving payment, and would also include appraisals and Certificates of Authenticity, Thomas failed to send the art work and refused to provide refunds. Each victim paid between \$2,750 and \$12,650 for the art.

## NEW YORK

**Attorney General Eliot Spitzer** announced an agreement that will require PayPal, the nation's largest online payment service, to better disclose the rights of account holders when an affiliated merchant fails to deliver merchandise. An investigation by General Spitzer's office revealed that PayPal's "User Agreement" misrepresented certain terms and conditions to account holders, including a statement that it afforded its account holders "the rights and privileges expected of a credit card transaction." In practice, consumers were often denied these rights by PayPal. Under the agreement, PayPal must clearly describe account holder rights in its User Agreement, including any conditions or limitations to these rights, and reversal or refund policies. The company will pay New York State \$150,000 as penalties and costs of investigation.

The case was handled by Assistant Attorney General Kenneth Dreifach, Chief of General Spitzer's Internet Bureau.

---

## NEW HAMPSHIRE

**Attorney General Peter Heed**, together with Governor Craig Benson and Education Commissioner Nicholas Donohue, unveiled the NetSmartz Workshop computer program to educate children about the dangers of the Internet. The program was developed by the National Center for Missing and Exploited Children with the Boys and Girls Club of America. It uses computer animation and games, with four levels for different ages from kindergarten to high school. The program will be sent to seven schools in the state as part of a pilot program. In addition, parents and teachers in any school will be able to download the program and supplemental materials from a new Web site.

## OKLAHOMA

**Attorney General Drew Edmondson** announced that two people accused of selling items on their business Web site but failing to deliver the products were ordered to pay restitution totaling more than \$40,000 after pleading guilty in court. Tonya and Michael Ketchum had been charged with nine counts of violating Oklahoma's Consumer Protection Act after an investigation by General Edmondson's consumer protection unit. According to the state's complaint, the Ketchums ran a Web site advertising farm, lawn and garden equipment and truck accessories. They received payment for the equipment from consumers in Connecticut, Colorado, Wyoming, North Carolina, Pennsylvania, California, New York and Michigan, but the consumers never received the products they purchased. Both Ketchums received a five-year deferred sentence on each count with counts two through nine to run concurrently. They were also ordered to pay court costs and a victims' compensation assessment, and

---

each was ordered to pay \$20,133.25 in restitution.

## OREGON

**Attorney General Hardy Myers** filed a stipulated judgment against a Missouri Internet tobacco seller, [www.dirtcheapcig.com](http://www.dirtcheapcig.com), that he sued for allegedly selling cigarettes on the Internet to an Oregon minor. Under the judgment, the company admits no liability and agrees to comply with the new Sales and Delivery Restrictions Law in Oregon, which became effective on January 1, 2004 and bans the sale of cigarettes and tobacco products to a person under 18 years of age. The company also paid General Hardy's office \$15,000 for its consumer protection and education revolving fund.

## TEXAS

**Attorney General Greg Abbott** received the Commitment to Children Award from the Center for Child Protection (formerly the Children's Advocacy Center) for his initiative and commitment to protecting Texas children. Among other achievements, General Abbott spearheaded the Cyber Crimes and Fugitives units, which together have been responsible for the arrests of nearly 90 people in connection with child sex crimes. Most recently, Cyber Crimes Unit investigators made three more child predator arrests, including two men who are in the military. All were charged with attempted sexual assault of a child, a felony, and are being held on bond in county jails.

---



# In The Courts

## IN THE COURTS

### **Law Enforcement May Not Eavesdrop on Conversations in Automobiles Equipped With Onstar or Like Computing Systems**

*The Company v. United States*, No. 02-15635 (9<sup>th</sup> Cir., Nov. 18, 2003)

Under 18 U.S.C. 2518(4), a provider of wire or electronic communication service must provide law enforcement with the assistance necessary to accomplish wiretapping or eavesdropping interception with “a minimum of interference to services” when directed by a court order to do so. Upon request by the FBI, the U.S. District Court for the District of Nevada issued several *ex parte* orders requiring the Company to assist in intercepting oral communications in a particular vehicle equipped with a communications system. The Company complied with only one of the orders, and the government filed a Motion to Compel and for Contempt. The Company responded by filing motions for reconsideration and to quash or modify the court’s order. The district court found that the Company is a “telecommunications carrier” and “provider of wire or electronic communication service” within the scope of 18 U.S.C. § 2518(4) and § 2522; that the FBI’s request and the court order were not unreasonable; that the Company’s due process rights had not been violated; and that no “taking” had occurred. The court denied the Contempt motion, but ordered the Company to comply. It also denied all of the Company’s motions. The Company appealed.

Finding that the Company had an obligation within the meaning of the statute, the 9<sup>th</sup> Circuit then addressed the question of whether the order went too far in interfering with the service the Company provided by preventing the Company from supplying the System’s services to its customer when a vehicle was under surveillance. The Court found that FBI surveillance in the instant case completely disabled the monitored car’s System. The only operative function was the automatic emergency response signal. However, the Court noted that no one at the Company was monitoring for such a signal because the call was transferred to the FBI. The result was

that the Company could no longer supply any of the services it had promised its customer, including assurance of response in an emergency. The court found that the level of interference with the System resulting from the FBI’s surveillance was far beyond the “minimum of interference with the services” required by the statute. The court thus reversed the order of the district court.

### **Employer’s Search of Employee’s E-Mails Does Not Violate ECPA and Parallel Pennsylvania Statute Because of Communications Service Provider Exception**

*Fraser v. Nationwide Mutual Insurance Co.*, No. 01-2921 (3<sup>rd</sup> Cir., December 10, 2003)

Fraser, an independent insurance agent for Nationwide, was terminated, although the parties disagree on the reason. Fraser contends that he was terminated because of complaints he filed with the Pennsylvania Attorney General’s Office regarding Nationwide’s alleged illegal conduct. (*Note: As a result of these complaints, Nationwide was required to pay fines and entered into a consent order*). Nationwide argues that he was terminated for disloyalty because of a letter Fraser drafted to two competitors in which he sought to determine whether they would be interested in acquiring the policyholders of agents belonging to an association in which he was an officer. Fraser claimed that the letters were never sent; however, Nationwide claimed that they became concerned that Fraser might also be revealing company secrets. Nationwide therefore searched its main file server for any e-mail to or from Fraser that showed improper behavior. On the basis of the letters and the e-mail search, Nationwide terminated Fraser. Fraser filed suit in the U.S. District Court for the Eastern District of Pennsylvania to contest the alleged violation of his privacy rights under the Electronic Communications Privacy Act (ECPA) and parallel Pennsylvania statute, 18 Pa. Cons. Stat. § 5702 *et seq.* (*Note: Fraser’s suit contained three other claims, but this analysis will only cover the ECPA claim*). The District Court granted summary judgment for Nationwide, and Fraser appealed.

Fraser argued that, by accessing his e-mail on its central file server without his express permission, Nationwide violated Title I of the ECPA, which prohibits “intercepts” of electronic communications such as e-mail. However, the Third Circuit disagreed, finding that an “intercept” under Title I of the ECPA must occur contemporaneously with transmission (*Note: every circuit court to have considered this issue has agreed*), and Nationwide did not access Fraser’s e-mail at the initial time of transmission. Fraser also argued that Nationwide’s search of his e-mail violated Title II of the ECPA, which creates civil liability for one who “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.” 18 U.S.C. § 2701(a). The court noted that 18 U.S.C. § 2701(c)(1) excepts from Title II seizures of e-mail authorized “by the person or entity providing a wire or electronic communications service.” While there was no circuit court case law interpreting this exception, this court read § 2701(c) to except all searches by communications service providers. Thus, they held that, because Fraser’s e-mail was stored on Nationwide’s system, which it administered, its search of that e-mail fell within this exception to Title II. The district court’s grant of summary judgment was affirmed.

#### **Law Enforcement Officers’ Search of Computer Disc, Based Upon Bailee’s Consent, Violated Fourth Amendment**

*United States v. James*, No. 03-2506EM (8<sup>th</sup> Circ., December 23, 2003)

James was arrested in his home state of Illinois on a Missouri warrant alleging he had engaged in sexual misconduct with a child, in violation of Missouri state law. While in jail awaiting extradition to Missouri, he attempted to smuggle out a letter to his friends by giving the letter to another inmate, who then gave it to his lawyer to mail. The lawyer read the letter instead and, believing it to contain evidence of a crime, contacted an assistant state attorney, who then forwarded it to

the Missouri attorney responsible for prosecuting James on the sexual misconduct charges. The letter instructed James’ friends to call Michael Laschober and tell him to destroy all backup CDs in his possession because one has a virus. Believing that the discs might be of value to his case, that attorney sent two detectives to Laschober’s home. Laschober told the detectives that James often brought him computer discs to store and had recently delivered some more. He said James did it for safety reasons as he was concerned that his own computer would crash. Upon request, Laschober retrieved the recent discs, which were in an envelope sealed with tape. Laschober said he believed the discs contained church and financial records, as the previous discs had been so marked. Upon request, Laschober allowed the detectives to open the envelope where they found ten discs, the top one reading “CD VIRUS DANGER, CONFIDENTIAL CLASSIFIED...” The detectives asked Laschober if they could take the discs, and he consented, signing a modified consent form. Back at the station, they had to use a sophisticated computer to open the discs, where they found digital images of child pornography. The detectives had never sought nor acquired a warrant to search or seize the discs.

James was charged with possession of child pornography. Before trial in the United States District Court for the Eastern District of Missouri, James moved to suppress the discs, arguing that the detectives had violated the Fourth Amendment. The Magistrate recommended that James’ motion be denied because 1) Laschober gave valid consent; 2) the police were justified in relying on Laschober’s apparent authority to consent; 3) the search was justified under the doctrine of abandonment; and 4) the evidence would have been discovered anyway under an alternative line of investigation. Although the Magistrate advised both parties that they had 11 days to object, James failed to do so, and the District Court subsequently accepted the Magistrate’s recommendation. James subsequently filed an objection, which the District Court denied as untimely. James was found guilty and sentenced to 57 months in jail and a \$10,000 fine. He appealed.

The 8<sup>th</sup> Circuit noted that while consent to search is a valid exception to the warrant requirement, it must be given by the suspect or by

some other person who has common authority over, or sufficient relationship to, the item to be searched. The court was convinced that James did not give permission to Laschober to exercise control over the discs or to consent to the searching because he marked the discs “confidential.” It also required a sophisticated computer to get access to the discs, all of which indicated that James’ expectation that Laschober not view its contents. Further, the court found that the detectives’ reliance on Laschober’s apparent authority was unreasonable because they had read the intercepted letter from James and knew that James’ only authority was to scratch and destroy the discs. The standard of reasonableness, according to the court, was governed by what the law enforcement officers knew, not what the consenting party knew. The court also found that James had not abandoned the property because he had never denied ownership of the discs, had put his name on the envelope and did not relinquish the discs in a manner that showed abandonment. Lastly, the court

addressed the argument of inevitable discovery doctrine, which posits that if the prosecution can establish by a preponderance of the evidence that the information, otherwise to be suppressed by the exclusionary rule, inevitably would have been discovered by lawful means, then the exclusionary rule does not apply. Here, the court noted that James had already been arrested on sexual misconduct charges, so the investigation appeared to be over.

Thus, the 8<sup>th</sup> Circuit found that the detectives’ behavior violated the Fourth Amendment, and the evidence should have been suppressed. At the time of the search, there was no valid exception to the warrant requirement justifying their behavior. The judgment of the District Court was reversed, and the case remanded.



## PUBLICATIONS

### CHECK OUT THESE PUBLICATIONS

- “Internet Sex Crimes Against Minors: The Response of Law Enforcement” provides an overview of the characteristics of Internet sex crimes committed against minors in the United States and how these cases are handled. The report was supported by the Office of Juvenile Justice and Delinquency Prevention and can be accessed at [http://www.missingkids.org/en\\_US/publications/NC132.pdf](http://www.missingkids.org/en_US/publications/NC132.pdf).

---

- “Test Results for Disk Imaging Tools: dd Provided with FreeBSD 4.4” presents results of a study that used dd, a disk imaging tool, in the UNIX-based FreeBSD 4.4 environment. It documents results against 22 test assertions (both mandatory and optional), describes the testing environment, interprets results and includes summary log files of 32 test cases. It can be accessed at <http://www.ncjrs.org/pdffiles/nij/2030095.pdf>.

- The goal of the ISTEP (Information Systems Technology Enhancement Project) is to develop written documentation, software systems and procedures that will increase the utilization of information and information technology in police departments. A copy of the “ISTEP II Case Studies” can be ordered from the U.S. DOJ Response Center at 1-800-421-6770.

- “Test Results for Software Write Block Tools: RCMP HDL V0.8” presents the results from testing the Royal Canadian Mounted Police Hard-Disk Write Lock V0.8 against Software Write Block Tool Specification & Test Plan, Version 3.0. It can be accessed at <http://www.ojp.usdoj.gov/nij/pubs-sum/203196.htm>.



---

# Legislation

---

## LEGISLATIVE NEWS

### DIGITAL TAPING IN CINEMAS

At Hollywood's urging, several states have passed laws against videotaping movies in theatres. Ohio's bill, signed into law by Governor Bob Taft in December 2003, has taken effect in March 2004, and gives movie theatres the right to detain people suspected of videotaping movies, just as a department store can hold a suspected shoplifter. A first offense in Ohio would be punishable by six months in jail and up to a \$1,000 fine. A similar law took effect on January 1, 2004 in California and, although the new charge is a misdemeanor, it still carries consequences of up to one year in jail and a \$2,500 fine. Wisconsin and Pennsylvania passed equivalent bills in 1999, and Michigan lawmakers introduced legislation in December 2003. Michigan's bill would set penalties of up to five years in prison and a \$250,000 fine. Charges under these state laws focus simply on the operation of the camera, thus avoiding the details of federal copyright law, and are thus easier to prosecute.

### SPYWARE CONTROL

Leading Web publishers and businesses have taken action to lobby against Utah's proposed Spyware Control Act, which has passed the Utah state House and Senate and awaits Governor Olene Walker's signature. Under the bill, any software that reports its users' online actions, sends personal data to other companies or serves pop-up ads without permission is prohibited. The bill does contain some exceptions, such as for "cookies" used for personalizing Web pages and ads served by HTML or JavaScript. The bill originated after a local online contact lens distributor,

1800contacts.com, contacted the legislature when it discovered that some of its customers had received pop-up ads while visiting its Web site. These ads were served by software-based marketing programs installed on users' computers, not by the company itself. Technology providers such as American Online, Amazon.com, Cnet, eBay, Google, Microsoft and Yahoo signed a letter on March 1, 2004 to Utah Senate Majority Leader John Valentine and Representative Steven Urquhart, who sponsored the bill, warning that the bill was overbroad and could interfere with computer security by preventing information technology and security companies from collecting data to analyze and prevent virus attacks.

### NANOTECHNOLOGY RESEARCH

Research on nanotechnology, which involves manipulating matter on the scale of one-billionth of a meter, got a funding boost under legislation signed into law by President Bush. S. 189, now Public Law 108-153, authorizes \$3.7 million for research into the science of creating microscopic computer technology for biological, mechanical and other uses. Applications for such research include encryption, defense technologies and development of artificial intelligence. The money authorized by the legislation, which was sponsored by Senators George Allen (R-VA) and Ron Wyden (D-OR), will flow to the National Science Foundation, the Department of Agriculture and other federal entities. The National Science and Technology Council will oversee management of the program. Additionally, the legislation calls for the White House to create a National Nanotechnology Coordination Office and a National Nanotechnology Advisory Panel.

---

## **DATABASE PROTECTION – UPDATE**

H.R. 3261, the database protection bill, has advanced and been approved by the U.S. House Judiciary Committee (in the last issue, we reported that the bill had passed a Judiciary subcommittee). The legislation would make it illegal for people to download proprietary databases and use the data for competitive or commercial purposes. The committee-approved bill is significantly different from the original version, notably due to the adoption of exemptions for students, researchers, scientists and Internet service providers. Additionally, the amended bill allows lower civil damages than the original measure, and has dropped criminal penalties altogether. At the request of the American Indian community, the bill also provides that state and local governments cannot sue tribal governments. Despite the changes, the controversial bill still pits industry groups against one another. Developers and sellers of databases such as Lexis-Nexis claim they need a federal law to prevent other businesses and customers from downloading information from the proprietary databases and reselling it for commercial use. Opposing the legislation are a range of businesses and organizations, such as Internet service providers and the U.S. Chamber of Commerce, who argue that the legislation is too broad and could create a property right that protects basic, publicly known facts. Researchers and libraries

oppose the bill because they believe the database owners could try to assert legal protection over factual data needed for their work.

## **ILLICIT ONLINE DRUG SALES**

The House Energy and Commerce Committee has sent letters to major drug companies, including Eli Lilly & Co., GlaxoSmithKline U.S. Pharmaceuticals, Johnson & Johnson, Pfizer and Serono S.A., asking them to describe their efforts to prevent their products from being counterfeited or diverted to illicit online distributors. The committee previously asked for information from top shipping and credit card companies, including Visa International, MasterCard International, FedEx Corporation and United Parcel Service, about their efforts to curb sales of prescription drugs by unlicensed pharmacies. While several bills dealing with Internet pharmacies have been drafted, only one bill being drafted by Rep. Charles Norwood (R-GA) would target companies facilitating online drug transactions. That bill would establish penalties for search engines and Internet service providers who accept advertising from rogue drug companies. None of the proposed measures would set penalties for shipping or credit card companies.



# NEWS YOU CAN USE

## NEW YORK, CALIFORNIA PUSH FOR INTERNET SALES TAX

New York and California have become the latest states to seek Internet sales taxes; this year both states added a line requiring taxpayers to declare any tax they owe on out-of-state purchases. New York state officials say that the new tax return line will force taxpayers to confront their liability or potentially face audits that could uncover credit card statements and tax debt. They are expecting the new tax line, for which they have added seven pages of instructions and tables, to yield just \$2.5 million. New York, like most states, lets taxpayers estimate their liability based on household income. According to a University of Tennessee study, New York loses more than \$1 billion in sales tax revenues from out-of-state purchases. California projects its out-of-state sales line will bring in \$13 million this year out of an estimated \$1.2 billion owed by individuals and businesses.

In Ohio, when the line was added four years ago, 52,000 taxpayers participated. In 2002, the number participating dropped to 46,000, out of 5.7 million total returns. The state raises about \$2 million, but projects that about \$500 million is uncollected. When Maine added the line in 1989, it also created a “default assessment” of .04 percent of adjusted gross income if the line was left blank. By 1998, the default was removed because of concerns the system was not fair for taxpayers who simply forgot or did not know the rules. Without the default, Maine generated \$1.3 million from the line last year, but estimates that it might be missing out on as much as \$30 million a year.

According to the Federation of Tax Administrators, states with sales tax lines on their tax forms include Alabama, California,

Connecticut, Idaho, Indiana, Kentucky, Louisiana, Maine, Massachusetts, Michigan, New Jersey, New York, North Carolina, Ohio, Rhode Island, South Carolina, Utah, Vermont, Virginia and Wisconsin. Georgia, Hawaii and the District of Columbia have separate forms in their income tax packages.

## UN URGES ACTION AGAINST INTERNET DRUGS

According to an annual report by the United Nation’s International Narcotics Control Board (INCB), there is an increase in dealers using cyberspace to market narcotics and mind-altering drugs. The report adds that Internet pharmacies are shipping prescription-only drugs across the world and are targeting former patients who have become addicted to drugs. Specifically, the report warns the drug Ritalin, used to treat hyperactive children, carries a high risk of abuse, but has been advertised as a “mild and harmless stimulant.” It calls on governments to ask their judiciary to ensure that people caught trafficking controlled drugs on the Internet receive adequate penalties. The INCB also reported the following findings:

- European governments are creating a “permissive environment” for drug users, which could lead to a rise in the trade of illicit drugs;
- Europe is a major producer of synthetic drugs such as ecstasy. Governments should tighten controls on “precursors,” legal chemical compounds which are used to make illegal synthetic drugs;
- Drug traffickers are targeting middle-class U.S. citizens with high-purity heroin that they can smoke rather than inject;
- Turkmenistan is not doing enough to stem the flow of heroin coming from neighboring Afghanistan, the world’s top producer of the opium poppy used to make heroin.

---

## **IOWA LAUNCHES CITIZENS' Web site**

The Iowa Department of Management unveiled a new state Internet site designed as a tool for citizens to track state government performance. The site, [www.dom.state.ia.us](http://www.dom.state.ia.us), offers information collected by the Department and made available previously only to top government administrators and department heads. It includes progress reports and charts detailing the status of five key areas identified in the administration's leadership agenda: economy, education, health, safe communities and the environment. The site summarizes agency operations, government finance and economic indicators and detailed performance information from each state agency. It lists a mission, goals and an explanation of plans to improve outcomes for each of 47 departments.

## **FBI ANNOUNCES "JOHN DOE" CHILD PORNOGRAPHY INITIATIVE**

The FBI announced a program in which agents will go after suspected producers of child pornography by obtaining "John Doe" arrest warrants and releasing the suspects' photographs or videos to the public. The images, obtained from child pornography Web sites and other online sources, are displayed on television and the Internet. The FBI said that the effort has already paid off with two arrests and, in both cases, the arrests stemmed from pictures that were aired on "America's Most Wanted." The FBI believes that taking the photos or videos of the unknown suspects and prominently featuring them on this weekly program and on the FBI Web site will help curb the danger to children posed by pornographers. The new task force, which operates from a Maryland location, persuaded Justice Department prosecutors to seek "John Doe warrants" against suspected pornographers. Traditionally, such warrants are used only in cases such as bank robberies where photos of

unknown suspects are disseminated to help solve crimes, and prosecutors are reluctant to seek John Doe warrants and grand jury indictments because of the serious consequences that could arise from mistaken identities in child pornography cases.

## **CALIFORNIA E-VOTERS TO GET PAPER RECEIPT**

California will become the first state to require that all electronic voting machines produce a voter-verifiable paper receipt. California Secretary of State Kevin Shelley announced that the requirement applies to electronic voting machines already in use as well as those currently being purchased. Machines must be retrofitted with printers to produce a receipt by 2006, and beginning July 1, 2005, all counties will not be able to purchase any machine that does not produce a paper trail. However, voters they will not be allowed to keep the receipts, which will be stored at voting precincts and used for a recount if any voting irregularities arise. With the receipt, voters will be able to verify that their ballots have been properly cast.

The announcement follows the creation of a task force Shelley convened last year to discuss growing concerns about the security of electronic voting machines. The task force was composed of election officials, computer experts, members of the general public and representatives of the disabled community. It was divided between two factions: a contingent that opposed a paper trail and computer and voting experts who supported the requirement. Proponents of a paper trail say the California decision is likely to influence other states that have been undecided about whether to require voter receipts. In addition to the voter receipt, Shelley called for the creation of a technical oversight committee as well as additional requirements for software testing and auditing and new security protocols for manufacturers. He also called for random field testing on election days to ensure that voting machines are functioning properly.

---

## **FCC RELEASES NET PHONE GUIDELINES**

The Federal Communications Commission (FCC) released guidelines that it will use to decide what rules, if any, will govern companies providing Internet telephone services. The agency has already ruled that telephone calls that never touch the public switched telephone network, pure voice over Internet Protocol (VoIP), should not be regulated. VoIP is a technology for making phone calls that use the Internet Protocol, the most popular method for sending data from one computer to another. It is already being used by carriers as a way to cut traffic costs on international and long distance calls, and it is expected to eventually replace the public switched network, as the phone companies convert to IP-based fiber optic networks. Currently, about 11 percent of all voice traffic is classified as VoIP, although less than one percent of those calls initiated on a VoIP phone. The guidelines announced by the FCC consist mainly of a list of questions on which the FCC is seeking public comment. The agency will use the public comments to determine whether calls that travel over the Internet and the traditional phone network should be regulated, a key Internet phone regulatory issue.

## **GEORGIA PRISONS GIVE INMATES COMPUTERS, NOT LAWYERS**

As of January 1, 2004, Georgia state prison inmates were no longer able to use state-funded attorneys to help them file habeas appeals and challenge prison conditions. Under the new system, inmates have access to 170 computers and computer-readable DVDs that contain court decisions, statutes, administrative rules and legal treatises. They will not be able to do any research over the Internet, however, because prison officials fear it could create security problems. Some librarians and at least four paralegals will also be available. Like other states, Georgia will still provide attorneys for direct appeals by indigent defendants. State-provided lawyers cost Georgia \$1.1 million per

year, and it is estimated that the new system will save between \$300,000 and \$400,000 annually, although that savings might be significantly less if the Department of Corrections has to hire more paralegals than anticipated.

## **INTERNET SERVICE PROVIDERS SUE SPAMMERS**

Four of the largest Internet companies have filed six lawsuits against some of the biggest bulk e-mailers under the federal anti-spam law passed by Congress last year, which gives Internet service providers the authority to file these types of lawsuits. America Online (AOL), Microsoft, Yahoo and Earthlink, in a coordinated effort aimed at stopping the biggest spam producers, filed the suits in Georgia, Virginia, California and Washington. If they win any of the lawsuits, they could recover millions in damages from the spammers. However, it should be noted that several of the lawsuits are filed against "John Doe" defendants only identified by numbers, as they do not know the names of the spammers they are suing. Some of the defendants in the case are named. AOL has filed a lawsuit against Davis Hawke, who has several aliases and is accused of selling millions of AOL addresses to spammers. Microsoft has filed a lawsuit against JDO Media Inc., based in Ocala, Florida, accusing the company of using deceptive subject lines in commercial e-mail and not putting physical addresses in their solicitations.

## **INTERNET REGULATOR APPROVES DOMAIN "WAIT-LISTING"**

The Internet Corporation for Assigned Names and Numbers (ICANN), the Internet's main oversight body, approved at its semiannual meeting the creation of a controversial service to let people bid on domain names that are about to expire. VeriSign Inc., which operates the master "registry" of Internet addresses ending in dot.com, had proposed a "wait-listing" service which they claim would bring order to the flood of electronic requests they receive when Internet addresses become available when their owners let them lapse. The

---

service would create a master list of Internet speculators. Each would know if they won their bid for first rights to a name before it expired. There would never be a guarantee that an address would expire, leaving speculators to bid on who will be first in line in case it does lapse. Critics, however, charge that the service would crush many small companies that thrive on selling domain names and would hurt customers because they would have to pay in advance for names that might never expire. The U.S. Department of Commerce, which gives ICANN its authority to oversee dot.com, still must approve the wait-listing service before VeriSign can launch it.

And more ICANN news.....

### **ICANN APPROVES SIX USER GROUPS**

The Internet Corporation for Assigned Names and Numbers approved six community user groups in three regions. The "At-Large" groups aim to engage individual Internet users in ICANN activities and generally foster a greater understanding of, and participation in, the Internet governing process. Certification of the At-Large organizations comes after ICANN's board approved a framework for establishing local, regional and global user groups.

In Europe, ICANN's At-Large Advisory Board certified four groups: Forderverein Informationstechnik und Gesellschaft eV, Internet Society Bulgaria, Internet Society Luxembourg A.S.B.L. and Societa' Internet. The committee also approved the Arab Knowledge Management Society in the Asian-Pacific and Australia region and Alfa-Redi in the Latin America and Caribbean Island region. More information about At-Large applications can be accessed at [alac.icann.org/applications](http://alac.icann.org/applications).

### **MICROSOFT OFFERS REWARD FOR MYDOOM.B LEADS**

Microsoft will offer \$250,000 for information leading to the capture and

conviction of the individual or group responsible for the release of MyDoom.B. The MyDoom.B variant prevents an infected PC from accessing some Microsoft Web sites and targets Microsoft's main Web site with a denial-of-service attack. The reward is the third time Microsoft has posted a \$250,000 "Wanted" sign on the Internet. It offered the same amount for information leading to the capture and conviction of the persons or groups responsible for releasing the MSBlast worm and the Sobig.F virus.

Microsoft's reward is the second prompted by the MyDoom virus. The SCO Group previously announced that it is offering \$250,000 for information that leads to the capture of the writer of the original virus. Both the original MyDoom virus and the modified variant target SCO's Web site with a denial-of-service attack.

### **PRESIDENT URGES CYBERCRIME TREATY RATIFICATION**

President Bush has asked the U.S. Senate to ratify the Council of Europe's controversial cybercrime treaty. The treaty requires each participating nation to ban the distribution of software that is designed for the "purpose of committing" certain computer crimes, requires Internet providers to ensure "expeditious preservation of traffic data" upon request and permits real-time wiretapping of Internet service providers. It also covers extradition for computer crimes and permits police to request that their counterparts in other countries cooperate in conducting electronic surveillance. According to the Council, only Albania, Croatia and Estonia have ratified the treaty.

Although the United States is a non-voting member of the Council, it has pressed hard for the cybercrime treaty as a way to establish international criminal standards related to copyright infringement, online fraud, child pornography and network intrusions. Civil libertarians have objected to the treaty ever since it became public in 2000, arguing that it would endanger privacy rights and grant too much power to government investigators. Industry groups, such as the Americans for

Computer Privacy and the Internet Alliance, have also raised concerns that the treaty could limit anonymity or impose vague record-keeping requirements on U.S. Internet providers.

The treaty would also ban “hate speech” from the Internet, a common prohibition in European nations that violates the First Amendment. The ban covers “distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.” This is defined as “any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence against any individual or group of individuals, based on race, color, descent or national or ethnic origin, as well as religion.” The Justice Department said last year that it does not support this optional addition, but still endorses the underlying treaty.

### **FCC EXPANDS WIRELESS NET FREQUENCIES**

The Federal Communication Commission announced they would expand the spectrum of frequencies for wireless devices that do not require modems and phone jacks, an 80 percent boost in the amount of spectrum that these wireless networks could use to connect computers and other electronic devices to the Internet. The new frequencies are in the five gigahertz range on the radio spectrum, much higher than the frequencies used by commercial radio and television stations.

The Pentagon initially opposed efforts to open the spectrum to wireless Internet connections, concerned that it would interfere with military radar. However, the Defense Department dropped its objections after manufacturers of wireless devices agreed to include technology to detect and avoid interfering with radar operating on similar frequencies.

### **UN, MICROSOFT PARTNER TO HELP POOR COUNTRIES**

Microsoft and the United Nations Development Programme (UNDP) will work together to build information technology training facilities in developing nations, with a focus on establishing community education centers. The UNDP’s goal is to provide information technology resources and encourage the use of technology in addressing some of the developing world’s largest problems, such as the HIV and AIDS epidemic.

The effort will draw on the resources of Microsoft’s Unlimited Potential program, an initiative to furnish job skills and computer literacy in underserved communities. It is focused on achieving the United Nations’ Millennium Development Goals, a set of worldwide living standards that includes the eradication of hunger and poverty, the establishment of universal primary education and the reduction of child mortality.

The partners also detailed plans to work together in support of the United Nations’ Southern Africa Capacity Initiative, which focuses on technology improvements in the countries most adversely affected by HIV and AIDS. This Initiative targets development of information technology and communications capacity, e-government programs and basic services delivery in those countries. UNDP and Microsoft are currently researching pilot projects in Egypt, Mozambique and Morocco, with plans to expand into additional countries in the coming months.

### **OVER 50% OF FEDERAL AGENCIES FLUNK SECURITY SURVEY**

More than half of the federal agencies surveyed received a grade of D or F in an investigation of computer security conducted over the past year, according to a “scorecard” released by the House Government Reform Subcommittee on Technology, Information Policy and Intergovernmental Relations. The Department of Homeland Security, which has a division devoted to monitoring cyber security, received an F and the lowest overall number score of 34. The Nuclear Regulatory Commission (NRC) and National

---

Science Foundation received an A, with the NRC drawing the top score of 94.5. Intelligence agencies such as the CIA and National Security Agency did not receive grades. In total, 14 agencies improved their grades in this annual review of computer security, while the federal government overall received a D, up from the F scored last year.

The grading system is based on the Federal Information Security Management Act (PL 107-347), which mandates government-wide standards for assessing computer security. The grades are based on an inventory of all information technology security procedures, such as the ability to quickly patch security holes and the number of trained computer security professionals at the agencies.

### **FCC TOUGHENS E-RATE RULES**

The Federal Communications Commission toughened the rules for its controversial E-Rate program, a \$2.5 billion initiative to help schools and libraries connect to the Internet. Supported by fees added to consumers' telephone bills, the program has been criticized by Congress for alleged abuses. The new rules aim to correct some of the alleged abuses by prohibiting the transfer of equipment purchased through the fund to other locations for three years and limiting support for upgrading or replacing internal connections to no more than twice every five years.

Since the inception of the program in 1997, approximately 90% of U.S. schools and libraries have received some assistance from E-Rate. The FCC oversees the program, but outsources its administration to the Universal Service Administrative Company (USAC), a private non-profit. Last year, the Center for Public Integrity, a non-profit organization,

issued a report, based on two FCC audits as well as independent interviews, claiming E-Rate was rife with fraud. That report led the House Energy and Commerce Committee to launch an investigation into the program. The FCC also held a forum on possible reform of the program, after which USAC announced it was organizing a task force to study reform actions.

### **IBM AGAIN LEADS IN PATENTS GRANTED**

The U.S. Patent and Trademark Office granted IBM 3,415 patents in 2003, marking the eleventh consecutive year the company has been the top recipient. IBM is the only company to garner more than 3,000 patents in one year, which it has done for the past three years. More than 1,400 of the total IBM patents last year were in software, marking the second year that software accounted for more than 40 percent. Other leading areas in IBM's patent portfolio included on-demand computing, an effort to make information technology resources available as necessary to handle spikes in usage; pervasive computing, which connects handheld computers and other devices to the Internet; and life sciences. Typically, IBM submits an application for a patent during the product development process, and many enhancements are released into products before a patent is granted or rejected.

Other tech companies are increasing their patent efforts as well. For example, Hewlett-Packard (HP) jumped to the fifth position on the list of patents awarded in 2003, up from ninth position in 2002. HP received 1,750 patents last year, a 27 percent increase from 2002. Recently, all of HP's intellectual property was moved into a separate, wholly owned holding company to be managed by a new intellectual property licensing unit.

---

## POSITION ANNOUNCEMENT

### Counsel for National Programs

The National Center for Justice and the Rule of Law, a program at the University of Mississippi School of Law, anticipates an opening for the position of Counsel for National Programs. The start date of the position is July 1, 2004. This position's primary focus will be cyber crime and cyber security issues. A secondary focus may be in the area of search and seizure. The Center has established cooperative relationships with other national organizations, corporations, academics, and state-wide agencies in numerous states. Through these relationships, the Center has created national training programs for state prosecutors in all 50 states and has developed model projects to facilitate the prosecution of persons engaged in cyber crime. The Center's projects are unique and address concerns of national interest. The Counsel for National Programs must be able to manage these existing programs and develop new projects and relationships. The Counsel for National Programs will have the opportunity to make significant contributions to the development of the law in the area of emerging technology.

The successful candidate will have visiting faculty status at the law school and be afforded the opportunity to teach advanced criminal law and procedure classes.

Applicants must have a J.D. degree from an ABA-accredited school, be admitted to the bar, have substantial criminal experience, supervisory experience, strong interpersonal skills, a record of academic achievement, and advanced writing, oral, and editing skills.

The position is non-tenure track and is dependent on the Center's ability to retain funding. Interested persons should send a cover letter, resume, writing sample, and references. **Contact:** Professor Thomas K. Clancy, Director, National Center for Justice and the Rule of Law, University of Mississippi, School of Law, P.O. Box 1848, University, MS 38677-1848. For more information about the Center, please visit their Web site at [www.olemiss.edu/depts/law\\_school/ruleoflaw](http://www.olemiss.edu/depts/law_school/ruleoflaw). The University of Mississippi is an EEO/AA/Title VI/Title IX/Section 504/ADA/ADEA employer.

---

The Cybercrime Newsletter is developed under the Cybercrime Training Partnership between the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL) at the University of Mississippi School of Law. It is written and edited by Hedda Litwin, Cybercrime and Violence Against Women Counsel ([hlitwin@naag.org](mailto:hlitwin@naag.org), 202-326-6022), and formatted by Valarie Gibson, Project Assistant ([vgibson@naag.org](mailto:vgibson@naag.org), 202-326-6262).

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

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

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