

Cybercrime Newsletter

A JOINT PROJECT OF



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

HEDDA LITWIN, PROJECT COUNSEL & EDITOR

MAY-JUNE 2009

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, Cyberspace Law Counsel (hlitwin@naag.org, 202-326-6022).

This project is supported by grants provided 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

TABLE OF CONTENTS

FEATURES.....	1
AG'S FIGHTING CYBERCRIME.....	3
ETHICS OPINION.....	9
IN THE COURTS.....	9
SUPREME COURT UPDATE.....	12
LEGISLATIVE NEWS.....	13
NEWS YOU CAN USE.....	14
PUBLICATIONS OF INTEREST.....	17
SAVE-THE-DATE.....	17

like to feature articles written by you. Please contact us with information, proposed articles and comments about this newsletter. Thank you.

FROM THE BENCH: JUDGE SOTOMAYOR ON TECHNOLOGY

By Jennifer Adcock²⁰

If confirmed, Judge Sonia Sotomayor would become one of the most tech-savvy justices on the U.S. Supreme Court. In October of 2002, she authored the opinion in *Specht v. Netscape*,¹ a case involving downloadable software and contract formation over the Internet. The plaintiffs in *Specht* alleged privacy violations caused by software they downloaded from a web site maintained by the defendants.² In the process of downloading the software, a link to the license agreement was provided on the webpage in a location visible to the plaintiffs only if they had scrolled down past the "Download" button on their

screen.³ That license agreement contained an arbitration clause which the defendants attempted to enforce.⁴ The question was one of reasonable notice, and the Second Circuit denied the defendants' motion to compel arbitration, with Judge Sotomayor writing, "where consumers are urged to download free software at the immediate click of a button, a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms."⁵ She went on to say "there is no reason to assume that viewers will scroll down to subsequent screens simply because screens are there."⁶ Therefore, the court concluded that downloading of the software did not constitute acceptance of the license terms provided in the agreement, and the plaintiffs were not bound by the arbitration clause.⁷

Judge Sotomayor also wrote opinions for two cybersquatting cases; *Mattel v. Barbie-club.com*⁸ and *Storey v. Cello Holdings, LLC*.⁹ In *Mattel*, the trademark owner Mattel brought action against 57 Internet domain names¹⁰ under the Anticybersquatting Consumer Protection Act (ACPA) of 1999.¹¹ Judge Sotomayor's opinion, affirming the district court's dismissal, rejected Mattel's assertion that *in rem* jurisdiction exists "in any judicial district in which sufficient documents evidencing the disputed domain name are deposited with the district court."¹² Instead, she held that "it is the presence of the domain name itself" which is the subject of the jurisdiction and therefore an action may only be brought in the district where the domain name registrar, registry, or other domain name authority is located.¹³

Storey v. Cello Holdings involved a dispute over the domain name "cello.com."¹⁴ Earlier actions brought by Cello resulted in a dismissal with prejudice from the district court and subsequently an alternative dispute-resolution panel proceeding which ended in an order for the transferral of the domain name to Cello.¹⁵ Storey then brought a cause of action under the ACPA for a declaration that his use of the domain name was lawful and seeking a restora-

tion of cello.com back to him, arguing that the previous order for transfer was improper because Cello was barred from pursuing the claim following the district court's dismissal with prejudice.¹⁶ The district court agreed with Storey and held that the dismissal with prejudice barred Cello from reasserting its claims in arbitration.¹⁷ Judge Sotomayor, writing for the Second Circuit, reversed the district court decision, noting that "the ACPA treats rights to registration and use of a domain name as contingent upon the registrant's ongoing use of the domain name without a 'bad faith intent to profit' from a mark."¹⁸ The court held that an offer by Storey to sell the domain name to Cello following the dismissal of the first action, could possibly be interpreted as a "bad faith" intent and therefore could have given rise to a new claim under the ACPA.¹⁹

Only time will tell how Judge Sotomayor's background in technology-related cases might impact the Court. However, her previous experience with these issues could be seen by some as an asset to a Court that has and must continue to become increasingly tech-savvy.

¹*Specht v. Netscape*, 306F.3d 17 (2nd Cir. 2002).

²*Id.* at 21.

³*Id.* at 23.

⁴*Id.* at 24.

⁵*Id.* at 32.

⁶*Id.*

⁷*Id.* at 35.

⁸*Mattel v. Barbie-club.com*, 310 F.3d 293 (2nd Cir. 2002).

⁹*Storey v. Cello Holdings, LLC*, 347 F.3d 370 (2nd Cir. 2003).

¹⁰*Mattel* at 295-96.

¹¹15 U.S.C. 1125(d)(2).

¹²*Mattel* at 299.

¹³*Id.* at 302-03

¹⁴*Storey* at 373.

¹⁵*Id.*

¹⁶*Id.*

¹⁷*Id.*

¹⁸*Id.* at 378 (quoting 15 U.S.C. § 1125(d)(1)(A)(i)).

¹⁹*Id.* at 386

²⁰Jennifer Adcock is a law student at the University of Mississippi School of Law and is an intern with the Cyberspace Law Project at NAAG this summer.

ATTORNEYS GENERAL FIGHTING CYBERCRIME

MULTI-STATE

The Attorneys General of seven states sent a letter to Craigslist asking the company to detail its new policies and procedures for keeping pornography and prostitution off its new adult services section. **Attorneys General Richard Blumenthal of Connecticut, Lisa Madigan of Illinois, Douglas Gansler of Maryland, Jim Hood of Mississippi, Chris Koster of Missouri, Kelly Ayotte of New Hampshire and Tom Corbett of Pennsylvania** are members of the executive committee of a multi-state task force. The letter asks Craigslist to: 1) detail its steps to determine if a post is a prostitution ad; 2) describe in detail that manual review process to screen ads; 3) identify the criteria for refusing a posting; 4) provide the number of ads it has declined; and 5) advise if funds from adult services ads will be distributed to charitable organizations. The letter also asks the company to post contact information and links to law enforcement and child protection agencies in each state, major city and region.

The Attorneys General of 42 jurisdictions reached a settlement with TJX Companies, Inc. over allegations that the company did not provide adequate data security for its customers. TJX was the victim of a massive data breach in 2006 which potentially exposed the personal identifying information from tens of millions of TJMaxx, Marshalls, Home Goods and A.J. Wright transactions. A multi-state investigation uncovered several vulnerabilities and flaws in TJX's data security systems. The settle-

ment ensures that TJX will employ a comprehensive "Information Security Program" that assesses internal and external risks to consumers' personal information, implements safeguards that best protect consumer information and regularly tests and monitors those safeguards. TJX must also replace all wireless systems in their retail stores with wired systems, Wi-Fi Protected (WPA) systems or wireless systems as secure as WPA systems. The company must also conduct risk assessments in several areas of their daily business transactions and be subject to compliance and reporting requirements to prevent another breach. In addition, TJX will pay \$9.75 million to the participating states as follows: \$5.5 million for state data collection and consumer protection efforts; \$1.75 million for reimbursement of investigative costs; and \$2.5 million to fund a data security trust fund to be used to advance security enforcement efforts and policy development in the areas of data security and protecting consumers' personal information. **Attorneys General of the following jurisdictions participated in the settlement: Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Hawaii, Idaho, Illinois, Iowa, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Vermont, Washington, West Virginia and Wisconsin.**

ARIZONA

Attorney General Terry Goddard announced that Christopher Breiland was sentenced to 25 years in prison, lifetime probation and lifetime registration as a sex offender. Breiland pled guilty to two counts of sexual exploitation of a minor and one count each of attempted sexual exploitation of a minor and aggravated taking the identify of another. As part of an

investigation into an identify theft scheme, the U.S. Postal Inspection Service executed a search warrant at Breiland's home and discovered child pornography and a list of child pornography web sites. Subsequent forensic analysis of the computers that were seized revealed hundreds of child pornography images. Breiland had been convicted of 11 other felonies since 1987 and, at the time of his arrest, was wanted for absconding from bail. Assistant Attorney General Todd Lawson prosecuted the case.

CALIFORNIA

Attorney General Edmund Brown, Jr. petitioned the U.S. Supreme Court to uphold the state's law prohibiting the sale or rental of violent video games. The case stems from a 2005 California law that requires violent video games to be labeled with an "18," prohibits the sale or rental of these games to minors and authorizes fines of up to \$1,000 for each violation. The Video Software Association filed suit to block the law before it became effective. The U.S. District Court for the District of Northern California invalidated the law, and Attorney General Brown appealed. In February, the Ninth Circuit Court of Appeals upheld the district court ruling.

COLORADO

Attorney General John Suthers took part in a new public service announcement (PSA) campaign to encourage parents to use video game ratings, which are assigned by the Entertainment Software Rating Board. In the radio and TV ads, Attorney General Suthers urges parents to check the rating each time they purchase or rent a video game to ensure it is appropriate for their family, as well as to set controls on their game system. The PSAs are provided to stations and local cable TV operators across the state.

FLORIDA

Attorney General Bill McCollum's CyberCrime Unit arrested Michael Tyler on charges he used the Internet to sexually solicit a Pennsylvania teenager and groomed her to engage in sexual activity online. The Unit received a cybertip from Pennsylvania authorities after the victim called the National Suicide Hotline. Unit investigators executed a search warrant on Tyler's home and seized two computers and a laptop, which will undergo forensic analysis to identify additional evidence. Tyler admitted to soliciting the 15-year-old. He will be charged with one count of lewd and lascivious conduct, although additional charges may be added. The U.S. Immigration and Customs Enforcement, the state Department of Law Enforcement, the Pinellas County Sheriff's Office and the Clearwater Police Department assisted with the arrest as part of Attorney General McCollum's Tampa CyberCrime Task Force. The victim is receiving services from victim advocates.

HAWAII

Attorney General Mark Bennett announced that Chris Mabe was indicted for Electronic Enticement of a Child in the First Degree. He is accused of using the Internet to solicit a law enforcement officer who he believed to be a 14-year-old girl. In online chats, Mabe indicated that he wanted to engage in sexual activity with the "girl" and arranged to meet her. He was arrested when he arrived at the designated meeting place. The investigation and arrest were carried out by members of the state Internet Crimes Against Children Task Force. If Mabe is found guilty, Hawaii law requires that courts must impose a mandatory sentence of 10 years in prison.

ILLINOIS

Attorney General Lisa Madigan's investigators joined the Illinois Sex Offender Registry Team (I-SORT) to conduct compliance checks of 121 registered sex offenders to ensure that they are living at the locations where they are registered. While 63 offenders were determined to be in compliance with the sex offender registration laws, 31 offenders were not, and Attorney General Madigan's office and I-SORT members will investigate. Participants also left notices to comply with reporting at the residences of 27 offenders who did not answer or were not home when investigators arrived.

KANSAS

Attorney General Steve Six took part in a new public service announcement (PSA) campaign to encourage parents to use the Entertainment Software Ratings Board's video game ratings. In the radio and TV ads, Attorney General Six urges parents to check the rating whenever they buy or rent a video to ensure its appropriateness for their family, as well as take advantage of the Board's new "rating summaries" for greater detail about game content.

KENTUCKY

Attorney General Jack Conway announced the indictment of James Donovan on five counts of distribution of matter portraying a sexual performance by a minor, four counts of possession of matter portraying a sexual performance by a minor and one count of tampering with physical evidence for allegedly reformatting his computer hard drive after learning about an investigation involving his computer. All counts are class D felony charges. The investigation was conducted by Attorney General Conway's Cybercrimes Unit, a member of the Internet Crimes Against Children Task Force.

LOUISIANA

Attorney General James "Buddy" Caldwell announced that Ronnie Green was arrested and charged with one count of Pornography Involving Juveniles. Following an undercover investigation by the Baton Rouge Police Department, a search warrant was obtained for Green's residence. Attorney General Caldwell's High Tech Crime Unit, the Baton Rouge Constable's Office, East Baton Rouge Sheriff's Office, Immigration Customs Enforcement, FBI and the West Baton Rouge Sheriff's Office - all members of the Internet Crimes Against Children Task Force - assisted in the search of Green's residence and his arrest.

MARYLAND

Attorney General Douglas Gansler sent letters to companies that advertise on Peoplesdirt.com, an Internet forum that solicits and publishes anonymous and malicious personal attacks on teenaged children, informing them that the site misrepresents itself as "suitable for persons ages six and older" and a site that does not contain explicit sexual content or suggestive themes. Attorney General Gansler also sent a letter to the Go Daddy Group, the company that hosts the Peoplesdirt.com web site, informing them that Peoplesdirt.com appears to violate the company's "Morally Objectionable Activities" clause in its Terms of Service Agreement. That clause states that Go Daddy reserves the right to terminate service for sites whose content contains morally objectionable activities which "defame, embarrass, harm, abuse, threaten, slander or harass third parties." While the site is divided geographically with categories for all 50 states, the majority of posts are in the Maryland category.

MASSACHUSETTS

Attorney General Martha Coakley's Computer Forensics Lab received the 2009 Computer and Enterprise Investigations Conference Excellence in Computer (CEIC) Forensics Award for its distinction as one of the premier computer forensics labs in the country. David Papargiris, Director of the Lab, accepted the award on behalf of Attorney General Coakley's office. The CEIC award is given in honor of Bill Seibert, a Northeastern University Criminal Justice graduate and employee of Guidance Software who, during his 20-year law enforcement career, conducted complex investigations and successful prosecutions involving the sexual exploitation of children and fraud.

MISSISSIPPI

Attorney General Jim Hood announced that Isaac Hartley was arrested and charged with 10 counts of possession of child pornography. The arrest was made by investigators with the Internet Crimes Against Children (ICAC) Unit of Attorney General Hood's Cyber Crime Division, with assistance from the Madison and Ridgeland Police Departments and other ICAC Task Force affiliates. Hartley faces a minimum of five years and up to 40 years in the custody of the state Department of Corrections for each count, for a potential minimum of 50 years in prison.

MONTANA

Attorney General Steve Bullock's office filed a complaint against AirTEL Wireless, a Minnesota-based cell phone provider that operated in the state until abruptly closing its doors without reimbursing its customers. Also named in the suit was Alan Gingold, AirTEL's managing member. The complaint charges AirTEL with violating Montana's Unfair Trade Practices and Consumer Protection Act by continuing to sell its services despite knowing that they were

going out of business and the services sold would have no value. The complaint says that the company owes state consumers over \$106,000.

NEW JERSEY

Attorney General Anne Milgram announced that Daniel Zaremba was charged in a state grand jury indictment with second-degree distribution of child pornography and fourth-degree possession of child pornography. The indictment alleges that Zaremba knowingly used Internet file sharing software to make multiple video and photograph files containing child pornography on his computer readily available for another user to download from a designated shared folder. Zaremba was arrested by the New Jersey State Police, and a search warrant executed on his computer revealed images of child pornography. A subsequent forensic examination revealed at least 59 files with titles indicative of child pornography. The Digital Technology Investigation Unit of the State Police coordinated the investigation, and Deputy Attorney General Lee Schaer prosecuted the case for Attorney General Milgram's Division of Criminal Justice Major Crimes Bureau. Second-degree crimes carry a maximum sentence of 10 years in prison and a fine of \$150,000, and fourth-degree crimes carry a maximum sentence of 18 months in prison and a fine of \$10,000.

NEW YORK

Attorney General Andrew Cuomo entered into a settlement with computer security software vendors Symantec and McAfee to resolve claims that the companies renewed customers' software subscriptions without their knowledge or authorization. Under the settlement, both companies will make detailed disclosures to consumers about subscription terms and renewal, and each will pay \$375,000 in penalties and costs. Attorney General Cuomo's office conducted an extensive investigation into the

companies' online marketing and sales practices and found that they failed to adequately disclose to consumers that subscriptions would be automatically renewed and customers charged. In addition, the investigation revealed that it was difficult for consumers to contact the companies in order to opt out or request refunds. Under the settlement, both companies will clearly disclose any automatic renewal program and provide an easy, automated means for consumers to opt out. They will also provide electronic notification before and after renewal of the subscription and clearly disclose the length of time they will continue to support and provide updates to the software. The investigation was conducted by Assistant Attorneys General Carolyn Fast and Clark Russell, with assistance from Investigator Vanessa Ip, under the direction of Justin Brookman, Chief of the Internet Bureau, and Michael Berlin, Deputy Attorney General for Economic Justice.

OKLAHOMA

Attorney General Drew Edmondson sent a memorandum to all state agencies reminding them of their responsibilities under state law following a data security breach. The memo comes after three agencies reported the loss of sensitive personal information. After such a breach, state law requires that the agency send written notice to affected people without unreasonable delay.

OREGON

Attorney General John Kroger announced that Rick Prather was sentenced to nearly 10 years in prison after pleading guilty to a 16-count indictment, which included charges of using a child in a display of sexually explicit conduct and encouraging child sexual abuse in the first degree. Kroger received a 115-month prison sentence and because the charges are Measure 11 crimes, he is not eligible for early release. Prather admitted persuading

three underage girls to send sexually explicit photographs of themselves to his cell phone. His arrest and conviction followed an investigation by Attorney General Kroger's Internet Crimes Against Children unit. Senior Assistant Attorney General Michael Slauson prosecuted the case in cooperation with the Deschutes County District Attorney's Office.

PENNSYLVANIA

Attorney General Tom Corbett announced the arrest of Alan Berlin, who is accused of using Internet chats and instant messages to sexually proposition a 15-year-old boy. According to the criminal complaint, Berlin, a former state Senate staff member, also requested nude photos of the boy and suggested arranging a meeting with the boy and another adult so he could take photos. The boy's parents discovered sexually graphic messages on their son's computer and contacted Attorney General Corbett's Child Predator Unit, which began an investigation and, assisted by officers from the Carlisle and North Middleton Township Police Departments, arrested Berlin. Berlin is charged with one count of unlawful contact with a minor (related to deviate sexual intercourse), a first-degree felony punishable by up to 20 years in prison and a \$25,000 fine; one count each of unlawful contact with a minor (related to sexual exploitation of children), criminal attempted sexual exploitation of children and criminal attempted sexual abuse of children (related to child pornography), all second-degree felonies, each punishable by up to 10 years in prison and \$25,000 fines; and one count each of unlawful contact with a minor and criminal use of a computer, both third-degree felonies punishable by up to seven years in prison and \$15,000 fines.

SOUTH CAROLINA

Attorney General Henry McMaster announced that Corey Lancaster was arrested in an undercover Internet sting conducted by the City of Greenville Police Department, a member of Attorney General McMaster's Internet Crimes Against Children Task Force. Lancaster was arrested on one count of Criminal Solicitation of a Minor, a felony punishable by up to 10 years imprisonment, and one count of Attempted Criminal Sexual Conduct with a Minor, a felony punishable by up to 20 years imprisonment. Arrest warrants allege that Lancaster solicited sex on the Internet from an individual he believed to be a 13-year-old girl, but he was really communicating with an undercover police officer. Lancaster arranged to meet the "girl" for sex and was arrested upon his arrival at the predetermined location. He consented to a search of his residence, and a computer was seized. The Laurens County Sheriff's Office, also a Task Force member, assisted with the search. The case will be prosecuted by Attorney General McMaster's office.

UTAH

Attorney General Mark Shurtleff announced that Kyle Fuchs of Massachusetts was sentenced to eight to 10 years in prison after Steve Gamvroulas, an investigator with the Utah Internet Crimes Against Children Task Force, identified him and one of his victims in child pornography pictures. Fuchs was sentenced for raping three girls and posting online photos of his victims. Gamvroulas contacted the Massachusetts State Police, and Fuch's computer was seized. Investigators found 5,000 more sexually explicit images of underage girls, including 174 pictures where the girls could be identified.

WASHINGTON

Attorney General Rob McKenna's office filed a civil lawsuit against Wizzy-Wiz eCommerce, accusing the company's owners of repeatedly failing to honor their promises to help businesses sell their products online. Attorney General McKenna's office received 22 complaints from customers, who claim they are owed an average of \$1,800 each. The complaint names Jeremy Avey, Alexander Martin and Brent Stamphill as defendants, in addition to three businesses: Cybercom Technologies; TNT Cart, also operating as Strada Technologies; and White Crane Technologies. Defendants advertised services such as shopping cart integration, search-engine optimization, web site design and competitor research, but are accused of misrepresenting the quality of their services, neglecting to deliver services as promised, proving poor customer service, failing to honor money-back guarantees, making unauthorized charges to consumers' debit and credit accounts and threatening legal action against consumers who post negative comments to online forums. The state seeks injunctive provisions to stop the alleged violations, civil penalties and restitution for affected consumers.

WISCONSIN

Attorney General J. B. Van Hollen recognized the Whitewater Police Department for their work on the Internet Crimes Against Children Task Force. It was nominated for the recognition award by Special Agent Eric Szatkowski for their assistance in a child pornography investigation.

ETHICS OPINION: MINING SOCIAL NETWORKS

In March, the Philadelphia Bar Association's Professional Guidance Committee issued an advisory opinion, No. 2009-2, which addressed an inquiry by an attorney who wanted to dig for relevant evidence on a witness' Facebook and MySpace accounts. The attorney wanted to hire a third party who would try to gain access to the accounts through the witness' friendship networks ("befriending" a person in social networking speak) without revealing that he or she would be mining for information to give to the attorney. The attorney asked whether this conduct was permissible under the Rules of Professional Conduct and whether he could use any information obtained.

The Committee was adamant that "friending" under false pretenses was deception. It noted that the attorney was responsible for the conduct of the third party under Rule 5.3: Responsibilities Regarding Nonlawyer Assistants. Therefore, the attorney is responsible for the misdeeds of a third party he or she employs to assist in covert operations.

The Committee also determined that such conduct would violate Rule 8.4©: Misconduct by "engaging in conduct involving dishonest, fraud, deceit or misrepresentation." Since the proposed conduct purposely concealed a material fact from the witness, it would rise to the level of misconduct. The Committee also distinguished between Internet social networks as "private areas" which are closed to the general public, as opposed to public areas on the Internet.

Some jurisdictions have carved out exceptions to the ethical rule against attorney use of deception. As noted in the opinion, the New York Lawyers' Association Committee on Professional Ethics issued an opinion in May 2007 finding that the use of deception in the investigation of civil rights or intellectual property violations that were currently taking place or imminent was permissible. The Oregon Ethics Rules were amended to allow deceptive practices if "the lawyer in good faith believes there is a reasonable possibility that unlawful activity has taken place, is taking place or will take place in the foreseeable future." However, the Philadelphia Bar Committee, like its counterpart in Colorado, has disallowed such carve-outs.

IN THE COURTS

FOURTH AMENDMENT: DELAY IN OBTAINING SEARCH WARRANT

U.S. v. Mitchell, 2009 WL 1067212 (11th Cir. April 22, 2009). The 11th Circuit held that a federal agent's 21-day delay in seeking a warrant to search the computer hard drive seized from a suspect required that the evidence eventually obtained from that warrant be suppressed. Police suspected Peter Mitchell of downloading child pornography and went to his home to talk to him. Mitchell admitted that his computer probably contained child pornography, but would not consent to a search, so the lead agent seized his computer hard drive to prevent destruction of evidence. Three days later, the agent left for a two-week training course. When he returned, three weeks after the seizure, he applied for and was granted a search warrant for the drive, where images of child pornography were found. Mitchell was charged with receipt and possession of child pornography. He filed a motion to suppress the evidence obtained from the delayed warrant, arguing the delay in obtaining the warrant was unreason-

able, but the U.S. District Court for the Southern District of Georgia denied the motion. So Mitchell pled guilty to the charges, conditional on his right to appeal the motion in the 11th Circuit. The 11th Circuit held that the evidence found on the hard drive had to be suppressed. The court found that a personal computer “is the digital equivalent of its owner’s home, capable of holding a universe of private information...” and the delay was a significant interference with Mitchell’s possessory interest. The court noted that even a lawful search can violate the Fourth Amendment because its execution unreasonably infringes on possessory interests protected by the Fourth Amendment’s prohibition on unreasonable searches. The court also concluded that the government had failed to show that the agent could not have obtained the warrant sooner. Mitchell’s conviction was vacated.

COMMUNICATIONS DECENCY ACT: ISP FAILURE TO REMOVE POST

Barnes v. Yahoo! Inc., 2008 WL 1232367 (9th Cir. May 7, 2009). The Ninth Circuit Court of Appeals held that the Communications Decency Act (CDA) provides no protection to an Internet service provider who promises, but then fails, to remove content provided by a third party. Cecilia Barnes’ ex-boyfriend posted nude photos of her, solicitations to engage in sexual relations with her and her contact information on Yahoo! web sites and chat rooms. Barnes sent Yahoo! many formal requests to remove the posts, but to no avail. Right before a local news station did a story on her plight, Yahoo’s director of communications contacted Barnes and promised to remove the posts. Barnes relied on this promise and took no further action, but the posts were not removed. Barnes then sued Yahoo! for negligent undertaking and promissory estoppel. In response, Yahoo! moved to dismiss, arguing that it was immune from liability under § 230 of the CDA. The U.S. District Court for the District of Oregon granted

the motion, and Barnes appealed. The Ninth Circuit agreed with the district court as to the negligent undertaking claim, but not as to promissory estoppel. In doing so, the court distinguished between Yahoo’s failure to remove the posts and Yahoo’s failure to keep its promise to remove the posts. As to the former, the court noted that Ninth Circuit precedent holds that the CDA shields an Internet service provider when it is performing the customary duties of a publisher, including reviewing, editing and deciding whether to publish or remove third party content, such as in Yahoo’s actions in deciding whether to take down the posts as requested by Barnes. However, promising to take action is different, as contract law treats a promise as creating an expectation on the part of another and therefore a legal duty. The court found that while the CDA provides protection when Yahoo was acting as a publisher, it did not provide protection when Yahoo failed to keep its promise to remove the posts. The court therefore affirmed as to the negligent undertaking claim, but reversed as to the promissory estoppel claim and remanded.

FOURTH AMENDMENT: ATTACHING GPS DEVICE

State v. Sveum, 2009 Wisc App. LEXIS 343 (May 7, 2009). The Wisconsin Court of Appeals has ruled that attaching a Global Positioning System (GPS) device on the outside of a car does not violate the Fourth Amendment. Michael Sveum, who had been convicted of and imprisoned for stalking Jamie Johnson, continued to stalk her after his release. Johnson reported his stalking to the police, and they obtained a warrant authorizing them to covertly attach a GPS device to Sveum’s car in order to track it. They attached the device on the car when it was parked in Sveum’s driveway. Five weeks later, the police retrieved it and downloaded a detailed history of the vehicle’s movements during that time period. Based on that information, the police obtained a

warrant to search Sveum's residence and car, where they found more evidence incriminating him. Sveum was charged with aggravated stalking. At trial, he moved to suppress the tracking evidence from the GPS device, arguing that it violated his Fourth Amendment right to be free of unreasonable searches and seizures. The trial court denied his motion, and he was found guilty. On appeal, the Wisconsin Court of Appeals affirmed, finding that no search or seizure occurs when police use a GPS device to track a vehicle while it is visible to the general public. The court relied on two U.S. Supreme Court cases involving a beeper attached to property inside a vehicle: *U.S. v. Knotts*, 460 U.S. 276 (1983), which held that it did not implicate the Fourth Amendment to use a beeper to track a vehicle in public view; and *U.S. v. Karo*, 468 U.S. 705 (1984), which held that it did not violate the Fourth Amendment to use a beeper to obtain information that could not be obtained by observation from outside a property's cartilage. The court also relied on a case from the Seventh Circuit, *U.S. v. Garcia*, 474 F. 3d 994 (7th Cir. 2007), which held that attaching a GPS device to a car was not a Fourth Amendment search.

COMMUNICATION WITH A MINOR: OVERBREADTH CHALLENGE

State v. Aljutily, 202 P.3d 1004 (Wash. Ct. App. March 13, 2009). The Washington Court of Appeals upheld a state statute prohibiting communication with a minor for the purpose of exposing or involving a minor in sexual misconduct. Tarig Aljutily appealed his felony conviction for communication with a minor for immoral purposes, arguing that the statute under which his conviction was based, RCW 9.68A.090(2), is unconstitutionally overbroad and burdens protected speech. Aljutily's charge and subsequent conviction stemmed from his online communications with two police officers posing as a fictitious 13-year-old girl named "Amber." Aljutily

contacted "Amber" through a MySpace profile and later through a Yahoo instant messenger account, both of which were set up by the police. He sent her sexually explicit photographs of himself and communicated his interest in engaging in sexual intercourse with her. On several occasions during the communications, both Aljutily and the officers posing as "Amber" made references to her being only 13 years old. Aljutily contended that the statute violates the overbreadth doctrine because (1) it penalizes communication with someone the person believes to be a minor without requiring that the belief be objectively manifested, and (2) there is no scienter required when the communication involves an actual minor. He claimed that there is no requirement that when an actual minor is involved, the speaker know that the minor is in fact a minor. Prior case law has interpreted the statute to prohibit communication, by words or conduct, that is (1) done for immoral purposes, (2) intended to reach a minor, and (3) received by a minor or someone the person believed to be a minor. The appeals court held that the requirements that the communication be made with the intent that it reach a minor and done with the immoral or predatory purpose of exposing or involving a minor in sexual misconduct sufficiently limits the amount of speech or conduct that the statute regulates and ensures that a substantial amount of protected expressive activity is deterred. Therefore the court held that the statute is not overbroad under either the *First Amendment* or *article I, section 5 of the Washington Constitution*. Aljutily's conviction was affirmed.

Ed. Note: This case was reviewed by Jennifer Adcock, a law student from the University of Mississippi School of Law, who is currently an intern for the summer at the National Association of Attorneys General (NAAG) under its contract with the National Center for Justice and the Rule of Law at the University.

UNAUTHORIZED USER OF WEB SITE: TERMS OF USE

CoStar v. Field, 2009 WL 841132 (D. Md. March 31, 2009). The U.S. District Court for the District of Maryland found that a user who gains access to a web site by using another subscriber's account and password is subject to the web site's terms of use. CoStar, a company maintaining an online real estate database for paying subscribers, sued Lawson and Gresset, d/b/a TGC Realty Counselors, two out-of-state companies, for breach of contract and tortious interference with contract, claiming both companies accessed the web site by using a paid subscriber's account and password. The complaint was filed in federal court in Maryland pursuant to the forum selection clause in the web site's terms of use. Lawson and Gresset moved to dismiss for lack of jurisdiction, arguing that they did not have sufficient contacts with the state to satisfy its long arm statute or due process. The district court noted that a user was required to actively consent periodically to the terms of use. Therefore Lawson and Gresset, by periodically assenting to the terms of use, explicitly and implicitly assented to its terms and were bound by them. The court also relied on *Burcham v. Expedia*, 2009 WL 586513 (E.D. Mo. March 6, 2009), which held that the decision as to whether online contracts are binding should be made using traditional contract principles of reasonable notice and manifested consent. The motion to dismiss was denied.

CONVICTED SEX OFFENDERS: LOCAL RESIDENCY RESTRICTIONS

G.H. v. Township of Galloway, 2009 WL 1272549 (NJ May 7, 2009). The New Jersey Supreme Court upheld a lower court's opinion invalidating local residency restrictions that set up buffer zones for convicted sex offenders living in their communities. The local ordinance in Galloway Township

provided that a registered sex offender was prohibited from living within 2,500 feet of a school, park, playground or daycare center. A violation of the ordinance would require the offender to move within six months or face a fine of up to \$5,000, up to six months in prison and up to 90 days of community service. The Cherry Hill Township ordinance was similar, but provided for fines per offense up to \$1,250, together with up to 90 days imprisonment and up to 90 days of community service. The appellate court determined that Megan's Law preempted and therefore invalidated the local ordinances, and the state Supreme Court affirmed.

SUPREME COURT UPDATE

The U.S. Supreme Court declined to take up an appeal in *Commonwealth v. Sodomsky*, in which Kenneth Sodomsky sought to suppress evidence of child pornography found on his computer. Sodomsky had taken his computer to Circuit City to have a DVD burner installed. While testing to ensure the burner worked, the technician encountered child pornography files and contacted his manager, who telephoned the police. Sodomsky's computer was seized, and police obtained a search warrant to search it and found child pornography.

On appeal, the Pennsylvania Superior Court reversed the lower court, which had held that the files were inadmissible. The Superior Court found that "If a person is aware of, or freely grants to a third party, potential access to his computer contents, he has knowingly exposed the contents of his computer to the public and has lost any reasonable expectation of privacy in those contents." 939 A.2d 363, 369 (Pa. Super. Ct. 2008). The Pennsylvania Supreme Court agreed.

LEGISLATIVE NEWS

INTERNET TAXES

LOUISIANA. On June 4, the Louisiana House passed HB 569, a bill that would levy a 15 cent monthly surcharge on Internet access in the state. The bill was introduced at the request of Attorney General Buddy Caldwell, and the revenue collected would finance a division in the Attorney General's Office that investigates Internet crimes, particularly online child exploitation. It would take effect on January 1, 2010.

Ed. Note: Just before this issue went to press, the Commerce, Consumer Protection and International Affairs Committee of the Louisiana Senate voted without objection to defer the bill, essentially preventing a full Senate vote. The committee also rejected a proposed amendment that would have instead allowed for voluntary donations to the Attorney General's online investigations unit.

DATA SECURITY

NEVADA. On May 29, Nevada Governor James Gibbons signed SB 227 into law, which will require entities doing business in the state to encrypt data storage devices containing personal information that they move outside their physical and logical storage boundaries.

U. S. HOUSE. On June 3, H.R. 2221, a bill sponsored by Representative Bobby Rush (D-IL) was amended and approved by the Subcommittee on Commerce, Trade and Consumer Protection and forwarded to the full Committee on Energy and Commerce. The bill would require any person or entity engaged in interstate commerce and possessing personal information in electronic form to establish data security policies and procedures to protect such data.

STRATEGIC TECHNOLOGY PLANNING

On May 12, HR 2020, a bill sponsored by Representative Bart Gordon (D-TN) that would authorize support of networking and information technology research and require federal agencies to develop a five year strategic plan to be updated every three years, was amended and passed by a 2/3 majority of the House. The bill was received in the Senate and referred to the Committee on Commerce, Science, and Transportation.

The following bills have been introduced since the last issue of the Cybercrime E-Newsletter.

INTERNET GAMBLING

On May 6, Representative Barney Frank (D-MA) introduced HR 2267, a bill that would establish a licensing and enforcement framework to permit licensed operators to accept wagers for Internet gambling. It includes safeguards against compulsive and underage gambling, money laundering, fraud and identity theft. The bill would allow for individual states and Indian tribes that have pre-existing state laws limiting Internet gambling to opt out of licensing within 90 days from the bill becoming law. State Attorney Generals would also be permitted to bring civil actions in order to enjoin or to force compliance with the Act. The bill was referred to the Committee on Financial Services, the Committee on Energy and Commerce, and the Committee on the Judiciary.

On May 6, Representative Jim McDermott (D-WA) introduced HR 2268, a bill that would require Internet gambling operators to file returns identifying themselves and the individuals placing wagers with them. It would also ensure that gambling winnings are taxed. The bill was referred to the Committee on Ways and Means.

Also on May 6, Representative Frank introduced H.R. 2266, a bill that would delay from December 1, 2009 to December 1, 2010 compliance with the Unlawful Internet Gambling Enforcement Act of 2008. The legislation was prompted by financial sector concerns over the industry's ability to identify and block unlawful Internet gambling transactions. The bill was referred to the Committee on Financial Services.

COMPUTER-ASSISTED REMOTE

HUNTING

On May 7, Representative Steve Cohen (D-TN) introduced HR 2308, a bill that would prohibit computer-assisted remote hunting. Violators would be fined under Title 18 or imprisoned up to five years. The bill was referred to the Committee on the Judiciary.

FOREIGN ONLINE CENSORSHIP

On May 6, Representative Christopher Smith (R-NJ) introduced HR 2271, a bill to ban U.S. Internet web hosting servers from responding to or sending personal identifying information to a country that restricts Internet use. The bill was referred to the Committee on Foreign Affairs and the Committee on Energy and Commerce.

INTERNET SAFETY

On May 14, Senator Bob Menendez introduced S 1047, a bill that would authorize grants for age-appropriate, research-based Internet safety education programs. The bill would also authorize a study on Internet safety. The bill was referred to the Committee on the Judiciary.

SEX OFFENDERS

On May 21, Representative Peter King (R-NY) introduced HR 2612, a bill authorizing grants and access to information from the National Crime Information Center databases to Parents for Megan's Law, Inc. to implement the Sex Offender Registration Tips Program. The bill was referred to the Subcommittee on Crime, Terrorism and Homeland Security. The Senate version of the bill is S 1146, introduced on the same day by Senator Charles Schumer (D-NY) was referred to the Committee on the Judiciary.

On May 6, Representative Bobby Scott (D-VA) introduced HR 2289, a bill that would require states to enact laws and develop policies to allow child offenders who are serving a life sentence to have a meaningful opportunity for parole or supervised release during their first 15 years of incarceration and at least once every three years thereafter. It also would authorize grants to states to improve legal representation for child offenders facing a potential life sentence.

NEWS YOU CAN USE

10 PERCENT OF VIDEOGAME PLAYERS ARE ADDICTED

Approximately one in 10 videogame players exhibit signs of addictive behavior that could have negative effects on their family, friends and school work, according to a new study. The study, conducted by researchers at Iowa State University and the National Institute on Media and the Family, found that some gamers show at least six of the 11 symptoms of pathological gambling, as defined by the American Psychological Association. Symptoms include lying about the amount of time they play games, using games to escape problems, becoming

restless or irritable when not playing and skipping homework and doing poorly in school because of the time spent playing. The researchers studied 1,178 American children and teenagers, aged eight to 18. They found that addicted gamers played 24 hours a week, twice as much as the casual gamer, and some even steal to support their habit. The findings will be published in *Psychological Science*, a journal of the Association of Psychological Science.

U.S. FALLS TO THIRD PLACE IN IP PROTECTION RANKING

The United States dropped from second place to third on the 2009 Global Intellectual Property Index, the second annual ranking of 24 countries on intellectual property protection and enforcement practices by Taylor Wessing, a European law firm. The U.S., which was the only country on the index to decline in ranking, is topped by the United Kingdom in first place and Germany in second. The index ranking includes five types of intellectual property: patents, trademarks, copyright, design and domain names. The U.S. rankings on each type varied widely. On copyright competitiveness, the U.S. ranked first due to its progressive copyright laws with fair use principles. On the domain name index, which measures ease of registering domain names, low infringement rates and/or effective dispute processes, the U.S. ranked second, behind the United Kingdom. It ranked in third place in patent competitiveness, behind the United Kingdom and Germany, because of the high cost of U.S. patent protection enforcement. The U.S. did poorly in design protection competitiveness, ranking fifth behind the United Kingdom, Germany, Australia and the Netherlands. Finally, the complex requirements for trademarks by the U.S. Patent and Trademark Office resulted in a sixth place ranking in trademarks, trailing the United Kingdom, Germany, Australia, the Netherlands and Canada. The full report can be accessed at <http://taylorwessing.com/>

[ipindex/](#).

FCC SUPPORTS NATIONAL PLAN FOR RURAL BROADBAND

On May 22, the Federal Communications Commission (FCC) issued a report on expanding broadband availability that recommends other agencies develop rural broadband strategies consistent with a national broadband plan the FCC will submit to Congress by February 17, 2010. The report, "Bringing Broadband to Rural America," was required by the 2008 farm bill. With increased deployment of high-speed Internet service to rural areas sometimes ignored by carriers, the report acknowledges that steps must be taken to overcome socio-economic barriers. It urges public and private sectors to develop consumer education and training initiatives and design programs to make high-speed Internet service more affordable. It also calls for the federal universal service fund, which subsidizes telecommunications costs in rural and low-income areas, to be expanded to include broadband. The full report can be accessed at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-291012A1.pdf.

WHITE PAPER ON CLOUD COMPUTING RELEASED

The Cloud Security Alliance, a non-profit organization formed to promote best practices for cloud computing security, released a white paper, "Security Guidance for Critical Areas of Cloud Computing." While the paper does not define cloud computing, it lists its five principal characteristics: abstraction of infrastructure, resource democratization, services-oriented architecture, elasticity/dynamism of resources and utility model of consumption and allocation. It also covers three cloud delivery models and four cloud service deployment and consumption modalities. In addition to explaining the basics of cloud computing, the paper also

includes 15 different challenges, including legal, electronic discovery and security issues. The paper may be accessed at <http://www.cloudsecurityalliance.org/guidance/csaguide.pdf>.

REPORT: 50% INCREASE IN MALWARE-INFECTED COMPUTERS

On May 5, online security provider McAfee released its first quarter security report for 2009, which found that 12 million more computers were infected by malware since January, a 50 percent increase from last year. The report also noted that the U.S. now hosts the largest percentage of infected computers at 18 percent, followed by China at 13.4 percent. The report also predicts that spam levels will rise again in 2009, as spammers recover from the shutdown of the McColo server farm in November. Since then, the volume of spam has increased by 70 percent. The report can be accessed at http://img.en25.com/Web/McAfee/5395rpt_aver_t_quarterly-threat_0409_v3.pdf.

STUDY: SOFTWARE PIRACY ON THE RISE

On May 12, the Business Software Alliance (BSA), an organization representing the software industry, released its sixth annual "Global Software Piracy Study," which found that software piracy rates rose from 38 percent in 2007 to 41 percent in 2008, meaning that 41 percent of all software installed is pirated. The study estimates that resulting losses to software companies was \$53 billion last year. Fortunately, piracy in the U.S. was the lowest in the world at only 20 percent of the total, since more software is sold in the U.S. than in any other country. The study noted that many losses stem from businesses that use unlicensed copies of soft-

ware. The full study may be accessed at <http://global.bsa.org/globalpiracy2008/index.htm>.

NIST BOARD WANTS FEDERAL PRIVACY REGS UPDATED

Federal privacy law should be updated to reflect today's technologies and information systems, as well as provide for advanced threats to privacy and security, according to a report sent by the National Institute of Standards and Technology's Information Security and Privacy Advisory Board (ISPAB) to Peter Orszag, Director of the Office of Management and Budget (OMB). The Board, which includes technology experts from industry and academia, calls for Congress to amend the 1974 Privacy Act and 2002 E-Government Act to improve privacy notices, cover commercial data sources and update the definition of "system of records." It suggests that OMB, as well as other major agencies, hire full-time chief privacy officers and that a council of chief privacy officers be created. The report, "Toward a 21st Century Framework for Federal Government Privacy Policy," said that the federal government's cookie policy should be updated to let visitors to federal government web sites decide whether a cookie is set, such as with a "remember me" check box. Additionally, the Board felt that OMB should issue privacy guidance for non-law enforcement use of location data by agencies, work with the Department of Homeland Security's U.S. Computer Emergency Readiness Team to create and share information on data loss and adopt a public reporting structure on how the government uses Social Security numbers. The full report can be accessed at <http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/spab-report-may2009.pdf>.

CONSUMER PRIVACY RELIANCE AND WEB TRACKING AT ODDS

Although most people want more control over how their personal information is used, that often clashes with the data collection practices of Internet companies, according to a privacy study by graduate students at the School of Information at the University of California, Berkeley. The students – Joshua Gomez, Travis Pinnick and Ashkan Soltani – studied consumer expectations by reviewing complaints filed with the Federal Trade Commission and data collected by the state of California. They analyzed company practices using Ghostery, a browser plug-in that detects cookies, web beacons and other trackers that allow third parties to gather information about web site visitors without their knowledge. In a sample of nearly 400,000 web domains, Google was the most conspicuous tracker on third party sites. Google Analytics, a free product that allows online publishers to gather statistics about visitors to their sites, was used on 81 of the top 100 sites. Cookies from DoubleClick, the advertising company owned by Google, were present on 70 of those sites. Combining trackers from both services, Google had a presence on 92 of the top 100 sites. Cookies from Atlas, Microsoft's DoubleClick rival, appeared on 60 sites, and trackers from two other analytics companies, Quantcast and Omniture, appeared on 54 sites. The full study can be accessed at <http://knowprivacy.org>.

PUBLICATIONS OF INTEREST

“The Right and Wrong Responses to Sexting”

This blog posting by Mary Lou Leary, Assistant Professor of Law at Catholic University of America, can be accessed at <http://www.thepublicdiscourse.com/viewarticle/php?selectedarticle=2009.5.12.001.pdart>.

Jerry Lee Crime Prevention Symposium

Presentations from the Symposium, held April 27-28, 2009, can be accessed at <http://gemini.gmu.edu/cebcp/jerryleepresentations.html>.

SAVE THE DATE

Please save the date for an in-depth training on Internet Crimes Against Children, scheduled for **October 13-15, 2009** at the University of Mississippi School of Law. Travel scholarships to attend will be available under the partnership between the National Association of Attorneys General Research and Training Institute and the National Center for Justice and the Rule of Law at the University of Mississippi. **Attorneys who need a long lead time to obtain approval from their office should start that process now.**