National Association of Attorneys General

CYBER CRIME NEWSLETTER

National Center for Justice and the Rule of Law
The University of Mississippi School of Law

Issue 12 **July/August 2005**

News Highlights in This Issue

Six Attorneys General Sue Diet Supplement Maker 6

Alaska, Illinois, Ohio Enact ID Theft Laws 11-12

Policy Briefings for Congress Now Online 15

State-by-State Justice System Expense Data Released 20

Authenticated Instant Messages Allowable as Evidence 19

18 States Launch Network for Internet Tax Collection 16

Online Child Predator Law Signed in North Carolina 12

Interactive Web Site Satisfies Texas Long Arm Statute 17

Browser-Based Attacks Up 20 Percent 14

New Jersey Legislature Approves GPS Monitoring Bill 12

Washington Commercial E-mail Law Not Preempted 17

Federal Ban Against Unsolicited Faxes Enacted 12

Few "Canadian E-Pharmacies" Based in Canada 13

South Carolina "Harmful to Minors" Law Struck Down 18

New Computer Forensic Tool Tested 20

Virginia "Phishing" Law Becomes Effective 13

FTC Announces New Data Disposal Rule 15

Encryption Program on Computer is Relevant Evidence 18

Study on Insider Cyber Attacks Released 15

Automatically Created Header on Computer Not Hearsay 17

Industry Groups Support Cyber Crime Treaty 15

Table of Contents

Feature: ID Theft Passport Programs 2

AG Initiatives 6
Six AGs Sue Supplement Maker
AG King: Guilty Plea in False Claims Case
Arizona AG Sues Online Realty Firm
AG Beebe Hosts "Protecting Children Online"
Colorado AG Unveils Online Consumer Guide
AG Brady: Web Site on Wanted Persons Debuts
Florida AG: Arrests in Online "Pill Mill" Case
AG Carter Seeks Shutdown of Bogus Site
Louisiana AG: Child Pornographer Arrested
AG Rowe Appeals Online Tobacco Law Decision
Maryland AG Will Introduce ID Theft Legislation
AG Reilly: Online Car Scam Offender Arraigned
Michigan AG: Online Child Predator Convicted
AG Hood: Guilty Plea in Internet Auction Case
Missouri AG Sues Fraudulent eBay Seller
AG Bruning Convicts Internet Predator
New Jersey AG Charges Sergeant With ID Theft
AG Madrid Obtains Plea From Online Predator
New York AG Settles With Adware Installer
AG Cooper: Child Pornographer Arrested
Ohio AG: Ex-Police Chief Indicted for Pornography
AG Edmondson Charges Ex-Agent With Online Fraud
Pennsylvania AG Sues Online Diploma Mill
AG Lynch Files Suit Against Online Realty Scammer
South Carolina AG Expands ICAC Task Force
AG Abbott Arrests Online Predator
Utah AG Charges Five With Child ID Theft
AG McKenna Conducts "Fraud Fighter" Workshop
Wisconsin AG Sues Internet Services Provider

Legislation Update 11
Alaska, Illinois, Ohio Enact ID Laws
Senate Committee OKs State ID Theft Preemption Bill
Ban on Unsolicited Faxes Becomes Federal Law
New Jersey Legislature Approves GPS Monitoring Bill
Virginia Phishing Law Becomes Effective
House, Senate to Confer on PATRIOT Act of 2005

News You Can Use 13
United Airlines Approved for Wi-Fi Flights
Few "Canadian E-Pharmacies" in Canada
Report: Browser Attacks Up
FCC Launches E-Rate Review
Report: Big Black Market in Illegal Music
Congressional Policy Briefings Now Online
Industry Groups Support Cyber Crime Treaty
CERT Releases Insider Cyber Attack Study
FTC Announces New Data Disposal Rule
Study: Online Pricing Varies With User
All Federal Employees to Get Electronic IDs
Eighteen States Advance Plan to Tax Online Sales

In the Courts 17

Tools You Can Use 20
New Computer Forensic Tool Tested
Detailed Criminal Victimization Data Released
State Justice System Expense Tables Available
Federal Victim Assistance Guidelines Updated

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

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

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.

IDENTITY THEFT PASSPORT PROGRAMS

By Thomas Taff*

Identity theft is a growing problem in the United States, and the Federal Trade Commission (FTC) estimates that 27 million citizens were victimized by identity theft from 1998 to 2003.[1] In the wake of recent data theft scandals at commercial data brokers, many state legislatures are considering new legislation to deal with the growing epidemic of identity theft. While the average consumer may be able to mitigate the initial economic damage, the real damage from identity theft is a tarnished consumer credit report.[2] While most states recognize identity theft as a crime, many of them also have recognized that the damage from identity theft goes far beyond the initial illegal transactions. Some states, such as Florida, have enacted "security freeze" legislation to protect victims from poor credit reports.[3] Likewise, many states have passed consumer protection laws criminalizing identity theft and the trafficking of stolen identities. Six states: Arkansas, Montana, Nevada, Ohio, Oklahoma and Virginia have taken additional legislative steps to protect residents living in their respective states by creating state identity theft passport programs.[4] Virginia was the first state government to establish an identity theft passport program is administered through the Office of the Attorney General. Arkansas, Montana, Nevada and Ohio have recently enacted legislation in 2005 that create identity theft passport programs. In these four states, the Attorney General, working with local law enforcement, administers the passport program. The Oklahoma identity theft passport program, created in 2004, is administered through the Oklahoma State Bureau of Investigation. This report will focus on the technical aspects of the state identity theft passport laws, as well as the effect of this legislation in addressing the current identity theft crisis. Identity theft passport programs are one of many possible legislative solutions to the identity theft crisis in the United States, and there are key differences that distinguish the various state identity theft passport programs from one another. Notably, the programs are a supplement to a well-educated, alert consumer. Attorneys General around the

country continue to educate and assist the average consumer through education programs and timely consumer alerts.

Earlier this year, Arkansas passed House Bill 1740, now Act 744 of the Regular Session, establishing the state identity theft passport program.[5] The law gave the Attorney General's Office the power to issue identity theft passports to state residents. The passport registration form can be accessed from the Attorney General's web site.[6] An applicant must meet several technical requirements before he or she becomes eligible for the passport program: the person must be an Arkansas resident, and he or she must "file a police report." The victim can then use the identity theft passport when dealing with local law enforcement officers and creditors. Even after the victim has received the passport, the certificate is not binding upon third parties. A creditor or police department is not required by law to acknowledge the identity theft card. While the personal records of the victim are not public, the Attorney General's office does have the authority to release documents to other police departments. The law states, "The Attorney General may provide access to the applications and supporting documentation to other criminal justice or law enforcement agencies in this state or another state." This law is fairly new, and so there are no statistics yet on the usage or deterrent effect of this identity theft passport program. Furthermore, unlike the Ohio law, the Attorney General is not required to report to the other branches of government.

Arkansas has taken other steps as well to guard its citizens against the crime of identity theft. House Bill 1354, now Act 280 of the Regular Session, was signed into law by Governor Mike Huckabee this year, and the new law clarifies the definition of identity theft as a crime where a person, "accesses…another person's identifying information for the purpose of opening a credit account…without the authorization of the person identified by the information."[7] Furthermore, the Arkansas law upgraded the crime of identity theft from a Class D felony to a Class C felony. It also gave examples of data that would be considered "identifying information," such as "driver's license numbers" and "social security numbers." The bill allows the Attorney General to prosecute the offender under a deceptive business practices legal theory. Arkansas thus joins a long list of states that have stiffened penalties for violators of state identity theft laws.

Ohio also enacted an identity theft passport program; however, the Office of Attorney General ran an identity theft passport program before the General Assembly enacted the current legislation authorizing it.[8] With the Attorney General's support, the Ohio General Assembly ratified House Bill 48, and Governor Bob Taft then signed the bill into law. While the Arkansas and Ohio programs share a number of similarities, there are some administrative and structural differences between the two identity theft passport programs. Under the Arkansas program, a victim of identity theft can directly apply to the Office of the Attorney General for the passport. In contrast, under the Ohio program, a victim of identity theft applies to the local law enforcement department, and the department files the report with the Attorney General's Office. However, just as is the case with the Arkansas program, the Ohio identity theft passport can be used with both creditors and law enforcement officials. The passport is not binding, and the creditor or police officer has the legal discretion as to whether to honor the identity theft passport. The Ohio identity theft law does unnecessarily restrict investigations by Ohio law enforcement officials. Furthermore, the Attorney General's Office has the legal authority, in specified circumstances, to provide the identity theft documents to other jurisdictions. The act specifically states, "The Attorney General may provide access to the applications…to other criminal justice agencies in this or another state." One unique feature of the Ohio program is the fact that the identity theft passport law requires the Attorney General to prepare an annual report on identity theft for the governor and select state legislative officials. The law also contains an important privacy clause that protects the identity of a victim, and state officials do not have access

to the personal identifying information of any victim when they review the annual identity theft report. Ohio law, in striking similarity to recent Arkansas legislation, allows for a liberal interpretation of "personal identifying information." Also, House Bill 48 stiffens the penalty for identity theft, and the minimum penalty for identity theft is raised from a misdemeanor to a fifth degree felony. Under the new Ohio law, a perpetrator of identity theft faces heightened penalties if the amount stolen exceeds certain set amounts. Under this new formula, a person convicted of identity theft could face a second-degree felony charge. Another unique feature of the Ohio law is that it provides special penalties for perpetrators who commit crimes against the elderly or the disabled. If the perpetrator steals more than $100,000 from a disabled or elderly victim, he or she could face a first-degree felony charge.

Virginia established the first identity theft passport program in 2003; however, there are some key differences between its identity theft passport program[9] and the recently created Ohio and Arkansas identity theft passport programs. While the programs in Ohio and Arkansas allow a victim to use his or her passport card when dealing with creditors, the Virginia identity theft passport program has a much narrower focus. The Virginia identity theft passport program is restricted to use within the state criminal justice system, and the program's objective is to protect victims of identity theft from criminal misidentification. The Office of the Attorney General "may provide assistance to the victim in obtaining information necessary to correct inaccuracies or errors in his credit report." However, according to the state identity theft law, it is up to the victim to work with the credit companies to correct his or her credit status. The statute specifically states "no legal representation shall be afforded such person." The law establishes clear limits on which individuals can apply for the passport. As a prerequisite, the identity theft victim must have been "charged or arrested" as a result of the identity theft before he or she can be processed through the state program. Furthermore, the Virginia program requires an expungement order from a Virginia circuit court while, in contrast, victims applying to the Arkansas and Ohio programs only need to present a copy of the police report and an identity theft application. In the Virginia passport program, the Attorney General is required by law to work with the Virginia Department of Motor Vehicles and also send a copy of the passport records to that department. As a result of this interagency cooperation, the Department of Motor Vehicles has a record of the passport for future reference. The Virginia Attorney General's Office does have some further obligations under current state law. The Office of the Attorney General is required to notify and interview the identity theft victim and check for any pending criminal actions against the victim. Under current Virginia rules, the identity theft passport is good for a three-year period. The aim of the Virginia passport program is to avoid wrongful convictions; it does not address the financial issues associated with identity theft.

The Nevada legislature passed new identity theft legislation in June of 2005, and under the new law, the Attorney General has the authority to administer a statewide identity theft passport program.[10] The current Nevada identity theft passport legislation shares many similarities with other states' identity theft programs. As a prerequisite, the law requires an identity theft victim to go through a local police department before acquiring the passport. The police, and not the victim, submit the passport to the Nevada Attorney General. The Nevada identity theft passport, similar to the Arkansas and Ohio programs, can be displayed to both police and creditors; however, the police and creditors have some discretion as to whether to accept the passport. A unique feature about the Nevada law authorizes the Attorney General to accept funds from outside the government to administer the program. The Nevada legislation also instructs the Attorney General not to divulge an identify theft victim's sensitive personal information unless the request comes from "a law enforcement agency in this or another state."

The state of Oklahoma also has an identity theft program, although it is not run through the

Office of the Attorney General.[11] Under the law the Oklahoma State Bureau of Investigations investigates identity theft claims, and maintains a database of identity theft records. Similarly, the Oklahoma administrative code establishes a list of items that must be presented by an identity theft victim before the state can issue a passport.[12] Furthermore, similar to Virginia law, an Oklahoma identity theft victim must obtain a court order of expungement before receiving a state-issued identity theft passport.

Montana's identity theft passport program becomes effective in October of 2005 under Montana House Bill 110.[13] The Montana identity theft passport program is similar to other passport programs already in place in other states. A victim can receive a passport by submitting an application and police report to local law enforcement. The procedural language in the Montana bill is similar to the language used in the Ohio identity theft passport law, although the Montana law does not specifically single out elderly or disabled persons. Likewise, the Montana law is different from the Virginia passport program because victims of identity theft can present their card to a variety of persons. The law specifically states that the victim can show the card to "any of the victim's creditors to aid in the creditor's investigation and establishment of whether fraudulent charges were made." Furthermore, the Montana identity theft passport program is similar to the Ohio and Arkansas passport programs because the passport does not bind law enforcement officials and creditors. Finally, the Montana law orders the Office of the Attorney General to adopt administrative rules to regulate the passport program.

State-administered identity theft passport programs represent a unique tool that state Attorneys General can use to contain identity theft. Currently, several states, including Rhode Island[14] and New Mexico,[15] are considering identity theft passport legislation in their respective state legislatures. Identity theft passport programs represent one approach to the problem that state legislatures can adopt. In fact, in response to the growing epidemic of personal identity breaches, many states are enacting security freeze statutes that allow victims of identity theft to "freeze" their credit ratings. Security freeze legislation is one solution that does not carry with it the presumed costs of administering a state passport program. Likewise, some states have raised the criminal penalties for perpetrators of identity theft. Also, in a time of tight state budgets, some states might prefer the security freeze legislation and stricter mandatory sentences as a less expensive alternative to a formal passport program. While many of these questions remain unanswered at this time, state governments will continue to innovate to meet the challenge of identity theft. Identity theft passport programs are one of those many unique innovations as state Attorneys General prepare to meet the challenges of law enforcement in a technologically advanced and complicated world.

**Tom Taff is a third-year law student at the University of Mississippi School of Law who was an intern with the NAAG/NCJRL cyber crime program this summer. All interns are required to write a research paper on a computer crime issue, and Tom chose to write about the above program.*

---

[1] Fed. Trade Comm'n, Identity Theft Survey Report 12 (2003). The report explained that "In total, 12.7 % of survey respondents reported that within the last five years they had discovered that they were victims of one of the three types of Identity Theft. This implies that approximately 27 million American adults have been victims in this period."

[2] Brian Delany, Identity Theft: The Fair Credit Reporting Act and Negligent Enablement of Imposter Fraud, 54 CATH. U. L. REV. 553, 555 (2005). The author asserts "furthermore, most victims do not learn about the theft of their identity for over a year, long after identity thieves have tainted the victim's credit history and name."

[3] FLA. STAT. ch. 817.5681 (2005).

[4] The new passport laws include: 2005 Ark. Acts 744, 2005 Ohio Laws 22, VA. CODE ANN. § 18.2-186.5 (Michie 2005), 2005 Nev. Stat. 321, OKLA. STAT. ANN. tit 22, § 19b (West 2005), and 2005 Mont. Laws 55.

[5] 2005 Ark. Acts 744

[6] http://www.ag.state.ar.us/

[7] 2005 Ark. Acts 280

[8] 2005 Ohio Laws 22

[9] VA. CODE ANN. § 18.2-186.5 (Michie 2005).

[10] 2005 Nev. Stat. 321. The law goes into effect January 1, 2006, but the law authorizes the attorney general to promulgate administrative rules after July 1.

[11] OKLA. STAT. ANN. tit 22, § 19b (West 2005). The law specifies "the Oklahoma State Bureau of Investigation shall administer the Oklahoma Identity Theft Passport Program, prescribe procedures and policies for issuing the identity theft passport consistent with this act, and provide information to law

enforcement agencies explaining the program." The Oklahoma passport program only applies to "law enforcement purposes…financial institutions…are not required to honor an identity theft passport."

[12] OKLA. ADMIN. CODE § 375:40-1-5 (2005).

[13] 2005 Mont. Laws 55

[14] H.B. 5647, Gen. Assem., Gen. Sess. (R.I. 2005). The proposed Rhode Island legislation requires the victim to submit a police report to the Attorney General, and the proposed language appears to give discretion to the Attorney General to issue the passport. The proposed language states "The Attorney General, upon verifying the certified copy of the police report, may issue an identity theft passport." Likewise, the passport is good for a two-year period after the Office of the Attorney General issues the passport. Finally, the law provides penalties for individuals who submit false documents to acquire a passport. The proposed legislation gives leeway to the Attorney General, and the proposed legislation states that "the Attorney General shall promulgate rules and regulations in order to implement the provisions of this section…"

[15] H.B. 734, 2005 Leg., 47th Sess. (N.M. 2005). This bill authorize the Office of the Attorney General to administer an identity theft passport program. There are some distinctions between the proposed New Mexico scheme and existing identity theft laws. The proposed law states "the attorney general…shall issue an identity theft passport to a person who claims to be a victim of identity theft…" Furthermore, the proposed legislation appears to propose less discretion for law enforcement. The language notes "an identity theft passport shall be accepted as evidence of identity by law enforcement and others who may challenge the person's identity." The language in House Bill 734 is slightly different language from past passport statutes, and it is unclear at this time whether this bill will become law.

AG INITIATIVES

MULTI-STATE

Six state Attorneys General filed suit in their respective states against Berkeley Premium Nutraceuticals, Lifekey, Inc., Boland Naturals, Inc., Warner Health Care and Wagner Nutraceuticals for making unsubstantiated claims about their dietary supplements on their web sites. **Arkansas Attorney General Mike Beebe, Illinois Attorney General Lisa Madigan, North Carolina Attorney General Roy Cooper, Ohio Attorney General Jim Petro, Oregon Attorney General Hardy Myers and Texas Attorney General Greg Abbott** alleged that the companies lured consumers by advertising "free" 30-day trials of their products. However, when consumers called their toll-free number or visited their web site to take advantage of the offer, they were asked for credit card information to cover shipping charges, but were not told that they would be automatically billed for additional shipments. It was difficult for consumers to cancel the automatic shipments or get their money back.

ALABAMA

Attorney General Troy King announced that Carvena Fitts, a former employee of the state Department of Industrial Relations, pled guilty to a felony ethics violation for using her office computer to create false claims for unemployment benefits. She was sentenced to two years imprisonment, which was suspended, placed on two years of supervised probation and ordered to pay $4,836 in restitution. The case was handled by Assistant Attorney General Brent Woodall of Attorney General King's Public Corruption and White Collar Crime Division and Senior Special Agent John Mulligan of his Investigations Division.

ARIZONA

Attorney General Terry Goddard and Bank Superintendent Richard Houseworth filed suit against Virtual Realty Company, Virtual Realty Funding Company (VRF) and their owner, Kenneth Perkins, alleging they misled homeowners into signing over their homes. Defendants allegedly advertised over the Internet and by direct mail that they could prevent homeowners who were in arrears on their mortgage payments from losing their homes, but in fact, their assistance was structured so that homeowners transferred title of their homes to defendants. VRF allegedly targeted Spanish-speaking communities and used densely worded legal documents.

ARKANSAS

Attorney General Mike Beebe hosted a training program for law enforcement called Protecting Children Online in conjunction with the Arkansas Internet Crimes Against Children Task Force, the Office of Juvenile Justice, the Office of Juvenile Justice and Delinquency Prevention, the National Center for Missing and Exploited Children and the Fox Valley Technical College. The training addressed key issues in the effective investigation, prosecution, intervention and prevention of computer-facilitated crimes against children, and it featured experts from across the United States.

COLORADO

Attorney General John Suthers unveiled an online Consumer Resource Guide to provide information and advice to consumers on avoiding identity theft and other schemes and fraud. The Guide also contains contact information and links to helpful resources. The Consumer Resource Guide is available online at http://www.ago.state.co.us/index.cfm under "Topics" or the toolbar "Consumer Protection."

DELAWARE

Attorney General M. Jane Brady announced the debut of the "Wanted Persons Review," a web site listing the names and offenses of more than 50,000 individuals wanted in Delaware. The list gives potential tipsters non-emergency phone numbers for police agencies statewide, as well as an automatic e-mail to contact Delaware Crime Stoppers directly. Attorney General Brady, who chairs the state Criminal Justice Council's Warrant/Capias Committee that developed the idea for the web site, said that the list will be updated under DELJIS News at www.state.de.us/deljis.

FLORIDA

Attorney General Charlie Crist joined state Department of Law Enforcement (FDLE) Commissioner Guy Tunnell in announcing that state agents arrested nine people on charges they operated unlicensed Internet "pill mills." The organization is accused of illegally filling, without prescriptions or pharmacists, more than $10 million worth of Internet drug orders since late 2003, the vast majority of which were for the pain killer hydrocodone. More than 650,000 pills, valued at $1.9 million, were seized, and authorities obtained the forfeiture of more than $2.2 million in cash and property. The arrests were the culmination of "Operation Backdrop," a nine-month investigation by the Diversion Response Team that included members of FDLE, Attorney General Crist's Medicaid Fraud Control Unit and Office of Statewide Prosecution, the U.S. Drug Enforcement Administration and the Florida Department of Health.

INDIANA

Attorney General Steve Carter has asked a court to shut down a web site operated by Elite Activity, an online club that purports to be a charity, but is alleged by Attorney General Carter to be an illegal pyramid scheme. A restraining order against the group was previously granted, but Attorney General Carter found the group still in operation, and has asked that Elite Activity be found in contempt of court.

LOUISIANA

Attorney General Charles Foti, Jr. announced that a joint investigation between his High Technology Crime Unit (HTCU), the Dallas Police Department's Internet Crimes Against Children (ICAC) Unit and the National Center for Missing and Exploited Children led to the arrest of Dennis Willoz, Sr., who was charged with one count of pornography involving juveniles. The investigation ensued after a complaint was received from Microsoft MSN who detected the traffic of child pornographic images. Bond for Willoz was set at $75,000.

MAINE

Attorney General Steve Rowe appealed a federal court decision that invalidated a significant portion of the state law aimed at preventing youth access to tobacco from Internet and mail order sales.

The 2003 law requires tobacco retailers to be licensed by the state in order to have tobacco delivered to Maine citizens. The decision being appealed can be accessed at: www.med.uscourts.gov/Opinions/Hornby/2005/DBH_05272005_2-03cv178_NH_Motor_Transport_v_Rowe.pdf.

MARYLAND

Attorney General J. Joseph Curran, Jr. announced that he will introduce a legislative package during next year's legislative session to better protect state citizens from identity theft. Attorney General Curran will propose a bill that would require notification of consumers when their personal information has been breached so that they may take prompt action to protect themselves. The bill would also require companies to maintain adequate security for consumers' personal information, including encryption of personally identifiable information. A second bill would allow consumers to restrict access to their credit reports.

MASSACHUSETTS

Attorney General Tom Reilly announced that Odilon DeMoura was arraigned as part of an ongoing investigation into an online car sales scam. DeMoura, a/k/a Adam DeMoura, was charged with, and pled not guilty to, four counts of larceny for more than $250 and one count of conspiracy. DeMoura was arrested following an investigation by Attorney General Reilly's office into allegations that he was offering cars for sale on eBay, taking payments from out-of-state buyers and never delivering the vehicles. DeMoura used the screen names "rockstar 6474" and "aladdinautosales" and allegedly cashed more than $28,000 in checks. Assistant Attorney General Marc Jones of Attorney General Reilly's Corruption, Fraud and Computer Crime Division is prosecuting the case.

MICHIGAN

Attorney General Mike Cox announced that a jury convicted Michael Phillips, a science teacher, of Child Sexually Abusive Activity and Using a Computer to Commit a Crime, both 20-year felonies. Attorney General Cox's investigators arrested Phillips when he traveled to engage in sexual activity with a minor he targeted on the Internet. Instead, Phillips met agents who had conducted an undercover operation using the minor's persona. Phillips was suspended by the school district upon his arrest, and Attorney General Cox's Education and Social Services Division is now working with the Michigan Department of Education on possible action against his teaching license.

MISSISSIPPI

Attorney General Jim Hood's Cyber Crime Unit obtained a guilty plea from a former college student to four counts of Internet auction fraud. The defendant offered for sale "signed" Michael Jordan jerseys, "signed" Mickey Mantle baseballs and other supposedly autographed items on eBay, none of which he had in his possession. He was sentenced to five years on each count, which was suspended, and three years supervised probation with Internet restrictions. He was also ordered to pay restitution to the victims and a fine to Attorney General Hood's office for the victims' compensation fund, as well as investigative and court costs.

Ed. Note: The editor thanks Jean Smith Vaughn, Special Assistant Attorney General for the Office of the Attorney General of Mississippi, for information about this case.

MISSOURI

Attorney General Jay Nixon sued Michael Pickens for advertising bulk sales of top quality brand name new or "gently used" clothing on eBay, but delivering little more than trash to consumers who paid for his products. When a consumer placed an order, Pickens would arrange a shipment from a supplier of old, unwanted clothing and household items typically sent to impoverished nations. Consumers who attempted to obtain refunds from Pickens were ignored or refused. Attorney General Nixon's lawsuit asks the court to issue a permanent injunction against Pickens and award civil penalties of $1,000 per violation of the Missouri Merchandising Practices Act. The lawsuit also requests that Pickens be ordered to pay court costs,

restitution and 10 percent of the amount of restitution to the Missouri Merchandising Practices Revolving Fund.

NEBRASKA

Attorney General Jon Bruning obtained a conviction against an Internet predator, the third such conviction in a month for Attorney General Bruning's office. Steven Liston was convicted by a jury of one count of online enticement of a child, a class IIIA felony punishable by up to five years in prison and/or $10,000 in fines. The case was handled by Assistant Attorney General Corey O'Brien.

NEW JERSEY

Attorney General Peter Harvey announced that the Division of Criminal Justice charged Gary Stolinski, a State Police sergeant assigned to the State Governmental Security Bureau, with allegedly engaging in identity theft and credit card fraud. The indictment charges that Stolinski, a 17-year police veteran, used a State Police computer and resources to apply for credit cards using the personal identifying information of others without their authorization. American Express security investigators determined that the applications were fraudulent, and an investigation was conducted by the Division of Criminal Justice and the State Police Internal Affairs Bureau. The prosecution was coordinated by Deputy Attorney General Susan Kase of Attorney General Harvey's Special Prosecutions Bureau. Stolinski has been suspended without pay and faces up to 15 years in state prison and up to $175,000 in fines.

NEW MEXICO

Attorney General Patricia Madrid obtained a no contest plea to six felony counts against accused online sexual predator and New Mexico resident Thomas Kaufman. Kaufman's arrest was the culmination of a joint investigation between Attorney General Madrid's Internet Crimes Against Children (ICAC) Unit and detectives from the Naperville, Illinois Police Department. The investigation began after Naperville police were informed of an Internet relationship between a local 13-year-old girl and an older New Mexico man and sought the assistance of Attorney General Madrid's ICAC Unit. The ICAC investigators cooperated immediately, leading to the arrest of Kaufman. As a result of the plea agreement, Kaufman will be required to register as a sex offender and participate in a structured long-term offender treatment program. He faces potential prison time of 18 months on each fourth degree felony charge for a possible six years in prison.

Ed. Note: The editor thanks Sam Thompson, Communications Director for the Office of the Attorney General of New Mexico, for information on this case.

NEW YORK

Attorney General Eliot Spitzer reached an agreement with web marketer Intermix Media Inc. under which the company agreed to pay $7.5 million over three years to settle accusations that it surreptitiously installed software on computers. Attorney General Spitzer had charged Intermix with installing adware (software that delivers pop-up advertisements or similar promotions) by offering free screen savers or other products that, when accepted, would download the adware. Although a final agreement must be approved by the court, Intermix said it has voluntarily stopped distributing its adware program, is hiring a "chief privacy officer" and joining the Network Advertising Initiative, a self-regulatory industry group. Intermix did not admit any wrongdoing or liability.

NORTH CAROLINA

Attorney General Roy Cooper announced that Reginald Scippio was arrested for trafficking in images of child pornography, as well as viewing and downloading child pornography from the Internet. The arrest was part of a statewide child pornography investigation that has resulted in about 60 search warrants. Agents from the State Bureau of Investigation located suspects from Internet addresses that were being used to share child pornography videos and images. Scippio was charged with five counts of second-degree and five counts of third-degree sexual exploitation of a minor.

OHIO

Attorney General Jim Petro announced that David Harrison, a former police chief, was indicted by a grand jury on 23 counts, including 15 felony charges of illegal use of a minor in nudity-oriented material or performance, for accessing and reproducing pornographic images using his work computer. Harrison had pled guilty to pandering obscenity of a minor two years ago and was on probation, but withdrew his plea this year, allowing Attorney General Petro's office to present additional charges against him. Scott Longo of Attorney General Petro's Child and Elder Protection Section is serving as special prosecutor in the case.

OKLAHOMA

Attorney General Drew Edmondson charged Sabrina Sands, a former employee of Gore's Southlake Insurance Agency, with six counts of violating the Oklahoma Computer Crimes Act and four counts of embezzlement. Sands allegedly pocketed policy holder premium payments for her own use and then electronically submitted payments to the insurance agency by debiting the Southlake account, thereby causing a loss to the agency. Sands is also accused of electronically securing insurance for herself or her husband and debiting the premium payments from the Southlake account. According to the complaint, Sands profited by more than $6,000 from her scheme. The case will be prosecuted by Attorney General Edmondson's Insurance Fraud Unit.

PENNSYLVANIA

Attorney General Tom Corbett filed suit accusing Dennis Globosky of violating state consumer protection laws by operating an online diploma mill offering bogus degrees from a nonexistent school. Globosky offered degrees from the "University of Berkley," hoping to confuse consumers into thinking he was offering degrees from the real University of California at Berkeley. According to the lawsuit, Globosky offered degrees from associate level to doctorate at prices ranging from $2,065 to $4,995 on web sites, including http://www.berkley-u.edu and 17 other feeder sites. He advertised that studies could be completed from home with no exams. No criminal charges have been filed against Globosky, but he faces civil fines and restitution.

RHODE ISLAND

Attorney General Patrick Lynch filed a Verified Complaint and obtained a Temporary Restraining Order against JMC Investments LLC, 45 Shawmut LLC, Michael Solotke, Rick Simpson and Ronnie Ramos for allegedly engaging in an online scam involving real property. Defendants are accused of falsely advertising via mail and the Internet that they could assist homeowners in avoiding foreclosure without the necessity of selling their homes. Instead, the homeowners were enticed into unknowingly executing deeds conveying their homes to the defendants.

SOUTH CAROLINA

Attorney General Henry McMaster expanded his Internet Crimes Against Children (ICAC) Task Force by adding the Spartanburg County Sheriff's Department as a partner. Under the partnership, Attorney General McMaster's office will provide funding, training and resources, and the Sheriff's Department will conduct proactive undercover Internet predator sting operations. As part of the agreement, Attorney General McMaster's office will also prosecute their Internet predator cases, with a local solicitor prosecuting other child exploitation crimes.

TEXAS

Attorney General Greg Abbott's Cyber Crimes Unit arrested Jonathan Brooks, a veterinarian, who drove to another county to meet an individual he thought was an underage girl for sex. In fact, the "girl" was an undercover Cyber Crimes Unit investigator who had been chatting with Brooks online. He was charged with attempted aggravated sexual assault of a child, a second-degree felony. Brooks is awaiting indictment after posting a $175,000 bond.

UTAH

Attorney General Mark Shurtleff charged five people with third-degree felony counts of identity fraud and forgery under his "Operation Protect the Children," which focuses on child identity theft. Children's Social Security numbers are attractive to thieves because they are generally not used until they come of age, so Attorney General Shurtleff's office has focused on tracking down numbers in use. His office is delving into the records of the Department of Workforce Services to find children who are reporting income.

WASHINGTON

Attorney General Rob McKenna's office, working with the American Association of Retired Persons (AARP), conducted a workshop to train a group of state seniors to become volunteer Fraud Fighters. Participants learn about some of the most popular scams, including identity theft and Internet fraud. Experts explain the psychological principles and persuasive tactics that underlie selling techniques. To date, nearly 2,600 seniors have attended Fraud Fighter training since Attorney General McKenna's office and the AARP founded the program.

WISCONSIN

Attorney General Peg Lautenschlager filed a lawsuit against Radical Persson, Inc., a California corporation that allegedly charged over 1,000 businesses for Internet services they did not authorize. Using the names "EChurch Network" and "ILab Technologies," the company targeted small businesses in order to sell Internet access, web site hosting and Internet advertising, obtaining payment by including their monthly charges on the customer's telephone bill. The company also falsely represented that the businesses would be listed in its web business directory, but failed to do so. The lawsuit seeks refunds for all of the victims as well as penalties for violation of state consumer laws. The case is being handled by Assistant Attorney General John Greene.

LEGISLATION UPDATE

Identity Theft

Alaska Governor Frank Murkowski signed House Bill 131 into law on July 14, 2005, increasing the penalties for certain types of identity theft involving credit cards, ATM cards and ID cards. The bill, now Chapter 67, SLA 05, raises the penalty from a class A misdemeanor to a class C felony, punishable by sentences of up to 2-5 years in prison. In addition, it now becomes a class C felony to steal more than $50 by identity theft instead of the previous threshold of at least $500. The new law was effective upon signing.

Illinois Governor Rod Blagojevich signed House Bill 1633 into law on June 16, 2005, making Illinois the second state in the nation to require companies to notify consumers if their personal information may be compromised due to a breach in company security. The bill, now Public Act 94-0036, allows notice to be given in writing or electronically. A violation constitutes an unlawful practice under the state Consumer Fraud and Deceptive Practices Act.

Ohio Governor Bob Taft signed House Bill 48 into law on June 14, 2005, enhancing the penalty for identity theft if the victim is elderly or disabled from a first degree misdemeanor to a fifth degree felony. The bill also provides legislative support for Attorney General Jim Petro's Identity Theft Verification Passport

program, which provides an identification card for identification theft victims to help establish their status as a victim. The legislation will take effect 90 days from its signing.

The U.S. Senate Commerce, Science and Transportation Committee approved S. 1408 on July 14, 2005, an identity theft bill sponsored by Senator Gordon Smith (R-OR). The bill would preempt all state identity theft laws. It would set standards for notifying consumers of data breaches, and would require businesses, schools and other organizations that maintain sensitive personal information to secure it with physical and technological standards to be specified by the Federal Trade Commission. It would also give consumers the right to freeze their credit reports to prevent unauthorized access and limit solicitation of Social Security numbers. An amendment adopted without objection would prohibit the sale, purchase or display of Social Security numbers without consumer consent, except in the case of national security or public health issues. The Senate Judiciary Committee is expected to consider the bill in early fall.

Online Child Predators

On June 29, 2005, **North Carolina** Governor Mike Easley signed into law Senate Bill 472, legislation that makes it a felony to solicit anyone, including police officers posing as children, over the Internet. Under the old law, a predator who solicited an officer posing as a minor could only be charged with a misdemeanor. The new law, which becomes effective on December 1, 2005, requires those convicted to register on the state's Sex Offender Registry and to submit DNA samples for the state's convicted offender database. It also allows the governor's office or the Attorney General's office to initiate investigations into other sexual crimes related to the Internet and children, such as disseminating obscene material to minors.

Unsolicited Faxes

President Bush signed S. 744 into law on July 9, 2005, requiring businesses that send faxes to notify recipients of their right to opt out of future faxes and requiring them to comply with such requests. Under the legislation, now Public Law 109-21, businesses and associations may send unsolicited faxes only to those with whom they have an "established business relationship."

GPS Monitoring

On June 30, 2005, the **New Jersey** Assembly unanimously passed S1889/A4016, legislation establishing the use of Global Positioning System (GPS) technology to monitor sex offenders. The bill requires the chairman of the State Parole Board, in consultation with the Attorney General, to establish a two-year pilot program for the continuous satellite-based monitoring of about 250 sex offenders who have been determined to have a high risk of offending again. Ninety days after completion of the pilot, the chairman would submit a report to the Governor and the Legislature recommending whether monitoring should be continued as a statewide program. The legislation also authorizes annual polygraph examinations of certain sex offenders. The bill passed the Senate on June 27, 2005, so it now awaits Acting Governor Richard Codey's signature into law.

Phishing

On July 1, 2005, **Virginia's** new "phishing" law, codified as Virginia Code Section 18.2-152.5:1, became effective. Entitled "Using a computer to gather identifying information: penalties," the law makes it illegal to "use a computer to obtain, access, or record, through the use of material artifice, trickery or deception, any identifying information…" A person who violates the section is guilty of a Class 6 felony, and a person who violates the section and sells or distributes the information

obtained, or who uses the information obtained in the commission of another crime, is guilty of a Class 5 felony.

Ed. Note: The editor thanks Gene Fishel, Assistant Attorney General in the Technology and Transportation Division of the Virginia Attorney General's Office, for information on this law.

Terrorism

On July 29, 2005, the U.S. Senate called for a conference to resolve differences with members of the U.S. House on H.R. 3199, the USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005. The House passed the bill on July 21, 2005, but the Senate added an amendment. The current bill repeals the sunset dates, and thus makes permanent, specified provisions of the original PATRIOT Act, including provisions governing information sharing and the use of wiretaps, search warrants and electronic surveillance. It requires a government attorney, after the disclosure of the contents of an intercepted communication, to file notice with the judge who authorized the interception within a reasonable time, identifying the entities to which the contents were disclosed. The bill also limits an order for the use of pen registers and traps and trace devices to one year when the applicant has certified that the information likely to be obtained is foreign intelligence information that does not concern a U.S. person.

NEWS YOU CAN USE

UNITED AIRLINES GETS WI-FI APPROVAL FROM FAA

United Airlines, the world's second largest carrier, became the first domestic airline to get regulatory approval from the Federal Aviation Agency (FAA) to install and offer wireless Internet access (Wi-Fi) to its passengers and crew on flights within the United States. The approval applies to United's B757-200 aircraft that was used to test the technology. United, which is partnering with Verizon Communications, Inc. on this venture, must still get approval from the Federal Communications Commission. Wi-Fi is available at airports and some international flights, such as on Lufthansa and Japan Airlines, which offer the service for a fee. Pricing for United's service, which will likely launch in a year, is undetermined. Lufthansa charges a flat fee of $29.95 per flight or $9.95 for 30 minutes.

STUDY: FEW "CANADIAN E-PHARMACIES" BASED IN CANADA

More than 75 percent of web sites that purport to sell discounted prescription drugs from online stores in Canada are controlled or owned by individuals or companies located outside of Canada, including many in the United States, according to a study commissioned by the Office of Criminal Investigations of the Food and Drug Administration (FDA). Of the 11,000 Internet pharmacies examined in the study, only 1,000 sites actually sold prescription drugs, while most of the sites referred viewers to 1,009 online stores, 86 percent of which are currently hosted by United States companies. Almost 70 percent of the sites were registered by United States citizens, of which more than half are registered to a single unidentified web design firm in New England. According to the FDA, two thirds of the online pharmacies identified in the study explicitly state on their web sites that customers did not need a prescription to purchase medicines. The study was

conducted by Cyveillance, a Virginia company whose clients include three large pharmaceutical manufacturers. The report released to the public did not include information on any of the 214 pharmacy sites identified as based in Canada.

REPORT: BROWSER ATTACKS UP, VIRUSES DOWN

Despite a slight dip in the number of viruses and worms, browser-based attacks are increasing, according to the third annual report on information technology security and the work force by the Computing Technology Industry Association (CompTIA). CompTIA's survey of 500 organizations found that 56.6 percent had been the victim of a browser-based attack, up from 36.8 percent in 2004 and 25 percent in 2003. Additionally, the survey found that while 18 percent of organizations had been victims of phishing in 2004, this year the number of organization victims had grown to 25 percent. Viruses and worms continue to be the No. 1 security threat, with two-thirds of organizations reporting attacks, down slightly from 68.6 percent in 2004. The study included interviews with 489 government, information technology, financial and education professionals.

FCC LAUNCHES E-RATE REVIEW

The Federal Communications Commission is launching a comprehensive review of the troubled E-Rate program, under which telecommunications companies or contractors provide equipment and services for Internet usage to schools and libraries at a discount, and the federal government covers the difference through the E-Rate fund. Nearly 90 percent of U.S. schools and libraries receive subsidies from the fund. The FCC oversees the program, but outsources its administration to the private nonprofit Universal Service Administrative Company. The review comes three months after the Government Accountability Office (GAO) issued a report to Congress concluding that the FCC has not developed any measures to track the program's effectiveness. During the review, the FCC will examine and potentially streamline the funding distribution of the program.

INDUSTRY REPORT: BIG BLACK MARKET IN ILLEGAL MUSIC

A total of 1.2 billion music CDs copied and sold illegally both physically and on the Internet in 2004 created a $4.6 billion black market accounting for 34 percent of all the CDs sold worldwide, according to the International Federation of Phonographic Industry's (IFPI's) annual Commercial Piracy report. However, the report noted that while the number of pirate CDs remains high, there was only a two percent growth in illegal sales from 2004, marking the lowest level in five years. According to IFPI, this was due in part to increased enforcement efforts in foreign countries, where seizures of commercial CD burning equipment last year were twice the levels of 2003. The IFPI found that Spain was Europe's "most serious piracy problem country," shrinking the legitimate market there by one-third in the last three years. Other countries named in the report as having "unacceptable levels" of piracy and needing more government action included Brazil, China, India, Indonesia, Mexico, Pakistan, Paraguay, Russia and the Ukraine. The report also noted that the sale of pirate music exceeded the legitimate market in a record 31 countries.

POLICY BRIEFINGS FOR CONGRESS NOW ONLINE

The Center for Democracy and Technology (CDT), a technology policy organization, has created an online database of Congressional Research Service reports at http://www.opencrs.com. The reports are produced by CRS, a public policy arm of Congress, and are reserved for members of Congress, committees and their staffs. A member of the public can get a report only if a lawmaker chooses to release it. The site includes searchable links to more than 3,300

reports, as well as thousands of updates to those reports, that were gathered by CDT, the National Council on Science and the Environment, the Federation of American Scientists, the library at the University of Maryland's law school, a web site associated with the Franklin Pierce Law Center in New Hampshire and the National Memorial Institute for the Prevention of Terrorism. CDT is also asking the public to help in filling out its collection.

INDUSTRY GROUPS PUSH FOR CYBER CRIME TREATY

A coalition of industry groups and individual companies sent a letter to the U.S. Senate Foreign Relations Committee urging ratification of the Convention on Cyber Crime adopted through the Council of Europe. The coalition, which includes the Cyber Security Alliance, the Bankers' Association for Finance and Trade, the Business Software Alliance, the Information Technology Association of America and VeriSign, asked the Senate to review the treaty and focus on the importance of global cooperation in fighting computer network-based crimes. The United States signed the treaty in November 2001. It requires global cooperation and law enforcement on searches and seizures and provides for timely extradition for computer network-based crimes. To date, eight of the 42 countries that have signed the treaty have completed their ratification process.

CERT RELEASES INSIDER THREAT STUDY

The U.S. Secret Service and Carnegie Mellon University's CERT Coordination Center released a study advising companies that in order to avoid insider cyber attacks, they must ensure good password, account and configuration management practices, as well as the right processes in place for disabling network access when employees are terminated. According to the report, the need to have formal processes for handling employee grievances and negative events in the workplace, as well as for reporting suspicious behavior, are also crucial. The report is based on an investigation of 49 cases of insider attacks via computer systems in critical infrastructure sectors between 1996 and 2002. In most cases, the primary motivation for the attacks appears to have been revenge, and most attacks involved former employees who shouldn't have been able to access the systems after they left the company. About 57 percent of the attacks were carried out by systems administrators, while 33 percent were caused by privileged users. The report may be accessed at http://www.cert.org/archive/pdf/insidercross051105.pdf.

FTC ANNOUNCES NEW DATA DISPOSAL RULE

The Federal Trade Commission announced that a new data disposal rule has gone into effect under the Fair and Accurate Credit Transaction Act of 2003. The new rule requires all businesses and individuals to destroy private consumer information obtained from credit bureaus and other information providers. Electronic files must be erased or destroyed, and failure to properly dispose of the data could result in a $2,500 federal penalty per violation, as well as exposure to lawsuits for damages. The rule does not set a time limit for compliance, nor does it say how securely data must be kept until it is destroyed. Further information about the new rule may be accessed at http://www.ftc.gov/opa/2005/06/disposal.htm.

STUDY: ONLINE PRICING BASED ON USERS' HISTORY

The Annenburg Public Policy Center released a study which concludes that, unbeknown to most Americans, Internet merchants often charge different prices to different consumers for the same merchandise, a practice called "price customization." The study, entitled "Open to Exploitation," found that nearly two-thirds of adult Internet users incorrectly believe the

practice is illegal. The study also found that while first-time buyers at an e-retailer might see higher prices than a repeat customer, e-retailers may not offer discounts to repeat customers who buy the same brands regularly without looking at alternatives on the site. The study report may be accessed at http://www.annenburgpublicpolicycenter.org/04_info_society/Turow_APPC_Report_WEB_FINAL_pdf.

ALL FEDERAL EMPLOYEES TO GET ELECTRONIC ID CARDS

All federal agencies were required by June 30, 2005 to submit plans to the White House Office of Management and Budget (OMB) for making electronic identity cards available to their employees and contractors under the Homeland Security Presidential Directive 12. All federal employees are expected to have the cards for facilities and network access by October 27, 2006. The Federal Information Processing Standard 201, issued in February 2005, stipulates that the IDs must be machine-readable and issued only through an official accreditation process. The standard also specifies that the cards contain a photograph, cryptographic keys and biometric data so that a cardholder's identity can be verified either by security personnel or an automated card reader.

18 STATES MOVE FORWARD ON INTERNET SALES TAX

Tax officials and legislators from 18 states, meeting as the Streamlined Sales Tax Project, agreed to establish a network for collecting taxes on Internet sales, with 11 states overseeing the project and incentives to encourage retailers to participate. Starting on October 1, 2005, software vendors contracted by the Project will provide free tax collection and remittance software and services to online merchants who voluntarily agree to collect and remit taxes on e-sales on behalf of the 11 states that have amended their laws to fully comply with standards developed by the Project. In the other seven states, tax collection would be optional until their tax codes are in compliance. Taxes would be based on rates in effect where the buyer lives, and retailers would be compensated for the cost of collection. States will also offer a one-year amnesty for e-retailers that may owe taxes on past online sales. The states comprising the governing board are Indiana, Iowa, Kansas, Kentucky, Michigan, Minnesota, North Carolina, Nebraska, Oklahoma, South Dakota and West Virginia. New Jersey recently enacted legislation that will bring it into compliance, and will become a full member on October 1, 2005. Associate member states are Arkansas, North Dakota, Ohio, Tennessee, Utah and Wyoming. Some states that participated in the Project are waiting to undergo compliance until the U.S. Congress enacts legislation supporting the plan.

IN THE COURTS

An interactive web site meets the general jurisdiction requirements of the Texas long arm statute.
I & JC Corp. v. Helen of Troy L.P., 164 S.W.3d 877 (Tex. App. 2005).

The presence of child pornography on the .bmp files of a home computer, combined with the subsequent purchase of software programs to remove pornographic images on the computer, is sufficient to show that the defendant knowingly possessed the images.
United States v. Bass, 411 F.3d 1198 (10th Cir. 2005).

A federal lawsuit brought under diversity of citizenship against a nonresident does not offend due process, because the defendant posted potentially defaming e-mails on a message board in the forum state.
Abiomed, Inc. v. Turnbull, No. Civ. A. 05-10105-NMG, 2005 WL 1693839, at *1 (D. Mass. July 11, 2005).

An e-mail between two parties meets the writing requirement of the merchant's exception to the statute of frauds.
Bazak Int'l Corp. v. Tarrant Apparel Group, No. 04 Civ. 3653VM, 2005 WL 1705095, at *1 (S.D.N.Y. July 18, 2005).

The Washington Commercial Electronic Mail Act is not expressly pre-empted by the language of the CAN-SPAN act because the state statute regulates false and deceptive practices.
Gordon v. Impulse Mktg. Group, Inc., No. CV-04-5125-FVS, 2005 WL 1619847, at *1 (E.D. Wash. July 11, 2005).

In order to prove an arbitration agreement existed between a business and a participant, the business must show that the participant clicked on the acceptance button on the company's web site.
Martin v. Snapple Beverage Corp., No. B174847, 2005 WL 1580398, at *1 (Cal. Ct. App. July 7, 2005).

Personal jurisdiction cannot be asserted in a diversity case, when the plaintiff's agent completed the only Internet transaction within the forum state with the nonresident defendant.
Mattel, Inc. v. Anderson, No. 04 Civ. 5275RCC, 2005 WL 1690528, at *1 (S.D.N.Y. July 18, 2005).

A permanent injunction barring an individual from running a web-based tax protest business does not violate the First Amendment because the speech involved is unlawful commercial speech.
United States v. Bell, No. 04-1640, 2005 WL 1620325, at *1 (3rd Cir. July 12, 2005).

An automatically created header on a computer does not constitute hearsay, because the computer is not a declarant.
United States v. Hamilton, No. 04-4091, 2005 WL 1519112, at *1 (10th Cir. June 28, 2005).

The Communications Decency Act of 1996, which regulates indecency on the Internet, is not overbroad in blocking the communication of constitutionally protected speech.
Nitke v. Gonzales, No. 01 Civ. 11476, slip. op. at 1 (S.D.N.Y. July 25, 2005).

An anonymous comment posted on an Internet message board that is critical of a public company does not constitute defamation.
Ampex Corp. v. Cargle, 128 Cal. App. 4th 1569(Cal. Ct. App. 2005).

Congress did not exceed its Article I powers when it restored copyright protection to foreign authors who entered the public domain in the United States in non-compliance with copyright laws.
Golan v. Gonzalez, 01-B-1854, slip op. at 24 (D. Colo. April 20, 2005).

The trial court did not abuse its discretion when it admitted printed e-mails into evidence because they were properly authenticated.
People v. Downin, 828 N.E. 341, 351 (Ill. App. Ct. 2005).

Information on a web site cannot be judicially noticed without expert testimony because the accuracy of the information could be questioned.
People v. Schilke, No. 253117, slip op. at 1 (Mich. Ct. App. May 3, 2005).

If an employee signs a consent form allowing his or her employer to check his or her e-mail, there is no violation of the Stored Communications Act when the company searches the employee's files during a security investigation.
Borninski v. Williamson, No. Civ.A.3:02CV1014-L, 2005 WL 1206872, at *11-3 (N. D. Tex. May 17, 2005).

Presence of Encryption Program on Defendant's Computer Was Relevant to Question of Whether Defendant Was a Skilled User Who Intentionally Deleted Child Pornography Files.
State v. Levie, 695 N.W.2d 619, 624 (Minn. Ct. App. 2005).

A returning reservist can be fired for cause under USERRA if that employee defaces a company web site.
Haight v. Katch, L.L.C., No. 4:404CV3363, slip op. at 13 (D. Neb. May 20, 2005).

A general arbitration policy for employees, which was sent via a company e-mail, did not give the employee adequate notice of the policy change.
Campbell v. Gen. Dynamics Gov't Sys. Corp., 407 F.3d 546, 559 (1st Cir. 2005).

A statute that bans electronic images or visual depictions of sexual material deemed harmful to minors violates the First Amendment.
Southeast Booksellers Ass'n v. McMaster, 371 F. Supp. 2d 773 (D. S.C. 2005

If a company posts information about the Family Medical Leave Act on its web site, its employees have adequate notice of their rights under that act.
Dube v. J.P. Morgan Investor Services, No. 02-12290-GAO, slip op. at 4 (D. Mass. May 13, 2005).

Information contained in a secured folder on a laptop is protected by the attorney-client privilege even if the defendant has signed a confidentiality waiver allowing his or employer to inspect the computer.
People v. Jiang, No. H026546, 2005 WL 1415186, *19 (Cal. Ct. App. June 16, 2005).

A defendant's comments about an ex-employee's conduct on the Internet are not defamatory per se, because they were created after the employee was fired.
Cody v. Harris, 409 F.3d 853 (7th Cir. 2005).

A defendant who posts offensive information in an Internet chat room about the plaintiff's business does not have sufficient contact within the state to meet the requirements of the state long arm statute.
Knight-McConnell v. Cummins, No. 03 Civ. 5035, 2005 WL 1398590, at *3 (S.D.N.Y. June 13, 2005).

If a plaintiff can make a prima facie case of libel per se with regards to a defamatory e-mail, the First Amendment does not protect the speech, and the ISP must turn over the identity of the e-mail sender.
Pub. Relations Soc'y of America, Inc. v. Road Runner High Speed Online, No. 116210/04, 2005 WL 1330514, at *5 (N.Y. App. Div. May 27, 2005).

A defendant who distributes spam through a third party contractor does not meet the minimum contacts required to establish personal jurisdiction under the state long arm statute.
Beyond Sys., Inc. v. Realtime Gaming Holding Co., No. 119, 2005 WL 1458056, at *1 (Md. June 22, 2005).

Evidence of instant messages will be allowed as long as they are authenticated in accordance with the existing rules of evidence.
In re F.P., No. 1126, 2005 WL 1399264, at *3 (Pa. Super. Ct. June 15, 2005).

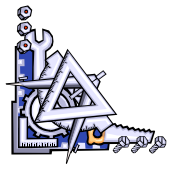
Evidence that defendant owned the residence and the computer, that he was in possession of the computer when child pornography was downloaded, and that the computer had "quick access" to a file containing the pornographic images, is sufficient to show that defendant knowingly possessed the images.
Kromer v. Commonwealth, No. 1900-04-2, 2005 WL 1388056, at *1 (Va. Ct. App. June 14, 2005).

A California court has personal jurisdiction over a Nevada hotel chain that allows California residents to conduct business over an interactive web site.
Snowney v. Harrah's Entm't, Inc., 35 Cal. 4th 1054 (Cal. Ct. App. 2005).

Despite their company web site privacy policy to the contrary, an airline did not violate the Electronic Communications Privacy Act when it released personal information to a federal regulatory agency.
In re Am. Airlines, Inc. Privacy Litig., 370 F. Supp. 2d (N.D. Tex. 2005).

A company selling books on their web site to California residents, and allowing the books to be returned to their stores in California, had sufficient contacts within California to justify the imposition a state tax.
Borders Online, LLC v. State Bd. Of Equalization, 129 Cal. App. 4th 1179 (Cal. Ct. App. 2005).

The Artists' Rights and Theft Prevention Act of 2004, which imposes criminal liability on certain copyright violators, does not modify the Copyright Act of 1976, which requires "actual" proof of distribution by the alleged violator.
In re Napster, Inc. Copyright Litig., No. C MDL-00-1369 MHP, slip op. at 11 (N.D. Cal. June 1, 2005).



TOOLS YOU CAN USE

New Computer Forensic Tool Tested

The National Institute of Justice (NIJ) made available "Test Results for Software Write Block Tools: PDBLOCK V1.02, V2.00, and V2.10" (online only) which presents, in three volumes, results from testing PDBLOCK Versions 1.02 (PDB_LITE), 2.00, and 2.10 against Software Write Block Tool Specification & Test Plan, Version 3.0. The three volumes can be accessed at http://www.ojp.usdoj.gov/nij/pubs-sum/209831.htm; http://www.ojp.usdoj.gov/nij/pubs-sum/209832.htm and http://www.ojp.usdoj.gov/nij/pubs-sum/209833.htm.

Detailed Criminal Victimization Data Released

"Criminal Victimization in the United States, 2003 -- Statistical Tables" (NCJ 207811) presents 110 tables with detailed data on major variables measured by the National Crime Victimization Survey. It can be accessed at http://www.ojp.usdoj.gov/bjs/abstract/cvusst.htm.

Justice System Expenditure and Employment Reviewed

Prepared by the Bureau of Justice Statistics, "Justice Expenditure and Employment Extracts, 2002 - Statistical Tables" (NCJ 209179) presents web-only tables that include national, state-by-state, and federal estimates of government expenditures and employment for the following justice categories: police protection, all judicial, and corrections. It can be accessed at http://www.ojp.usdoj.gov/bjs/eande.htm#selected.

New Edition of U.S. Attorney General Guidelines Released

"Attorney General Guidelines for Victim and Witness Assistance," a 75-page report (NCJ 210461) released by the U.S. Department of Justice, outlines the requirements for working with Federal crime victims and witnesses. It can be accessed at http://www.usdoj.gov/olp/final.pdf.