

Issue 16

News Highlights in This Issue:

Internet Cigarette Sales Settlement Reached by 37 AGs	3
E-mail and Online Chat CD Wins Best of California Award	2
Pennsylvania Security Breach Law Enacted	19
Draft Cyber Security Plan Released by DHS	13
Probable Cause Needed to Get Real Time Cell Phone Data	9
Congressional Report Examines Internet Drug Sales	16
New Jersey ID Theft Prevention Law Takes Effect	19
Illinois Video Game Law Violates First Amendment	10
ICANN Delays Plans for .xxx Domain	14
Utah Senate Committee OKs Credit Report Freezes	20
Online Dating Service Subject to New York Law	10
Industry Study: 1 in 4 Users Are Phishing Targets	16
Indiana Senate Committee Passes Junk Fax Bill	20
Free Anti-Spyware Software Certification Planned	13
Actual Damages Not Required to Recover Under ECPA	10
Passports to Have ID Chips in 2006	13
Florida, Missouri AGs Team up in Online ID Theft Case	3
Study: Many Domains Have False Registrations	16
E-Bay Seller Not Subject to Personal Jurisdiction	10

Table of Contents

<u>Features</u>	2
E-mail and Online Chat CD Wins Best of California Award	
<u>AG Initiatives</u>	3
AGs Reach Agreement with Cigarette Internet Firm	
Florida, Missouri AGs Team Up on Online ID Theft	
AG Goddard Announces ID Theft Indictment	
California AG Settles With Online Credit Repair Service	
AG Suthers Gives Internet Safety Presentation	
Connecticut AG Investigates Myspace.com Website	
AG Spagnoletti Hosts Internet Safety Assembly	
Florida AG Files Suit Against Bogus E-mail Operator	
AG Carter Announces Sex Offender Notices	
Kansas AG Launches Internet Safety Program	
AG Foti Charges Man with 68 Counts of Pornography	
Maryland AG Releases Report on ID Theft	
AG Cox Announces a Habitual Sex Offender Convicted	
Mississippi AG Says Online Predator Convicted	
AG Nixon Stops Online Phone Records Seller	
Nebraska AG Says Online Predator Convicted	
AG Madrid Announces Indictment of Child Pornographer	
Ohio AG Unveils eSORN Website	
AG Corbett Educates Children About Online Predators	
South Carolina AG Charges Child Predator	
AG Abbott Adds New Allegations Against Sony BMG	
Washington AG Files Suit Under New Spyware Act	
<u>In the Courts</u>	9
<u>News You Can Use</u>	10
Passport to Have ID Chips by October 2006	
Anti-Spyware Coalition Defines Spyware	
SEC Warns Online Traders about Cyber Thieves	
Draft Cyber Security Plan Released by DHS	
Anti-Spyware, Adware Software Certification Planned	
ICANN Nixes .XXX, OKS .ASIA	
Wikipedia to Require Registration after False Posting	
Free Speech under Attack, NYU Report Says	
Bill Gates Birthday Present to Dad: Scholarships	
Study Finds Domains with False Registration	
Industry Study: 1 In 4 Users Are Phishing Targets	
Publisher to Digitize Books to Protect Copyrights	
Report Examines Illicit Internet Drug Sales	
FTC Report: Can-Spam Act Is Effective	
FTC Study Finds Masking and Filtering Stops Spam	
Study Finds Employees Bypassing E-Mail Policies	
NJ Lawyers' Internet Ads Must Say They Were Paid For	
Patent Office Joins Effort to Improve Software Patents	
Homeland Security Awards Grant For Open Source Audits	
<u>Legislation Update</u>	19
NJ Identity Theft Prevention Act Takes Effect	
Pennsylvania Governor signs Security Breach Law	
Utah Senate Approves ID Theft Law	
Indiana Senate Judiciary Committee Approves Fax Bill	
FTC Works Closely With Foreign Law Enforcement	
FCC Establishes Requirements for VoIP	
Violence against Women and DOJ Reauthorization Act	

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

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

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

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



Recipients: Robert Morgester, Deputy Attorney General
Wayne Ikeuchi, Captain, Sacramento County Sheriff's Dept.
Todd Shipley, Director of Training Services, SEARCH

Left to Right: Robert Morgester, Captain Wayne Ikeuchi,
Todd Shipley, Awards Delegate Kais Manoufy

E-MAIL CD WINS BEST OF CALIFORNIA AWARD

The "High Technology Crime: E-Mail and Internet Chat Prosecutor/Investigator Resource" CD-Rom has won the Best of California award in the Best Sustainable Value category. The CD is a collective effort of the Office of the California Attorney General, the Sacramento Valley Hi-Tech Crimes Task Force (a unit of the Sacramento County Sheriff's Department Hi-Tech Crimes Division), the National Center for Justice and the Rule of Law of the University of Mississippi School of Law, and SEARCH, the National Consortium for Justice Information and Statistics. Its design,

development and production were underwritten by the Bureau of Justice Assistance, U.S. Department of Justice, and the Task Force.

The Best of California Awards program was established to salute IT professionals in California state and local government organizations for their dedication, hard work and contributions. The Best Sustainable Value award is presented to individuals and teams that have designed, developed and deployed applications that have been in operation at least two years and have realized benefits that can be documented.

This CD is intended as a reference tool to assist federal, state and local prosecutors and

investigators as they investigate and prepare to prosecute cases involving the misuse of electronic mail and online chat. The material is addressed in a practical, easy-to-use format that includes important "how-tos," such as legally obtaining electronic mail and Internet chat records, introducing computer-based evidence in court and presenting e-mail and chat record evidence to a jury. It provides:

-- A detailed introduction that will answer such questions as "what is electronic mail and how does it work" and "what is Internet chat;"

-- An in-depth look at the technical side of the Internet, e-mail and Internet chat as they relate to investigations;

-- Instructional material for use in court presentations and training; and

-- Legal transcripts, documents, modifiable templates and other resource materials. These materials were selected and developed using the insight and professional experience of

prosecutors who have successfully investigated and prosecuted online crimes.

Over 20,000 copies of the CD have been directly released to law enforcement. Since duplication of the CD is permitted, it is estimated that another 80,000 copies have been created. This disk is now being used by local, state, and federal investigators and prosecutors nationally. It has been adapted for use in law enforcement training programs, including those hosted under the partnership between the National Association of Attorneys General and the National Center for Justice and the Rule of Law, where each attending prosecutor received a copy of the CD.

Ed. Note: The editor thanks Robert Morgester, Deputy Attorney General, Office of the Attorney General of California, for the information contained in the above article.



AG INITIATIVES

MULTI-STATE

The Attorneys General of 37 states reached an agreement with Philip Morris USA in which the company will voluntarily incorporate protocols aimed at combating the illegal sale of PM USA cigarettes over the Internet and by mail. The protocols provide for the (a) termination of cigarette shipments to PM USA's direct customers that the Attorneys General have found to be engaging in illegal Internet and mail order sales; (b) reduction in the amount of product made available to direct customers found by the Attorneys General to be engaged in the illegal re-sale of PM USA cigarettes to Internet vendors; and (c) suspension from the company's incentive programs of any retailer found by the Attorneys General to be engaging in such illegal sales. The negotiations with PM USA were led by New York Attorney General Eliot Spitzer. In

addition, the Attorneys General from the following jurisdictions joined the agreement: Alabama, Arkansas, American Samoa, California, Colorado, Connecticut, Delaware, District of Columbia, Georgia, Hawaii, Idaho, Illinois, Iowa, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, New Mexico, New Jersey, Northern Mariana Islands, Oklahoma, Oregon, Puerto Rico, South Carolina, South Dakota, Tennessee, Utah, Vermont, Washington, West Virginia, Wisconsin and Wyoming.

Florida Attorney General Charlie Crist and Missouri Attorney General Jay Nixon collaborated in the investigation of Henry Berry of Florida, who allegedly stole the identities of Missouri residents online in order to open credit

accounts and purchase merchandise and gift cards. Merchandise from online merchants was allegedly delivered to a Florida address where Berry receives mail, but the billing information on the deliveries was that of Missouri residents. Berry has previous convictions for possession of cocaine, carrying a concealed weapon, larceny, burglary and vehicle theft. Attorney General Nixon and Jefferson County Prosecuting Attorney Robert Wilkins charged Berry with two criminal counts of identity theft. The investigation also involved the Secret Service, the U.S. Postal Inspection Service and the Miami and Pembroke Pines Police Departments.

ARIZONA

Attorney General Terry Goddard announced that William Joachim and Freddy Sanchez were indicted on charges of aggravated identity theft, including allegations that they used the credit card account of at least five people, including Green Bay Packers' quarterback Brett Favre, to purchase goods and services over the Internet. Joachim and Sanchez were indicted on one count of fraud, two counts of aggravated taking the identity of another and one count of theft. Joachim was also charged with one count of misconduct involving weapons. If convicted on all charges, each man faces up to a maximum of 14 years in prison. Assistant Attorney General Todd Lawson is prosecuting the case.

CALIFORNIA

Attorney General Bill Lockyer filed a settlement of his lawsuit against MyPerfectCredit (MPC), the operator of an online credit repair service, which allegedly engaged in false advertising and unfair business practices. MPC advertised on the Internet that it would help consumers correct alleged errors on their credit reports. MPC obtained the credit reports from the credit reporting agencies, forwarded them to consumers responding to the ads and gave them a limited time to select the negative information for MPC to challenge. However, if a consumer did not

respond within five days, MPC challenged all negative information and charged the consumer a fee for each challenge in violation of the state Credit Services Act. The settlement requires MPC to provide restitution to consumers in addition to \$150,000 in civil penalties and \$6,000 to cover the state's costs of investigating the case.

COLORADO

Attorney General John Suthers gave an Internet safety presentation to parents and students at St. Vincent DePaul High School in Denver. He was joined by Sergeant Kirk Hon of the Denver Police Department, who provided a demonstration of how predators can contact children online. The presentation is part of Attorney General Suthers' Safe Surfing Initiative.

CONNECTICUT

Attorney General Richard Blumenthal launched an investigation of Myspace.com for allegedly allowing minors easy access to pornography and other inappropriate material. The site posts no warnings that pornography or adult content are present and has no mechanism in place to prevent minors from viewing it. Attorney General Blumenthal's office has received numerous complaints about the site and has referred the matter to the Chief State's Attorney's Office for possible criminal prosecution.

DISTRICT OF COLUMBIA

Attorney General Robert Spagnoletti hosted an Internet safety assembly at a junior high school in partnership with the National Center for Missing and Exploited Children (NCMEC). The assembly program, created by Netsmartz, educated eighth and ninth grade students, parents and teachers about how to help protect children and teens from online predators.

FLORIDA

Attorney General Charlie Crist filed a lawsuit against Rik Rodriguez for allegedly running a bogus email operation that sent more than 1,100 illegal emails to more than 2,500 recipients, linking them to web sites selling Fuel Saver Pro, a device falsely advertised as increasing gas mileage and decreasing harmful pollutants and emissions. Many messages used false information to disguise the origin of the email, while others wrongfully concealed the sender's address by substituting innocent persons' names or invalid email addresses. Rodriguez allegedly used as many as 100 different computers to avoid detection. The spam emails were captured by Microsoft through its MSN trap accounts and were referred to Attorney General Crist's office. Since the emails were sent before Florida's anti-spam law was enacted, the lawsuit alleges violations of the Florida Deceptive and Unfair Trade Practices Act, and Rodriguez faces penalties of up to \$10,000 per violation. The lawsuit will be litigated by Attorney General Crist's Economic Crimes Division.

HAWAII

Attorney General Mark Bennett announced that Joseph Colasacco was charged with electronic enticement of a child and promoting pornography to a minor for using the Internet to meet a 14-year-old boy. According to court documents, Colasacco met the boy through MySpace.com where both have web sites. He was arrested in the boy's bedroom with a pornographic DVD and magazines. Attorney General Bennett is asking the state legislature to enact a bill requiring a minimum sentence of one year for anyone convicted of Internet enticement.

ILLINOIS

Attorney General Lisa Madigan's Internet Crimes Against Children (ICAC) Task Force, working with the Macomb Police Department, arrested and charged Ronald Cope, an Illinois

Department of Corrections (IDOC) corrections officer, with one count of Indecent Solicitation of a Child, a Class 3 felony punishable by a maximum of five years. Cope was arrested when he arrived at a K-Mart store to meet and allegedly have sex with a 13-year-old girl he met on the Internet but in reality was an undercover officer from Attorney General Madigan's task force. Subsequent to the arrest, the task force, assisted by the Pike County Sheriff's Office, served a search warrant on and seized computer equipment from Cope's residence. The McDonough County State's Attorney's Office is assisting Attorney General Madigan's office on the prosecution of the case.

INDIANA

Attorney General Steve Carter announced a new e-mail service through which state residents will be able to learn when a sex offender moves into their neighborhood. The service, to be available in April 2006, will notify citizens who sign up of changes in the sex offender registry that affect them. People convicted of sex offenses are required by law to register their residence and work information with the state.

KANSAS

Attorney General Phill Kline launched a program designed to help students, parents and teachers stay safe on the Internet during a series of presentations across the state. Attorney General Kline was joined by representatives of the NetSmartz Workshop of Kansas, the Boys & Girls Club Kansas Alliance, members of the Kansas Legislature, and Clicky, the official spokes-robot for NetSmartz.

LOUISIANA

Attorney General Charles Foti, Jr. announced the arrest of Michael Chatellier, an employee of the Orleans Parish Criminal Sheriff's Office, on charges of 68 counts of Pornography

Involving Juveniles and one count of Computer Aided Solicitation of a Minor. During online chats with an undercover agent from Attorney General Foti's High Technology Crime Unit posing as an underage girl, Chatellier allegedly solicited the "girl," exposed himself, attempted to entice the "girl" for sexually explicit photos of herself and distributed child pornography images. The agents executed a search warrant at Chatellier's home, where they located child pornography on his computer. If convicted of the pornography charges, Chatellier faces a possible minimum mandatory sentence of two to 10 years without probation or parole. If convicted of the solicitation charge, he can be fined up to \$10,000 as well as imprisoned for two to 10 years without probation or parole. The Federal Bureau of Investigations and the Jefferson Parish Sheriff's Office assisted with the investigation and arrest.

MARYLAND

Attorney General J. Joseph Curran released his "Report on the Attorney General's Identity Theft Forum," which contains information from his November 2005 forum. According to the report, the number of identity theft complaints received by the Federal Trade Commission from state residents increased by more than 400% over the last five years. The report also highlights the problem of security breaches; the Choicepoint breach alone affected 2,750 Maryland consumers.

MASSACHUSETTS

Attorney General Tom Reilly reached an agreement with an Internet company registered to Jeremy Paradies, a Massachusetts resident, after seeking an emergency court order to shut down its web site selling consumer electronics that has allegedly bilked 128 British consumers. Complaints about the site, mydv.co.uk, now owned by Massachusetts-based Nepco, included failure to refund overcharges and misleading British consumers into thinking the site was based in the United Kingdom. According to the agreement,

Nepco had to refund or fulfill customer orders by a deadline, as well as alert customers that they are not British-based.

MICHIGAN

Attorney General Mike Cox announced that habitual sexual predator Timothy Westbrook was found guilty of two counts of Child Sexually Abusive Activity and two counts of Using a Computer to Commit a Crime, both 20-year felonies. Westbrook used the Internet to contact what he believed was a 14-year-old girl to arrange a sexual encounter. He went to meet the online persona and was arrested by Attorney General Cox's investigators. Westbrook was sentenced to 8-40 years in prison as a habitual third offender. He must also pay a \$60 Crime Victims' Rights fee and \$240 in state costs, must provide a DNA sample for the national registry and register as a sexual offender.

MINNESOTA

Attorney General Mike Hatch proposed restricting the Department of Public Safety from distributing drivers' license data in bulk quantities to anyone other than law enforcement without the license holders' consent via "opt-in," as well as limiting access to individual driver's license data. Attorney General Hatch argues that con artists currently can easily obtain state drivers' license data from at least one Internet site. Current law requires drivers' license data to be public, and the state charges a fee to cover the cost of disseminating the data.

MISSISSIPPI

Attorney General Jim Hood announced that Shawn Bigham, a former New Houlka law enforcement officer and youth minister, was sentenced to eight years in prison, to be followed by five years of post release supervision, after he pled guilty to one count each of sexual battery and

touching a child for lustful purposes. Bigham communicated with the victim, who was a member of his church youth group, via e-mail and chats. Sherita Sullivan of Attorney General Hood's Cyber Crime Unit did the forensics on the case.

MISSOURI

Attorney General Jay Nixon obtained court orders to stop Internet business Locatecell.com and its operators from offering to sell the cell phone records of customers in the state. The web site advertised that for \$65 anyone could enter a cell phone number and receive the name and address of the cell phone user. For \$110, Locatecell.com would also provide a list of calls made from that cell phone number. Attorney General Nixon had sued the defendants for violating state consumer protection laws by misrepresenting that it was legal for them to obtain and sell the records. In fact, the defendants did not have authorization from the wireless and cellular telephone service providers to access the customer information and records they advertised.

NEBRASKA

Attorney General Jon Bruning announced that Ryan Geiger, who was convicted of online enticement of a child, a Class IIIA felony, was sentenced to one year and one day in prison. Following his release, Geiger must register as a sex offender. Geiger had initiated a sexually explicit conversation in a Yahoo! online chat room with what he thought was a 14-year-old girl but was actually a State Patrol investigator with the Internet Crimes Against Children Unit. He was arrested when he went to meet the "girl." The case was prosecuted by Assistant Attorney General Corey O'Brien.

NEW MEXICO

Attorney General Patricia Madrid announced that the Grand Jury returned a 25-count

indictment of Ronald Mabry on child sexual solicitation, exploitation and pornography charges. Five of the counts stemmed from an online chat session with what Mabry believed to be a 13-year-old girl, but who was actually an agent from Attorney General Madrid's Internet Crimes Against Children (ICAC) Unit. Mabry was arrested when he attempted to meet the "girl" by ICAC agents and Bernalillo County Sheriff's deputies. Following the arrest, agents seized computers and storage media at Mabry's home, and the ensuing forensic examination revealed pornography involving both children and adults. Mabry is facing a sentence of up to two years imprisonment and a \$5,000 fine for the fourth degree counts and a sentence of up to four years and a \$5,000 fine for each of the third degree counts.

NORTH CAROLINA

Attorney General Roy Cooper sent a letter to sheriffs and police chiefs across the state, urging them to send their officers to state-sponsored classes to learn how to catch Internet predators. The effort comes in the wake of a new North Carolina law that went into effect on December 1, 2005 making it a felony, instead of a misdemeanor, to proposition an undercover officer posing as a child on the Internet.

OHIO

Attorney General Jim Petro unveiled an enhancement to the electronic Sex Offender Registration and Notification (eSORN) web site that allows the public to view information about Ohio's most wanted sex offenders and submit tips to help track them down. The site, which can be accessed at www.ag.state.oh.us, now includes a list of the "most wanted" sex offenders and is comprised of all adult sexual predators who have committed offenses and have warrants, as verified by the Law Enforcement Automated Data System (LEADS). There are currently four Ohio men on the list.

OKLAHOMA

Attorney General Drew Edmondson announced that Laraine Maple was charged with five misdemeanor counts of violating the state Consumer Protection Act for selling, but failing to deliver, five laptop computers on the Internet. According to the complaint, Maple admitted to using fictitious names and the names of family members to establish accounts on the eBay, Yahoo and Overstock.com Internet auctions sites. She further admitted that she did not have any of the products offered for sale and never intended to provide them to the buyers, who paid between \$252 and \$400 for them.

PENNSYLVANIA

Attorney General Tom Corbett launched a statewide campaign to educate children about the dangers of online predators at Russell C. Struble Elementary School in Bucks County. Joining him were Bucks County District Attorney Diane Gibbons and members of the I Keep Safe Coalition, which created a web site, children's books and educational materials to emphasize online safety. Attorney General Corbett also introduced Faux Pas the Techno Cat, their safety icon, which will visit schools to give children Internet safety instruction.

SOUTH CAROLINA

Attorney General Henry McMaster announced the arrest of Timothy Simmons, Jr. on charges of Criminal Solicitation of a Minor, a felony offense punishable by up to 10 years imprisonment. According to arrest warrants, Simmons solicited sex online with two persons he believed to be underage girls but in reality were officers of the Westminster Police Department. He was taken into custody, and a search warrant was executed at his home. The Westminster Police Department is a partner in Attorney General McMaster's Internet Crimes Against Children (ICAC) Task Force.

TEXAS

Attorney General Greg Abbott added new allegations to his pending lawsuit against SONY BMG, alleging that the company's "MediaMax" technology for copy protection violates the state's spyware and deceptive trade practices laws. According to the allegations, consumers who use these CDs are offered a license agreement, but even if they reject the agreement, files are secretly installed on their computers, posing additional security risks to those systems. The lawsuit asserts that SONY failed to clearly warn consumers of the harm its copy protection software could cause when installed on consumers' personal computers, as well as the fact that files secretly embedded in CDs would likely compromise computers. In addition to violations of the Consumer Protection Against Spyware Act of 2005, which allows for penalties of \$100,000 for each violation, the amended suit alleges violations of the Texas Deceptive Trade Practices Act, which provides for a maximum penalty of \$20,000 per violation.

UTAH

Attorney General Mark Shurtleff filed charges against Daniel Duke, an 18-year-old college student, for allegedly using the Internet to arrange to have sex with a young girl. According to court documents, Duke contacted an undercover agent from the Utah Internet Crimes Against Children (ICAC) Task Force online who was posing as an underage female. He was arrested when he attempted to meet the "girl." Duke is facing two second-degree and two third-degree felony counts of enticing a minor over the Internet. His arrest involved investigators from Attorney General Shurtleff's office, the Utah Department of Corrections, the West Valley, West Jordan and Centerville Police Departments and U.S. Customs and Immigration Enforcement agents. Assistant Attorney General Paul Amann will prosecute the case.

WASHINGTON

Attorney General Rob McKenna filed the first lawsuit under the state's new computer spyware act, accusing New York-based Secure Computer, as well as associates in the United States and India, of falsely claiming that consumers' computers are infected with spyware and marketing Spyware Cleaner, a program that claims to remove it, through deceptive means. In fact, the program renders computers more susceptible to attacks. The lawsuit and a similar suit brought by Microsoft are

the result of parallel investigations by Microsoft experts and Attorney General McKenna's High Tech Fraud Unit. The suit alleges violations of Washington's 2005 Computer Spyware Act, the federal CAN-SPAM Act, the state Commercial Electronic Mail Act and the state Consumer Protection Act. If found liable, defendants can be fined \$100,000 per violation under the state spyware law, \$250 per violation under the CAN - SPAM Act, \$500 per violation under the state email law and \$2,000 per violation under their consumer laws.



IN THE COURTS

Alleged Internet Predators Can Be Charged With Attempting to Sexually Assault a Child, Even When the Intended Victim is a Persona Created by Law Enforcement

State v. Sorabella, No. 17215 (Conn. February 1, 2006)

State Cannot Exercise Personal Jurisdiction, in Case Brought Under State Anti-Spam Statute, Over Out-of-State Defendant, Based Solely Upon the Defendant Contracting With an Agent Who Sent One Unsolicited E-mail to a Person Within the State

State v. MLeads Enterprises, No. 20041072 (Utah February 10, 2006)

An arbitration clause in an Internet service provider's service agreement is unconscionable because it requires consumers to arbitrate relatively small claims in the company's home state and prohibits class actions.

Aral v. Earthlink, Inc. (2005) 134 Cal.App.4th 544.

Note: The California Attorney General was amicus curiae on behalf of the plaintiff and respondent.

Defendants' Alleged Unauthorized Access to Plaintiff's Password-Protected Site Did Not Give Rise to a Violation of the Digital Millennium Copyright Act.

Egilman v. Keller & Heckman, LLP, No. 1:04-cv-00876, 2005 WL 3077260 (D.D.C. Nov. 10, 2005).

The Government is Not Entitled to "Real-Time" Cell Site Data Absent Probable Cause

In re Application of United States for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers, No. 05-4486 (D. Md. November 28, 2005)

Ordering Defendant Not to Use the Internet Was a Reasonable Condition of Probation Following Conviction of Possession of Child Pornography

People v. Harrison, No. C048707 (Cal.App.4th November 30, 2005)

Note: The Office of the California Attorney General successfully argued this case.

Listing Used Books for Sale on Amazon.com Does Not Violate Author's Copyright

Okocha v. Amazon.com, 2005 U.S. App. LEXIS 23788 (3rd Cir. November 3, 2005)

There is No Fourth Amendment Privacy Interest in Subscriber Information Given to Internet Service Provider

United States v. Sherr, 2005 U.S. Dist. LEXIS 30463 (D. Md. November 16, 2005)

The Illinois Violent Video Games Law and Sexually Explicit Video Games Law Violate the First Amendment.

Entertainment Software Association v. Blagojevich, No. 05 C 4265 (N.D. Ill. December 2, 2005)

And see also...

Preliminary Injunction Issued Where Plaintiffs Established Likelihood of Success on the Merits That California Violent Games Law Violates First Amendment

Video Software Dealers Ass'n v. Schwarzenegger, No. 05-4188 (ND Cal. December 21, 2005)

Consumer Infringed Music Copyrights by Downloading and Saving Music Files, Despite Her Claim of Fair Use
BMG Music v. Gonzalez, 430 F.3d 888 (2005)

The Communications Decency Act Immunizes a Web Hosting Company From a Defamation Claim

Austin v. CrystalTech Web Hosting, 2005 WL 3489249 (Ariz. App. Div. December 22, 2005)

Online Dating Service is Subject to New York's Dating Services Law

Doe v. Great Expectations, No. 3034/05 (N. Y. Civ. Ct. November 9, 2005)

Alleged Infringer's Erasure of Computer Evidence Does Not Entitle Copyright Holder to Summary Judgment

Paramount Pictures Corp. v. Davis, 2005 WL 3303861 (ED Pa. December 2, 2005)

District Court Erred by Dismissing an Indictment Brought Against Web Site Operators on Grounds That Laws Criminalizing the Commercial Distribution of Obscene Material Violated the Privacy Rights of Their Customers

United States v. Extreme Associates, Inc., 2005 WL 3312634 (3rd Cir. December 8, 2005)

Employer Awareness of Worker's Visits to Child Pornography Sites at Work Created Duty to Act

Doe v. XYZ Corp., 2005 WL 3527015 (NJ Super. App. Div. December 27, 2005)

There is a Private Right of Action Available Under the Electronic Communications Privacy Act (ECPA) for the Unauthorized Interception of Encrypted Satellite Television Broadcasts

DirectTV, Inc. v. Pepe, No. 04-4333 (3rd Cir. December 15, 2005)

An Internet Auction Transaction Does Not Subject an eBay Seller to Personal Jurisdiction in the Forum

Action Tapes, Inc. v. Weaver, 2005 US Dist. LEXIS 29312 (ND Tex. November 23, 2005)

Actual Damages Are Not Required to Recover Under the ECPA, so Defendant Who Accessed Co-Worker's E-Mail Without Authorization is Not Entitled to Summary Judgment

Cedar Hill Associates, Inc. v. Paget, No. 04 C 0557 (ND Ill. December 9, 2005)

Defendant Who Knowingly and Purposefully Sent Commercial E-Mails Into State Was “Doing Business” in the State and Subject to Personal Jurisdiction

Gordon v. Ascentive, LLC, (Slip. Op.) 2005 WL 3448025 (ED Wash. December 15, 2005)

Child Pornography Downloaded Through Pop-Up Ads Was Enough to Support a Computer Search Warrant
State v. Helland, 2005 SD LEXIS 184 (December 7, 2005)

Broker Had No Duty to Tell Client of Plan to Transfer Client’s Online Brokerage Business to Another Broker, Even If It Profited by Transfer

Weil v. Morgan Stanley DW Inc., 2005 WL 3526441 (Del. December 22, 2005)

The ECPA Does Not Support the Issuance of an Order to Disclose Real Time Cell Phone Information Upon a Showing of Less Than Probable Cause

In re Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information, No. 05-508 (D.D.C. December 30, 2005)

Order for Real Time Cell Site Information is Authorized Under a “Hybrid Theory” Using the Patriot Act-Amended Definition of a Pen Register and the Stored Communications Act

In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, No. 05-1763 (S.D.N.Y. December 30, 2005)

Real Time Location Data Requires a Warrant

In re Application of the United States of America for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers, No. 05-4486 (D. Md. November 28, 2005)

The Communications Decency Act Section 230 Immunity Does Not Protect an Online Forum Operator From His Own Libels

Cisneros v. Sanchez, 2005 WL 3312631 (SD Tex. December 7, 2005)

Plaintiffs in Citigroup Data Tape Loss Case Must Arbitrate Their Claims

Cunningham v. Citigroup, 2005 US Dist. LEXIS 33805 (D. NJ December 16, 2005)

U.S. SUPREME COURT WATCH

Decisions

Will v. Hallock, (04-1332) 387 F.3d 147, vacated and remanded, January 18, 2006. The court unanimously ruled that refusal to dismiss a claim against federal officers on the ground that it is barred by the Federal Tort Claims Act (FTCA) is not immediately appealable under the collateral order doctrine.

Susan Hallock and her husband owned a computer software business that was allegedly driven out of business when federal customs agents seized its computers to search for child pornography after her husband’s (allegedly stolen) credit card number

was used to subscribe to a child pornography web site. Although no child pornography was found, business data on the seized computers was destroyed, leading to the failure of the Hallocks' business. Susan Hallock sued the United States under the FTCA, alleging that the customs agents were negligent in conducting the search, but the suit was dismissed for falling within an exception to the statute's waiver of sovereign immunity. While the suit was still pending, Susan Hallock also filed a separate *Bivens* action against the individual customs agents alleging that they deprived her of property in violation of the Fifth Amendment. When the FTCA suit was dismissed, the agents moved to dismiss, arguing that under 28 U.S.C. §2676, an FTCA judgment bars suit against the federal employee whose act or omission gave rise to the FTCA claim. The U.S. District Court for the Northern District of New York denied the motion to dismiss, holding that the FTCA dismissal was only procedural, and thus did not bar the *Bivens* action. The Second Circuit affirmed.

In an opinion by Justice Souter, the Supreme Court vacated the Second Circuit decision, holding that the court erred in assuming jurisdiction over the appeal under the collateral order doctrine. The case was remanded with instructions to dismiss the appeal for

lack of jurisdiction, thus allowing the Hallock case to proceed.

Certiorari Denied

The court declined to grant a petition for certiorari review in *Faulkner v. National Geographic Society*, 2005 WL 2706947 (U.S. 2005), thereby letting stand the Second Circuit decision of *Faulkner v. National Geographic Enterprises Inc.*, 409 F.3d 26 1980 (2d Cir. 2005). The lower court held that current copyright law permits a publisher to create a digital archive of copyrighted photographs and articles from past issues of National Geographic Magazine without permission by, and compensation to, the freelance photographers and/or writers who created the original work.

The court also denied certiorari in *1-800 Contacts, Inc. v. WhenU.com, Inc.*, 2005 WL 3144164 (U.S. 2005). The Second Circuit Court of Appeals had ruled in *1-800 Contacts, Inc. v. WhenU.Com, Inc.*, 414 F.3d 400 (2nd Cir. 2005) that an Internet marketing company did not infringe a company's trademark rights by using its name as a "keyword" to trigger the display of a competitor's advertisements.



NEWS YOU CAN USE

PASSPORTS TO HAVE ID CHIPS BY OCTOBER 2006

The U.S. State Department issued final rules for implanting electronic identification chips into all U.S. passports, despite continuing controversy over the security of the system and its impact on personal privacy. As of October 2006, all new and renewed passports will contain radio frequency identification chips that will include a digital photo and all other information currently printed in passports. As older passports expire, all passport holders will get an electronic version. Government employee and diplomatic passports will receive the chips in a pilot program in early 2006. Foreigners from countries who do not need visas to enter the United States also must have the chips by next October, and those countries will be responsible for providing their citizens with passports that comply with U.S. entry requirements. Of the 2,335 comments the department received since it issued the proposed rules, 98.5 percent were opposed to the program. Further information may be found at:

http://travel.state.gov/passport/eppt/eppt_2498.html

DHS RELEASES DRAFT CYBER SECURITY PLAN

The Anti-Spyware Coalition issued its final guidelines for detecting, rating and protecting against spyware.

The group, composed of software companies and consumer advocates, also finalized its definition of spyware, with only minor changes from the version it proposed in July 2005. The coalition defines spyware and other potentially unwanted technologies as programs deployed without sufficient user consent or that impair user control over any of the following: privacy, system security and user experience; use of their system resources; or collection, use and distribution of personal information.

SEC WARNS ONLINE TRADERS ABOUT CYBER THIEVES

The Securities and Exchange Commission (SEC) alerted consumers who buy and sell stocks on the Internet to be wary of cyber thieves. The warning resulted from a flurry of complaints from online stock traders the SEC has received in recent months. The SEC warns that consumers must also be vigilant about how they open e-mail and browse popular web sites, because they can be infected with keystroke logging programs. The SEC advises traders to guard their Social Security numbers and closely monitor banking accounts for discrepancies.

DHS RELEASES DRAFT CYBER SECURITY PLAN

The U.S. Department of Homeland Security (DHS) released a 175-page draft of the National

Infrastructure Protection Plan (NIPP). The plan outlines a broad framework for protecting the nation's critical infrastructure and key assets. The plan was first commissioned an early version in February 2005. According to a notice announcing the document's availability, the latest version provides greater detail. The plan asserts that cyber security responsibilities should ultimately lie with in the DHS, but calls on state and local governments to develop information security measures and to be aware of vulnerabilities in their systems. The report charges academia and research institutions with devising best practices for IT security, and the private sector with ensuring that it is satisfying cyber protection standards. The document suggests that work should be done through a "sector partnership model," of informal advisory bodies composed of private-sector and governmental representatives from the same subject area. The draft plan may be found at:

<http://politechbot.com/docs/dhs.nipp.110205.pdf>

ANTI-SPYWARE, ADWARE SOFTWARE CERTIFICATION PLANNED

A group of major Internet-related companies, including Yahoo!, America Online, Computer Associates, CNET Networks and Verizon, are backing a plan to certify software as adware and spyware. Dubbed the Truste Download Program and administered by the Washington, D.C.-based non-profit Truste, it essentially would be a white list of voluntarily-submitted software that meets anti-adware, anti-spyware criteria. The companies sponsoring the

plan would only distribute or advertise programs on the white list. Among the criteria that software will have to meet are easy uninstallation, clear consumer consent before downloading and disclosure of affiliate relationships. Several adware/spyware-like practices are also banned, including taking control of a PC, tracking keystrokes and modifying computer settings. Truste will closely monitor certified software to make sure that adware or spyware isn't added into the mix after approval has been given.

ICANN NIXES .XXX, OKS .ASIA

The Internet Corporation for Assigned Names and Numbers (ICANN) abandoned plans to debate a proposal to create an .xxx domain for adult online content. The proposal was due to get final approval at an ICANN board meeting in Vancouver, British Columbia, but the proposal was removed from the agenda. This is the second time that ICANN has pushed back plans to approve .xxx. ICANN said on Thursday that its governmental advisory committee needed more time to review a 350-page report into the creation of .xxx. This report was finished in August 2005, but was not released for several months.

ICANN also tentatively approved an “.asia” domain to unify the Asia-Pacific community and supplemental suffixes available for individual countries, such as ".cn" for China and ".jp" for Japan. Registrations for English-language names in ".asia" could begin six months after ICANN grants final approval. However, ICANN and the DotAsia Organization Ltd., which consists of domain name operators in Asian countries, will first have to iron out contract details. DotAsia also plans

to explore permitting site addresses in Asian languages.

WIKIPEDIA TO REQUIRE REGISTRATION AFTER FALSE POSTING

Wikipedia, the online encyclopedia that allowed anyone to contribute articles, will now require users to register before they can submit entries following the disclosure that it ran an article falsely implicating a man in the Kennedy assassinations. While it would not prevent people from posting false information, it is hoped that the new process will make it easier for the site's 600 active volunteers to review and remove factual errors, defaming statements and other material that does not comport with Wikipedia policy. People who modify existing articles will still be able to do so without registering. The change came after John Seigenthaler, a former administrative assistant to Robert Kennedy, complained in an op-ed published in USA TODAY that a biography of him on Wikipedia claimed he had been suspected in the assassinations of the former Attorney General and his brother, President John F. Kennedy.

FREE SPEECH UNDER ATTACK, NYU REPORT SAYS

The free expression rights of web site owners and remix artists are being hampered because of ambiguities in copyright law, according to a report titled, "Will Fair Use Survive?", released by Marjorie Heins and Tricia Bickels of New York University Law School's Brennan Center for Justice. The report suggests six major steps for change, including reducing penalties for infringement and making a greater

number of pro bono lawyers available to defend alleged fair users.

Research for the report, which began in late 2004, included surveying nearly 300 stakeholders and reviewing letters sent to those accused of violating copyright law. Co-author Heins, who is also the coordinator of the Brennan Center's Free Expression Policy Project, said she encountered a great amount of confusion over fair use principles as well as what she considered irrational infringement claims. The report highlighted a "chilling effect" occurring through takedown notices, which they call a tactic whereby copyright and trademark owners send letters to Internet service providers (ISPs) pressuring them to remove sites the owners determined to be infringing. The report finds that such notices are rooted in a provision of the Digital Millennium Copyright Act of 1998 that frees ISPs and search engines from copyright infringement liability if they "expeditiously" take down anything a copyright owner claims to be in violation of the law. According to the report, the entire process, from letter-sending to site takedown, can occur without any formal legal proceedings. While victims of the takedown notices have recourse by contesting the allegations with a counternotice, the authors note that the paperwork is often complicated. They recommend creating Web sites that clarify not only appropriate fair uses but offer sample retorts to questionable takedown notices. The report can be viewed at:

<http://www.fepproject.org/policyreports/WillFairUseSurvive.pdf>

BILL GATES' BIRTHDAY PRESENT TO DAD: SCHOLARSHIPS

Microsoft Corp. Chairman Bill Gates established the William H. Gates Public Service Law Scholarships with \$33.3 million to commemorate his father's 80th birthday. Five students a year will receive scholarships of approximately \$100,000 covering tuition, academic costs and living expenses at the University of Washington with the caveat that they must work at least seven years after graduation at a nonprofit organization or government agency or pay back the entire sum. Gates Sr., a lawyer and civic activist, is a graduate of the university. The first applications are due in February 2006, to be followed by an announcement of the recipients in April 2006. The program is designed to last for 80 years.

STUDY FINDS DOMAINS WITH FALSE REGISTRATIONS

More than eight percent of all Internet domain names are registered with false or incomplete information, according to a study by the U.S. General Accounting Office (GAO). The study showed that 2.31 million domain names have been registered with intentionally false information, such as a (999) 999-9999 telephone number, while 1.6 million registrations contained incomplete data. The GAO report said that the Internet Corporation for Assigned Names and Numbers (ICANN) is now requiring registrars to investigate and correct any reported inaccuracies in contact information.

INDUSTRY STUDY: 1 IN 4 USERS ARE PHISHING TARGETS

About one in four U.S. Internet users are targets of phony e-mails seeking personal financial information (phishing), according to a study conducted by AOL Time Warner Inc. and the National Cyber Security Alliance. Additionally, the study found that 70 percent of consumers who received such e-mails thought they were from legitimate web sites. Further, 74 percent of those surveyed use their computers for sensitive transactions such as banking, stock trading or reviewing medical information, yet 81 percent of home computers lacked at least one of three critical protections: updated software, spyware protection or a secure firewall. The study was based on in-home interviews with more than 350 Internet users.

PUBLISHER TO DIGITIZE BOOKS TO PROTECT COPYRIGHTS

U.S. publisher HarperCollins, a division of News Corp., announced plans to convert about 20,000 books in its catalog into digital form in an attempt to curb potential copyright violations and protect its authors' rights. The publisher has no immediate plan to raise revenue from the digital copies. HarperCollins will hold all the copies in a digital warehouse and will allow such companies as Google, Yahoo and Amazon.com to create an index, thereby helping users to locate the full work. The publisher has already invited proposals from vendors for the digitization.

REPORT EXAMINES ILLICIT INTERNET DRUG SALES

A survey of web sites selling controlled substances to U.S. residents showed that many sites are based in the U.S. and have been in operation for more than one year, according to a report prepared for a House Energy and Commerce subcommittee. IntegriChain, a New Jersey company that works for pharmaceutical manufacturers, prepared the report based on a sample of 180 web sites that advertised the sale of Schedule 2, 3 and 4 drugs. Those sites represented 129 distinct operations because some organizations operate multiple web sites. The report did not cover some of the drugs commonly advertised over the Internet, such as Viagra or Lipitor, since they are not controlled substances. The company said its findings question whether the more dangerous Schedule 2 drugs, such as Ritalin or Percocet, are easily available over the Internet, but the sale of anabolic steroids, which are Schedule 3 drugs, was a cause for concern.

FTC REPORT: CAN-SPAM ACT IS EFFECTIVE

The Federal Trade Commission (FTC) released a report to Congress finding that, although about 70 percent of the world's e-mail messages continue to be spam, the amount of spam is leveling off, cited as evidence that the Can-Spam Act is effective in protecting consumers. The FTC based its conclusions on data from e-mail security company MX Logic, which calculated that an average of 68 percent of the messages it screened in the past year were spam, down from an average of 77 percent the previous year. However, the company also reported that only three

percent of the total messages it screened last year and four percent this year met the FTC-mandated standards of providing a subject line that comports with the body of the message, a postal address, an opt-out link and, in the case of adult-oriented e-mail, a "SEXUALLY EXPLICIT" label in the subject line. MX Logic derives its numbers by evaluating a random sample of 10,000 messages each week from about 7,000 of its business clients. The report can be accessed at:

<http://www.ftc.gov/reports/canspam05/051220canspamrpt>.

And more FTC news...

FTC STUDY FINDS MASKING AND FILTERING STOPS SPAM

The Federal Trade Commission (FTC) released a study finding that unmasked e-mail addresses received more than 6,400 spam messages, while only one spam message reached masked e-mail addresses. Masking is the technique of altering an e-mail address to make it readable by people but not by computers. The agency looked at three aspects of spamming and efforts to control it: the automated harvesting of e-mail addresses on public areas of the Internet; using e-mail address masking to reduce address harvesting; and the effectiveness of spam filtering by Internet service providers (ISPs). To conduct its five-week study, the FTC established 50 test e-mail accounts at each of three separate ISPs, but only two ISPs used spam filters. It also posted 50 e-mail addresses on various web sites, chat rooms, message boards, USENET groups and blogs. The study found that messages posted in chat rooms, message

boards, USENET groups and blogs proved less likely to be harvested than those on general web sites. In addition, e-mail accounts at the ISP without a filter received 8,885 spam messages, while accounts at the ISPs that filtered received 1,208 spam messages (more than 86 percent blocked) and 422 spam messages (more than 95 percent blocked) respectively.

STUDY FINDS EMPLOYEES BYPASSING E-MAIL POLICIES

Six percent of workers admitted e-mailing confidential company information to someone they should not have, according to a study by the Radicati Group, a messaging research firm. The survey also found that the majority of corporate employees circumvent company e-mail controls by using their personal e-mail accounts. Sixty-two percent of those polled admitted to sending business messages from their personal accounts; 25 percent said that they regularly forwarded mail from their business to their personal account. Additionally, seventy percent of those polled had received offensive messages in their business inboxes, while 42 percent had received e-mail containing foul language from co-workers or business associates.

NJ LAWYERS' INTERNET ADS MUST SAY THEY WERE PAID FOR

The New Jersey Supreme Court's Committee on Attorney Advertising issued Opinion 36, "Internet Advertising and Disclaiming Impermissible Lawyer Referral Service," which says that attorney listings or ads must include wording that they were paid for and that the host is not acting as a referral

service. The opinion came in response to an attorney's inquiry into whether listing his web page on a site run by a private commercial advertising and marketing enterprise, where the attorney pays a flat fee for the listing and receives an exclusive listing for a particular county in a specific practice area, is permissible under the Rules of Professional Conduct. The committee said it was if the listing contains a prominently displayed disclaimer, in a font at least equal to the largest and most prominent font and type on the site, declaring that "all attorney listings are a paid attorney advertisement, and do not in any way constitute a referral or endorsement by an approved or authorized lawyer referral service." Including such language would ensure that the ad or listing comports with RPC 7.1, which allows lawyers to pay for advertisements, given certain restrictions, and RPC 7.2, which exempts lawyers from allowing someone else to promote their services if the promoter is operated, sponsored or approved by a bar association.

PATENT OFFICE JOINS EFFORT TO IMPROVE SOFTWARE PATENTS

The U.S. Patent and Trademark Office announced that it will cooperate with open source software developers on three initiatives to improve the quality of software patents. The office had come under increasing pressure from critics who contend that it issues patents without adequate investigation of earlier inventions, resulting in litigation. The open source project, which is being led by the IBM Corp., would build an automated system for creating a series of categories to organize software written by open source programmers and would

help patent examiners search for earlier examples in patent applications. Another initiative would set up a system on the patent office web site where people could submit search criteria and subscribe to electronic alerts about patent applications in specific areas. The third initiative, which is based on the work of R. Polk Wagner, an intellectual property expert at the University of Pennsylvania, would create a patent quality index that would serve as a tool for patent applicants to use in writing their applications.

HOMELAND SECURITY AWARDS GRANT FOR OPEN SOURCE AUDITS

The U.S. Department of Homeland Security (DHS) awarded a \$1.24 million, three-year grant to Stanford University and software vendors, Coverity Inc. and Symantec Corp., to fund daily security audits and

analysis of more than 40 open source projects, including Apache, Linux, Mozilla, MySQL and PostgreSQL. The grant, known as the Vulnerability, Discovery and Remediation Open Source Hardening Project, is part of an initiative by the DHS Science and Technology Directorate to encourage the development and deployment of technologies to protect key computer system networks. Under the terms of the grant, Stanford will receive \$841,276 to provide recommendations for developing secure open source software; Coverity will receive \$297,000 to conduct automatic daily security audits of the open source projects using its Prevent system; and Symantec will receive \$100,000 to provide recommendations on best security practices and on how to deploy software securely in order to lower the incidence of attacks. Coverity expects to have the daily audits for an initial 40 open source projects operational by March 2006.

LEGISLATION UPDATE

Identity Theft

New Jersey's Identity Theft Prevention Act took effect on January 1, 2006. The law (1) ensures that consumers can request a reporting agency to place a security freeze on their credit report; (2) gives consumers the right to receive a copy of a police report on suspected identity theft; (3) requires companies that collect and maintain computerized records of consumers' personal information to notify affected consumers in the event the data is compromised; and 4) limits use of a consumer's social security number as an identifier and prohibits public display and usage of the social security number on printed materials except when required by law. In addition, businesses are required to destroy records

containing a consumer's personal information when it is no longer needed.

Ed. note: The editor thanks Darryl Neier, Director of Litigation at Sobel & Co., for the above information.

Pennsylvania Governor Edward Rendell signed SB 712, the "Breach of Personal Information Notification Act," into law, which requires state agencies, political subdivisions, individuals or businesses operating in the state and storing or maintaining personal consumer information to notify those consumers if their security systems are breached. Notification of the breach may be made in writing, by telephone or via e-mail. It may also be done by a combination of e-mail, posting on the entity's

web site or notification to statewide media if the cost of providing notice is in excess of \$100,000 and would affect at least 175,000 people. If an entity provides notification to more than 1,000 people at once, it must also notify national consumer credit reporting agencies. Notification may be delayed if a law enforcement agency decides it will impede their investigation. A violation of the act constitutes an unfair or deceptive practice under the state's consumer protection law, and the state Attorney General is authorized to bring actions for such violations.

The Utah Senate Business and Labor Committee approved, 5-1, SB 69, a bill that would allow consumers to put freezes on their credit reports so that they could only be accessed with a password. Credit reporting agencies could charge fees for freezing reports, and consumers could sign up to have their reports frozen by paying the fees and sending certified letters. Conversely, the bill requires credit reporting agencies to unfreeze reports in 15 minutes or less. If the bill is enacted, it would take effect on September 1, 2006, but enforcement would not begin until one year later.

Junk Faxes

The Indiana Senate Judiciary Committee approved, 9-1, HB 1280 which would prohibit unsolicited advertising faxes unless the sender has an existing business relationship with the person they are faxing to or if that person gave them permission to send the fax. The bill would allow the Indiana Attorney General's office to recover civil penalties of up to \$1,500 per violation.

Online Fraud

The U.S. Senate Commerce, Science and Transportation Committee approved S. 1608, legislation that would allow the Federal Trade Commission (FTC) to work more closely with foreign law enforcement officials to combat perpetrators of online fraud. The bill, sponsored

by Senator Gordon Smith (R-OR), would authorize the FTC to disclose confidential information to foreign agencies, as well as provide investigative assistance to them. It would also permit FTC attorneys to assist the Department of Justice in litigation in foreign courts on matters in which it has an interest. A similar measure passed a U.S. House committee last year, but did not make it to the House floor.

Voice Over Internet Protocol (VoIP)

The Senate Commerce, Science and Transportation Committee also approved S. 1063, which would direct the Federal Communications Commission (FCC) to establish requirements for VoIP providers to ensure that 911 and E-911 services are available to their customers. The bill, sponsored by Senator Bill Nelson (D-FL), requires that (1) IP access to 911 and E-911 services be nondiscriminatory, (2) IP providers give customers a conspicuous notice of the unavailability of 911 and E-911 services, and (3) IP providers and users receive immunity in the provision and use of 911 and E-911 services to the same extent as local exchange companies.

Cyber stalking

A prohibition on posting or sending e-mail messages with the intent to "annoy abuse, threaten or harass" any person without disclosing the true identity of the sender was signed into law as a provision of the Violence Against Women and Department of Justice Reauthorization Act. Inserted in the new law as Section 113 and entitled, "Preventing Cyber stalking," it provides criminal penalties of fines and up to two years in prison, or both.