

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

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

SEPTEMBER-OCTOBER 2009

TABLE OF CONTENTS

FEATURES.....	1
AG'S FIGHTING CYBERCRIME.....	2
IN THE COURTS.....	6
LEGISLATIVE NEWS.....	11
NEWS YOU CAN USE.....	12
FREE SAFETY RESOURCE.....	15
EMPLOYMENT.....	17

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

SUPREME COURT GRANTS CERT IN SORNA CASE

By Hedda Litwin, NAAG Cyberspace Law Counsel

On September 30, the U.S. Supreme Court agreed to hear *Carr v. United States*, 08-1301 on the docket. The case raises two questions relating to the Sex Offender Registration and Notification Act (SORNA), 42 U.S.C. §16901 et seq., enacted on July 27, 2006, which created a comprehensive system of requirements for sex offender registration, as well as significantly increased the penalties for failure to register. The first question is whether SORNA applies to a person whose interstate travel occurred after his conviction for a covered sex offense, but before SORNA was enacted. If the answer is yes, the second question raised is whether it then violates the Ex Post Facto Clause.

Under SORNA, there are two types of registration requirements: (1) sex offenders must initially register following their conviction and (2) sex offenders who have already registered must keep their registration current by updating it within three business days of any change in their name, residence, employment or student status. A sex offender who “travels in interstate or foreign commerce” and fails to register may be imprisoned for up to 10 years under SORNA. Pursuant to SORNA, the U.S. Attorney General issued an interim rule, effective on February 28, 2007, which made SORNA applicable to persons who were convicted before the Act’s passage.

In 2004, Thomas Carr was convicted of first degree sexual abuse in Alabama. After his release from prison, he registered as a sex offender in Alabama. In 2004 or 2005, Carr moved to Indiana, but failed to register in the state as a sex offender. He was arrested for failure to register five months after the Attorney General’s interim rule and pleaded conditionally guilty in the U.S. District Court for the Northern District of Indiana. On appeal, Carr argued that SORNA was not applicable to him and, if so, would violate the Constitution’s Ex Post Facto Clause, but the Seventh Circuit Court of Appeals affirmed.

In his appellate brief, Carr argues that the Seventh Circuit misread the statute as to its applicability to a person who “travels in interstate or foreign commerce.” He maintains that Congress’ use of the present tense “travels,” and not “the past tense “traveled” shows its intent to include only present or future action. Carr also contends that applying SORNA to persons whose offense and interstate travel occurred before the Act became effective violates the Ex Post Facto Clause because the Act increases the penalty for failure to register from one year to 10 years for the first offense. Relying on the Court’s decision in *Collins v. Youngblood*, 497 U.S. 37 (1990), Carr contends that such use of the stat-

ute would contravene the principle that legislatures cannot increase the penalties for criminal acts retroactively.

The government’s brief makes short shrift of Carr’s misreading argument, contending that the present tense is commonly used to encompass all three tenses. It argues that the public interest involved is the same whether he moved from one state to another before or after the enactment of SORNA. As to Carr’s constitutional argument, the government contends it is not at issue because Carr failed to register after the statute applied to him. Thus, it argues that violation of the Ex Post Facto Clause is not a factor.

Note: The Court has also accepted another sex offender case, U.S. v. Comstock, which raises the question of the constitutionality of continued imprisonment of a sex offender who is considered to be dangerous after that individual has completed serving a prison sentence for the crimes.

ATTORNEYS GENERAL FIGHTING CYBERCRIME

DELAWARE

Attorney General Joseph Biden, III’s Office announced that Richard McCullough pled guilty to one count each of harassment and of non-compliance with a bond order. Attorney General Biden’s Office, with assistance from the University of Delaware, New Castle County and Wilmington Police Departments, arrested McCullough for using the Internet to stalk women, making contact with his victims using fictitious names. He then violated the no contact provisions of his bail release and was rearrested. McCullough was sentenced to 84 days in prison, followed by 18 months of probation and psychological treatment. He was also ordered to have no contact

with his victims.

FLORIDA

Attorney General Bill McCollum's CyberSafety Education Program was presented at its 1000th school in the state. The program combines real life stories and examples to help middle and high school students identify ways they could be victimized by online predators and encourages safe Internet use. The 50-minute interactive program has been presented to more than 482,000 students.

KENTUCKY

Attorney General Jack Conway joined the state Department of Education to announce that ConnectKentucky, a non-profit organization that implements strategies for technology deployment, use and literacy in the state, will become a member of their Internet safety partnership, CybersafeKY. The partnership hosted two free regional parent workshops to teach parents how to use technology and monitor activity on the Internet. ConnectKentucky provided 50 wireless printers donated by Lexmark as door prizes at the workshops. The partnership also developed a parent safety video that is available online. The video, about 10 minutes long, enables both parents and children to learn the basics of Internet safety.

MASSACHUSETTS

Attorney General Martha Coakley announced the opening of her Office's new, state-of-the-art Computer Forensics Lab, part of her Cybercrime Initiative which was designed to help the Commonwealth develop a statewide capacity to address cybercrime. The lab was designed to meet national standards of federal agencies, including the Department of Justice. The lab is also intended to be cost-effective, and includes such features as a climate-

controlled training room, capable of detecting the occupancy of the room and adjusting the temperature accordingly. Evidence stored in the lab will be protected by an enhanced security system as well as "grounded" floors to eliminate static electricity. The lab's space and technical capacity allow Attorney General Coakley's Office to handle more requests from police departments and state agencies.

MINNESOTA

Attorney General Lori Swanson filed a lawsuit against The Arthur Group, Inc. and its owner and chief executive, Barry Trimble, for luring unemployed Minnesotans looking for jobs into paying up to \$4,500 for job-finding assistance and then failing to keep their promises. The suit alleges that Trimble and the company obtained marketing leads (1) by placing ads for supposed executive-level jobs on Internet web sites such as CareerBuilder, and (2) from resumes posted by job seekers on Internet job boards. Among the failed promises made to job seekers were (1) failure to secure any job interviews; (2) misrepresentation of its success rate; (3) failure to provide resume-building and interview services; and (4) failure to reimburse fees as promised when a job was secured. The Arthur Group abruptly closed its web site and offices, leaving many job seekers who had paid thousands of dollars in the lurch. The lawsuit alleges violations of the state consumer fraud and deceptive trade practices laws and seeks restitution, injunctive relief and civil penalties.

MISSISSIPPI

Attorney General Jim Hood's Office received a federal grant to establish an Intellectual Property Theft Task Force. The grant will help fund "Operation Knock Out Knock-Offs," which will (1) provide statewide and regional training to increase the knowledge of local authorities on intellectual property (IP) enforcement, (2) assist local authorities in enforcement of IP laws through investigative and

prosecutorial assistance, and (3) educate merchants and the general public about the dangers of counterfeit goods. The task force will focus on counterfeit goods which raise safety concerns and include products sold both on and off the Internet.

NEVADA

Attorney General Catherine Cortez Masto's Office reached a settlement in a case filed with the Federal Trade Commission (FTC) against an international Internet payday lender operation. According to the complaint, defendants told consumers that the loans had to be repaid by their next payday with fees of up to \$80, or the loans would be extended automatically for extra fees to be debited from the consumers' bank accounts until repaid. Attorney General Masto's Office and the FTC also alleged that defendants threatened consumers with arrest or imprisonment, repeatedly called consumers at work using profane and abusive language and improperly disclosed the debts to third parties. The settlement order requires defendants to pay \$29,875 to the State and \$970,125 to the FTC and prohibits them from the practices described above. The order also contains recordkeeping and reporting provisions to allow the FTC to monitor compliance.

NEW JERSEY

Attorney General Anne Milgram announced that Stuart Patterson was indicted by a grand jury on charges of second-degree distribution of child pornography and fourth-degree possession of child pornography. Patterson was arrested after the State Police executed a search warrant that allegedly revealed multiple images of child pornography on his computer. The State Police Digital Technology Investigations Unit coordinated the investigation, and Deputy Attorney General Lee Schaer presented the case to the grand jury.

NEW MEXICO

Attorney General Gary King's Office reported that Jack Skinner (aka Jake Skinner) was sentenced to five years probation after pleading guilty to 11 counts of possession of child pornography. Attorney General King's Internet Crimes Against Children (ICAC) Unit began investigating Skinner based on a previous investigation, and a subsequent search warrant led to a grand jury indictment on 37 counts of possession of child pornography. Skinner's probation conditions require him to successfully complete a counseling/treatment program, participate in sex offender treatment for three years, register as a sex offender and be subject to the STEPS program of graduated sanctions. He also may not reside with or have unsupervised contact with children under the age of 18 years and cannot possess, own or view any pornographic or sexually explicit material.

NEW YORK

Attorney General Andrew Cuomo's Office sued to stop Mircea Veleanu's fraudulent artifact operation where Veleanu sold fake items for thousands of dollars over the Internet through such sites as eBay and GoAntiques.com. Veleanu claimed the artifacts contained high quality, expensive jade, but they were actually made of quartz or glass. He then refused to provide refunds or acknowledge that the pieces were fake. The lawsuit seeks to permanently bar Veleanu from advertising and selling jade artifacts unless they can be verified as authentic by the American Gemological Trade Association or a lab of equal reputation. It also seeks an accounting of all customers and full restitution for consumers he defrauded, including over \$13,000 to a single complainant. The lawsuit also seeks a civil penalty of \$5,000 for each deceptive act and costs. The case is being handled by Assistant Attorney General Nicholas Garin under the supervision of Vincent Bradley, Assistant Attorney General-in-charge of the Poughkeepsie Regional Office.

NORTH CAROLINA

Attorney General Roy Cooper's State Bureau of Investigation (SBI) announced that Gregory Brunner was sentenced to more than 12 years in federal prison after pleading guilty to one count each of the transportation and possession of child pornography. Brunner had been a long distance truck driver who had taken his laptop into a computer repair store during a trucking run. An SBI agent conducted a forensic examination of the laptop which contained a large volume of child pornography images. The Claremont Police Department participated in the investigation.

OHIO

Attorney General Richard Cordray filed a complaint against Decorate With Style, operating as USA Wallpaper, a home decorating company, for failure to deliver purchases made online. Consumers from Ohio and other states lost between \$18 to \$1,000 because the company failed to deliver merchandise or to refund the payments. Attorney General Cordray's Office received more than 240 complaints against the company, and the Better Business Bureau received more than 1,000 similar complaints over a three-year time period. The lawsuit seeks reimbursement for consumers as well as a \$25,000 penalty for each violation of the state Consumer Sales Practices Act.

OREGON

Attorney General John Kroger announced that fugitive John Hudson III was arrested by the U.S. Marshall's Fugitive Task Force and arraigned on child pornography charges. A grand jury had previously handed down a 40-count child pornography indictment against him, and a warrant was later issued for his arrest. Hudson's arrest follows an investigation conducted by Attorney General Kroger's

Internet Crimes Against Children (ICAC) Unit. Senior Assistant Attorney General Michael Slauson is prosecuting the case.

PENNSYLVANIA

Attorney General Tom Corbett's Child Predator Unit agents arrested Edward MacGregor, a retired construction worker, who is accused of using an Internet chat room to sexually proposition what he believed to be a 13-year-old girl, but was actually a Unit undercover agent. MacGregor is charged with two counts of unlawful contact with a minor (related to obscene or sexual materials), two counts of unlawful contact with a minor (related to child pornography) and one count of criminal use of a computer, all third-degree felonies which are each punishable by up to seven years in prison and \$15,000 fines. The State Police from the Blooming Grove barracks assisted in the arrest. MacGregor will be prosecuted by Deputy Attorney General Michael Spro of the Unit.

SOUTH CAROLINA

Attorney General Henry McMaster announced that Edward Slaton was arrested in an Internet predator sting conducted by the City of Mauldin Police Department, a member of Attorney General McMaster's Internet Crimes Against Children (ICAC) Task Force. Slaton was arrested on one count of Criminal Solicitation of a Minor, a felony offense punishable by up to 10 years imprisonment. The arrest warrant alleges that Slaton solicited sex on the Internet from an individual he believed to be a 13-year-old girl, but in reality was an undercover Police officer. A search warrant executed on Slaton's residence resulted in the seizure of three laptops and one desktop computer. The Newberry County Sheriff's Office assisted in the case, which will be prosecuted by Attorney General McMaster's Office.

TEXAS

Attorney General Greg Abbott announced that David Perez received a 30-year sentence after his conviction on child pornography charges. He was found guilty on nine counts of child pornography possession and received the maximum sentence on each third-degree felony charge. Perez also received an additional 30-year sentence on two counts of aggravated sexual assault after a child victim came forward and a 15-year sentence on two counts of indecency with a child after being reported by another child victim. The prison sentences will run concurrently and after release, Perez must register as a sex offender. Attorney General Abbott's Cyber Crimes Unit arrested Perez at his place of business after the U.S. House Committee on Energy and Commerce identified him as an individual who used credit cards to purchase access to child pornography web sites. Unit investigators conducted a forensic analysis of Perez's computer equipment and discovered more than 100 child pornography images and videos. Assistant Attorney General Heather Youree, together with the Crockett County District Attorney's Office, prosecuted the case.

UTAH

Attorney General Mark Shurtleff's Internet Crimes Against Children (ICAC) Task Force received a \$200,000 donation from Operation Kids to help fund undercover operations targeting online child abuse. The Task Force previously received \$50,000 from Operation Kids and used it to mount two month-long undercover operations.

WASHINGTON

Attorney General Rob McKenna's Office worked with the Australian Competition and Consumer Commission (ACCC) to shut down an Internet health scam that fleeced more than 60,000 consumers

worldwide. The Commission obtained an order against Leanne Vassallo and Aaron Smith, both of Sydney, concerning false, misleading and deceptive conduct. Attorney General McKenna's Office, which is separately pursuing civil charges against the defendants, brought the case to the ACCC's attention. Vassallo and Smith were alleged to have sold eBooks for a wide range of health conditions. Attorney General McKenna's Office is seeking injunctive relief, civil penalties and restitution.

WISCONSIN

Attorney General J.B. Van Hollen announced that the Endeavor Police Department joined the Internet Crimes Against Children Task Force. As part of this affiliation, the Department will receive reimbursement to fund ICAC-related expenses, priority for ICAC-related training, investigative assistance, access to the national ICAC e-mail group and recognition on Attorney General Van Hollen's web site.

IN THE COURTS

CHILD PORNOGRAPHY CONVICTION: CONDITIONS OF RELEASE

U.S. v. Thielemann, 2009 U.S. App. LEXIS 17080 (3rd Cir. August 3, 2009). The Third Circuit Court of Appeals upheld a convicted child pornographer's ban on Internet use as well as the possession and viewing of sexually explicit material. Paul Thielemann pled guilty to one count of receiving child pornography. The U.S. District Court for the District of Delaware sentenced him to the statutory maximum of 240 months in prison, in addition to two special conditions of supervised release: a ban on accessing the Internet for 10 years after his release and a ban on the possession and viewing of sexually explicit materials. Thielemann appealed his conviction.

tion, arguing that the district court considered non-charged relevant conduct – his admitted encouragement of the molestation of a minor victim – and applied a higher standard. The Third Circuit rejected this challenge, finding that the district court properly considered Thielemann’s involvement in the molestation of the victim and that his sentence was within the range suggested by the sentencing guidelines. Thielemann also challenged the two special conditions of release as violating his First Amendment rights. The appeals court disagreed, finding that the restriction as to sexually explicit material would protect children from Thielemann’s predatory conduct, thus outweighing any constitutional concerns. The court also found that the Internet restriction was not disproportionate when viewed in the context of Thielemann’s conduct in which he used the Internet to facilitate, entice and encourage the molestation of a child.

SEARCH AND SEIZURE: CONSENT OF LIVE-IN GIRLFRIEND

U.S. v. Nichols, 2009 U.S. App. LEXIS 16724 (8th Cir. July 29, 2009). The 8th Circuit Court of Appeals held that a live-in girlfriend with control over the premises could consent to a search. Andrew Nichols lived with his girlfriend and her seven-year-old daughter in a house that he owned. The girlfriend found an unlabeled computer disk in the house that contained several sexually explicit photographs of her daughter. She called the police, showed them the disk’s contents and gave them the disk. The police then obtained a search warrant for Nichols’ computer, and a subsequent search revealed computer files containing the same photographs as stored on the disk. Based on the evidence, a grand jury indicted Nichols for producing visual depictions of a minor engaged in sexually explicit conduct. Nichols filed a pretrial motion to suppress evidence found on the disk and computer. After an evidentiary hearing, a magistrate recom-

mended that Nichols’ motion be denied, which the U.S. District Court for the Western District of Arkansas adopted. Nichols then conditionally pleaded guilty and appealed the district court’s denial of his motion to suppress evidence, arguing that 1) the search was not authorized by a warrant, and 2) the girlfriend’s consent was invalid because she had no property interest in the house. The 8th Circuit rejected that argument, noting that the U.S. Supreme Court had rejected it also in *U.S. v. Matlock*, 415 U.S. 164 (1974). The court found that although the girlfriend had no property interest, she was a co-occupant of the residence and had unrestricted and joint access to the entire house, including complete access to the computer and the computer disk that officers searched. Nichols’ motion was denied, thus affirming the district court’s judgment.

SEARCH AND SEIZURE: SPECIFICITY OF SEARCH WARRANT

U.S. v. Payton, 2009 U.S. App. LEXIS 15969 (9th Cir. July 21, 2009). The 9th Circuit Court of Appeals decided that a warrant that authorizes a search for documents and other records, but does not specifically mention computers, will not support a computer search in the absence of special circumstances. Police had reason to believe that Michael Payton was selling drugs from his home, and they obtained a search warrant for drugs, sales ledgers about drugs and financial records. Only the affidavit of probable cause specifically mentioned computers, but it was not incorporated into the warrant. During the execution of the search, police found no evidence of drugs or drug sales. However, an officer found a computer in Payton’s bedroom with the screen saver up. He moved the mouse, which removed the screen saver, and clicked open a file, which appeared to be child pornography. Payton pled guilty to knowingly possessing images of child pornography in the U.S. District Court for the Eastern District of California, conditioned on his right to ap-

peal the district court's denial of his motion to suppress evidence of child pornography found on his computer during execution of the search warrant. The 9th Circuit found that the search of the computer exceeded the scope of the warrant and did not meet the Fourth Amendment standard of reasonableness because there was nothing that suggested evidence of drug sales would be found on the computer. The denial of Payton's motion was reversed, and the case was remanded with instructions to permit Payton to withdraw his conditional guilty plea.

CHILD PORNOGRAPHY CONVICTION: DOUBLE JEOPARDY

U.S. v. Bobb, 2009 U.S. App. LEXIS 17749 (11th Cir. August 6, 2009). The 11th Circuit Court of Appeals found that defendant was convicted for two distinct offenses, thus there was no Double Jeopardy Clause violation. Edward Bobb was convicted in the U.S. District Court for the Southern District of Florida of both "receiving" and "possessing" child pornography. He appealed, arguing that his convictions violated the Double Jeopardy Clause of the Fifth Amendment in that taking "receipt" of child pornography meant he necessarily must have "possessed" it. The 11th Circuit noted that Count I of the indictment charged Bobb with taking "receipt" of child pornography on November 12 by downloading seven zip files from a web site, while Count II charged him with having "possession" of more than 6,000 child pornography issues in August. Thus, the indictment charged him with two separate offenses. The convictions were affirmed.

ONLINE ENTICEMENT OF A MINOR: ENTRAPMENT

U.S. v. Myers, 2009 U.S. App. LEXIS 17722 (August 10, 2009). The 8th Circuit Court of Appeals found that defendant was not coerced into criminal activity, and therefore his entrapment claim failed.

Todd Myers engaged in a conversation in an online chat room with a policeman posing as a 14-year-old girl. Myers knew she was underage, but went ahead with plans to drop by "her" house for a sexual encounter. He also sent "her" a video of himself engaging in such conduct. Myers was arrested and later convicted in the U.S. District Court for the Eastern District of Arkansas of knowingly attempting to transfer obscene material to a person under the age of 16 years and of knowingly attempting to induce a child to engage in criminal sexual activities. He appealed, arguing that the policeman's role in the conversation amounted to entrapment. The court noted that as a defense, entrapment has two parts: 1) "government inducement of criminal conduct" and 2) "an absence of criminal predisposition on the part of the defendant." Here, the court found that the police did not coerce Myers, and the eagerness with which Myers responded to the criminal opportunity demonstrated his willingness to violate the law. Myers' conviction was affirmed.

4TH AND 14TH AMENDMENTS: BAN ON CELL PHONE USE WHILE DRIVING

Schor v. City of Chicago, 2009 U.S. App. LEXIS 17993 (7th Cir. August 13, 2009). The 7th Circuit Court of Appeals agreed with the lower court that there was no basis for a constitutional challenge to a local ordinance banning the use of cell phones while driving. Gayle Schor and two other drivers were ticketed for violating Illinois Municipal Code § 9-76-230 which banned using cell phones while driving. They filed an action claiming they were arrested in violation of the Fourth Amendment and state law. They also alleged that enforcement of the ordinance violated the Equal Protection Clause of the Fourteenth Amendment, and that the City of Chicago violated their constitutional rights. The U.S. District Court for the Northern District of Illinois dismissed the case for failure to state a claim upon which relief could be granted. The court also denied

the drivers' request for leave to amend their complaint on the basis that any amendment would be frivolous. On appeal, the 7th Circuit Court of Appeals agreed, finding "the case has no legs." The court found no Fourth Amendment issue since the police officers had found probable cause for the traffic stops. They also agreed with the district court that there was no basis for an amendment to add a vagueness challenge, stating that in today's world, it was impossible to take seriously the argument that the ordinance was so vague that no ordinary person could understand it. The lower court decision was affirmed.

FELONY INTIMIDATION: MYSPACE THREAT

Marshall v. State, 2009 WL 2243467 (Ind. App. July 28, 2009). The Indiana Court of Appeals reversed a conviction, holding that the state failed to prove its intimidation allegations because the message sent through MySpace was not sent to the account of the person being threatened. Dollie Marshall and Christopher Goodman traded cars, but the deal went sour. Marshall then got into an altercation with Goodman's mother, Jamie Lee, and was arrested. She was also ordered not to have contact with either Goodman or Lee, but a few days later, she sent a private message through MySpace to Goodman's account which threatened Lee. Based on the message, Marshall was convicted of felony intimidation against Lee after the prosecution argued that Marshall had communicated a threat to knowingly injure Lee with the intent that Lee be placed in fear of retaliation for calling the police. On appeal, the Indiana Court of Appeals reversed, holding that although an intimidating communication may be indirect, the state had to prove that Marshall must have known, or had reason to know, that her communication would reach Lee. In the instant case, there was no such proof that Marshall knew or had reason to know that Goodman would show the

message to his mother.

Ed Note: Monika Talbot, Deputy Attorney General for the Office of the Attorney General of Indiana, argued the case for the state.

ONLINE CHILD SOLICITATION: BRADY ARGUMENT

U.S. v. Daniel, 2009 U.S. App. LEXIS 17997 (7th Cir. August 13, 2009). The 7th Circuit Court of Appeals ruled that the government's failure to disclose the identity behind two screen names was not material in defendant's trial and his conviction was affirmed. James Daniel was caught during an online sting by police in Indiana designed to catch Internet predators when he struck up a chat with someone calling "herself" Amanda_13. Unknown to him, he was really communicating with a police officer posing as a 13-year-old girl. During Daniel's trial, the government introduced two chat sequences involving minor girls that were found on Daniel's computer. However, what the government failed to realize until sentencing was that one of the "girls," daisy13_indiana, was actually a police officer involved in the same sting operation. Additionally, the government was unaware until the court told it at oral argument that the other screen name, blonddt, was also an officer from the sting. Daniel was convicted and sentenced in the U.S. District Court for the Northern District of Indiana. On appeal, he argued for a new trial on the grounds that the government's failure to disclose the identity behind the two screen names of minor girls with whom he had chatted online violated *Brady v. Maryland*, 373 U.S. 83 (1963) under which the U.S. Supreme Court found that "...the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or punishment, irrespective of the good faith or bad faith of the prosecution." The appeals court rejected the Brady argument finding that the identities were not material to Daniel's trial. The

conviction and sentence were affirmed.

SEARCH WARRANTS: ELECTRONICALLY STORED INFORMATION

U.S. v. Comprehensive Drug Testing, Inc., 2009 WL 2605378 (9th Cir. August 31, 2009). An en banc decision by the 9th Circuit Court of Appeals reversed a decision by a three-judge panel of the same court and issued new guidelines for executing warrants for digital information. Comprehensive Drug Testing (“CDT”) was hired by Major League Baseball to test the urine of professional baseball players for drugs, and the players had agreed to take these tests with the assurance that the results would remain confidential. When the U.S. Attorney’s Office for the Northern District of California, which had begun an investigation into labs providing players with steroids, heard that ten players had tested positive for drugs, they obtained and served a grand jury subpoena for records of the suspected players. Although the warrant limited the search to ten players’ records, the government seized and reviewed computer records of hundreds of players, and used this information in support of further subpoenas. CDT and the players moved to quash the latest round of subpoenas, which the U.S. District Court for the Northern District of California granted. CDT also moved for return of records, which was granted by the U.S. District Court for the District of Nevada. The government appealed these decisions, and a divided three-judge panel of the 9th Circuit approved the search and subpoena and reversed. An en banc 9th Circuit disagreed, finding that “this was an obvious case of deliberate overreaching by the government in an effort to seize data as to which it lacked probable cause.” The court rejected the government’s plain view theory that allows agents to review computer files at will because the data is in “plain view,” warning that the government should “forswear reliance on the plain view doctrine.” The court added that “If law enforcement balks at such a

waiver, the warrant should require initial review by an independent third party under supervision of the court.” Next, the court said that the government should be honest, because a lack of candor about offers to retain the data until a motion to quash can be heard “shall bear heavily on the government.” Third, the court stated that the government must limit computer searches to data identified in the warrant. Finally, the court warned that the person segregating the seized data must be either a government “techie” who is not the investigating agent, and who promises not to divulge information about the non-responsive data, or an independent party. The orders of the two district courts were affirmed.

DATA BREACH: FAILURE TO IMPLEMENT ADEQUATE SAFEGUARDS

Shames-Yeakel v. Citizens Financial Bank, 2009 U.S. Dist. LEXIS 75093 (N.D. Ill. August 21, 2009). The U.S. District Court for the Northern District of Illinois ruled that a reasonable finder of fact could conclude that defendant bank breached its duty to protect its customer’s account against fraudulent access. Marsha and Michael Shames-Yeakel operated a home-based accounting business and maintained a business account at Citizens Financial Bank. An unknown person gained access to the account using their username and password and transferred \$26,500 to a bank in Austria, which refused to return the money. Citizens Bank notified the Shames-Yeakel’s it was holding them liable for the money, referring to a bank-customer agreement which stated that the bank had no liability for any unauthorized payment or transfer using the account holder’s password that occurs before the bank has been notified of a possible unauthorized use and has an opportunity to act. Citizens Bank billed them, and when they failed to pay, reported them as delinquent to national credit bureaus and threatened to foreclose on their home. The Shames-Yeakels sued the bank, including among other

claims one for negligence based on the theory that financial institutions have a common law duty to protect their customers' confidential information against identity theft. Citizens argued that they required all online banking customers to have usernames and passwords, but the Shames-Yeakels argued that these procedures were "single factor identification" and not state of the art. They argued that the bank should have used "multifactor identification," in which factors other than username and password are used to verify identity, and tokens, devices which are carried .by the user and generate ever-changing passwords. They referenced a 2005 document authored by the Federal Financial Examination Council which found that single-factor authentication was inadequate. The court agreed and allowed the suit to go forward.

And see...

DATA BREACH: POTENTIAL IDENTITY THEFT EXPOSURE

McLaughlin v. People's National Bank, Inc., 2009 WL 2843269 (D. Conn. August 31, 2009). The U.S. District Court for the District of Connecticut ruled that a claim for damages after a data breach may not be maintained based merely on a fear of future identity theft losses. People's National Bank had a contract with BNY Mellon to transport backup tapes of its customer information. On one of these transports, a box of tapes containing People's Bank customers' personal identifying information, went missing. Megan McLaughlin and other bank customers brought a class action against People's Bank and BNY Mellon, claiming that the loss of the tapes compromised their personal information and seeking damages for breach of fiduciary duty. The defendants moved to dismiss for lack of standing, arguing that the plaintiffs had pleaded no actual damages. The district court stated that in order to satisfy

standing requirements, a plaintiff had to show that it had suffered injury in fact that was concrete and particularized, as well as actual and not hypothetical. In the instant case, the plaintiffs' claim for damages were not based on direct losses, but solely on their fear of future losses, and thus was insufficient to satisfy the actual damages element.

LEGISLATIVE NEWS

Online Searches for Witnesses

CALIFORNIA. ENACTED. Governor Arnold Schwarzenegger signed SB 748 into law, a bill that would make it a misdemeanor to post information to the Internet that discloses the location of witnesses or their family members with the intent to injure them or incite violence, with a greater fine and prison time if bodily harm is suffered as a result. The bill also allows witnesses to submit opt-out forms to Internet search engine providers to keep their identifying information out of public databases. Businesses and agencies are required to remove identifying information about a witness within two days of receiving such opt-out form, or face a \$5,000 civil fine.

Internet Predators

NEW JERSEY. ENACTED. Governor Jon Corzine signed into law two bills, both proposed by Attorney General Anne Milgram, that are designed to strengthen law enforcement's ability to police the Internet for child predators. A-3761 allows law enforcement to intercept wire electronic communications of a suspected computer trespasser with the consent of the computer's owner or if law enforcement has probable cause to believe the information is related to an ongoing investigation. A-3763 creates the Computer Crimes Prevention Fund by imposing fines on those convicted of committing

crimes involving the Internet. The fines range from \$250 for disorderly persons offenses to \$2,000 for first-degree offenses.

Internet Safety

PASSED HOUSE SUBCOMMITTEE. On September 23, H.R. 3630, a bill which would provide grants for adolescent education on cybercrime awareness, was approved by the House Subcommittee on Crime, Terrorism and Homeland Security and forwarded to the full Judiciary Committee. The bill, sponsored by Representative Debbie Wasserman Schultz (D-FL), would authorize grantees to use funds for specific purposes, including developing and implementing cybercrime awareness programs, providing training to teachers and coordinating research to investigate online risks to children.

Illegal Cell Phone Use in Prisons

PASSED SENATE. On October 5, S. 251, a bill that would prevent prison inmates from using smuggled cell phones by allowing states to petition to operate wireless jamming devices in correctional facilities, passed the Senate. The bill, sponsored by Senator Kay Bailey Hutchison (R-TX) and co-sponsored by both Mississippi Senators, Thad Cochran (R-MS) and Roger Wicker (R-MS), would require the Federal Communications Commission to study and approve jamming devices for such use. The bill has the support of several national organizations, including the National Governors Association, the Fraternal Order of Police and the Council of State Governments.

Note: The Editor thanks Tom Clancy, Director of the National Center for Justice and the Rule of Law, for the above information.

NEWS YOU CAN USE

TEXTING WHILE DRIVING INCREASES COLLISION RISK 23X

Texting while driving increases the risk of a crash more than previously thought because motorists take their eyes off the road longer than they do when talking or listening on their cell phones, according to a study by the Virginia Tech Transportation Institute. The Institute used cameras to continuously observe light vehicle drivers and truckers for more than six million miles. It found that when drivers of heavy trucks texted, their collision risk was 23 times greater. Dialing a cell phone and using or reaching for an electronic device increased collision risk about six times in cars and trucks. The study found that right before a collision, drivers spent nearly five seconds looking at their devices, enough time to cover more than the length of a football field. The Institute recommended that texting should be banned for all drivers (currently banned in 14 states), and cell phone use should be prohibited for newly licensed teen drivers. The study also concluded that headset cell phone use is not substantially safer than hand-held because the primary risks with both are answering and dialing. Voice-activated systems are less risky if designed so that drivers do not have to take their eyes off the road. More information about the study can be found on the Institute's web site, <http://www.vtti.vt.edu>.

ICANN STUDY FINDS NO DOMAIN FRONT RUNNING

The Internet Corporation for Assigned Names and Numbers (ICANN) engaged Internet security guru Ben Edelman to conduct a study on the practice of domain front running, which occurs when "insider information" is gathered by a party from monitoring attempts by an Internet user to check

the availability of a domain name, and then that information is used by that party to register that domain name. Edelman conducted over 600 tests, broken into three rounds. He formed a list of sites to be tested based on top organic search results (using Google and Bing), for domain-related search terms, such as “register a domain,” “check whether a domain is available,” “domain availability” and “get a domain name.” He then checked whether each site provided a domain search function, discarding those that did not. Edelman’s tests found no evidence of domain front running. Edelman’s report can be accessed at <http://icann.org/compliance/edelman-frontrunner-study-16jun09-en.pdf>.

And more ICANN crackdown efforts...

“DOMAIN TASTING” DOWN SINCE PENALTIES ADDED

ICANN released a report indicating a 99.7 percent drop in “domain tasting” after new penalties were put into place. “Domain tasting” is the practice of registering a domain name and then returning it for a full refund during the first five days of registration. Nearly 17.7 domain names were “tasted” across all top-level domains (TLDs) in June 2008. Only 58,218 were deleted during the grace period in April 2009. The new rules allow a registrar to return up to 10 percent of their “net new registrations” each month, but returns above that amount are subject to both the registry fee of about \$7 and the \$18-20 ICANN fee. The report can be accessed at <http://icann.org/en/tlds/agp-status-report-12aug09-en.pdf>.

JUSTICE SERVED PICKS TOP 10 COURT WEB SITES

Justice Served, a consulting firm that provides services and training to courts in management and technology, released its 11th annual list of the 10 best court web sites in the world. Criteria included functionality, ease of use and appearance. Justice Served gives higher grades to sites that allow users to perform court business online, without having to appear in person, as well as sites that are geared to the public at large. This year’s best sites are:

Superior Court of California, Orange County – “terrific organization and navigation”

Colorado State Judicial Branch – “e-court functionality is front and center”

State Court of Chatham County, Georgia – “chock-full with e-dockets, e-tickets, e-fines and even e-probation”

Singapore Subordinate Courts – features include e-ADR

Superior Court of California, Santa Clara County – “particularly useful restraining and protective order content”

Courts Services of Ireland – not only provides court calendars online, but makes them readable on PDAs

Iowa Judicial Branch – “a full array of online services including dockets, payments and jury services”

Spokane County District Court – “truly the people’s court”

U.S. District Court, District of Maryland – “simple, straightforward organization”

Alabama’s Legal Information Network – “for lawyer and litigant alike”

The firm noted that when it began ranking court sites in 1999, it found 300 sites. By last year, the

number of court sites had grown to about 4,000, but in 2009, the number had significantly dropped to 3,000.

SURVEY: SECURITY NOT AN ISSUE FOR SMARTPHONE USERS

According to a survey conducted by Trend Micro, a security software firm, 44 percent of mobile phone owners said they believed surfing the Internet on a smartphone is as safe, if not safer, than doing so on a PC. The report, which was based on a poll of 1,000 smartphone owners 18 years of age or older, also found that smartphone users fear losing a phone or contact information more than viruses or phishing schemes. Only 23 percent of smartphone owners have security software installed, with one in five respondents saying that they don't think the software would be effective and that there is a limited risk. However, nearly one-half of respondents admitted they had received spam e-mails on their phones in the past three months, and 17 percent said the number of spam e-mails had increased. One-half of those surveyed have opened e-mail attachments on their smartphone during the last month, and nearly 40 percent have clicked on a URL link in an e-mail received on their phone. The full survey can be accessed at <http://trendmicro.mediaroom.com/index.php?s=23&item=503>.

REPORT: DON'T SHARE HOLIDAY PLANS WITH NETWORK "FRIENDS"

Nearly four in ten, or 38 percent, of people using social networking sites post details about holiday plans, and 33 percent post details of a weekend away, according to a survey by Legal & General, a British insurance company. In a report entitled "The Digital Criminal," the company found that people used social media sites to connect with people who were essentially strangers, presenting a serious risk

to the security of their homes. The survey, conducted by Opinion Matters, a European market researcher, involved sending out 100 "friend" or "follow" requests to strangers selected at random. Of those, 13 percent were accepted on Facebook and 92 percent on Twitter without any checks. The survey found that nearly two-thirds, or 64 percent, of 16-24 year-olds shared their holiday plans, with younger users the most likely to give away information. Men were found to be more relaxed about giving personal information online, with 13 percent including their mobile number on their profile, compared with seven percent of women. Nine percent of men also posted their address, compared with four percent of women. The report can be accessed at <http://www.legalandgeneralmediacentre.com/imagelibrary/detail.asp?MediaDetailsID=366>.

ALL TIME HIGHS FOR SPAM, MALWARE

Spam still accounts for 92 percent of all e-mail, according to the latest quarterly threat report by security software firm McAfee. The largest source of spam production is still the United States, although its spam production has dropped steadily over the last three quarters. Other major producers are Brazil, Turkey, India and Poland, all of which have experienced sharp spam production. McAfee also reports that there were almost 14 million new zombies in action in the quarter, a rise of more than 150,000 new threats each day. Another threat on the rise is AutoRun malware, which is triggered automatically when a person plugs in a USB stick, memory card or other external device. McAfee reported that in one 30-day period, it uncovered AutoRun malware in more than 27 million infected files. McAfee's report can be accessed at

http://www.mcafee.com/us/local_content/reports/6623rpt_avert_threat_0709.pdf.

REPORT: IT FOLLOWING WRONG THREATS

Corporate information technology departments are prioritizing the wrong threats to their computer systems, focusing on old problems and not on new cyberattacks, according to the latest biannual report from the SANS Institute, which provides training for computer security professionals. SANS staff weighed data on the most common attacks on corporate networks and data on which vulnerabilities are most prevalent on company networks. Tipping-Point, an intrusion-prevention technology company, provided the attack data, which was collected during its defense of 6,000 organizations this year, and Qualys, a vulnerability-management company, provided data on the most common security holes based on its analysis of nine million customer computers. The report notes that attacks on desktop programs, such as Microsoft Office, Adobe Flash Player, and Apple QuickTime, currently account for 10 percent of attack volume, up from zero three years ago. The report also noted that 60 percent of attack activity is now directed at hacking web sites, often by targeting SQL injection and cross-site scripting flaws in open source and custom-built web applications. The report can be accessed at <http://www.sans.org/top-cyber-security-risks/>

AMERICANS OBJECT TO ONLINE TRACKING

About two-thirds of Americans object to online tracking by advertisers, and that number increases by seven percent when people learn about advertisers' methods, according to a survey by researchers at the University of Pennsylvania and the University of California, Berkeley. The lead author of the study is Joseph Turow, professor of communication at the Annenberg School for Communication at the University of Pennsylvania. The authors hired a survey company to conduct 20 minute interviews with

1,000 adult Internet users. The results were then adjusted to reflect Census Bureau patterns in categories such as sex, age, population density and telephone usage. The survey company also asked about customized discounts and news, finding that 51 percent approved of such discounts and 58 percent were fine with such news. On the advertising question, there was little variance among age groups, with 55 percent of respondents aged 18 to 24 years objecting to tailored advertising. Additionally, 69 percent of respondents said "yes" when asked if there should be a law that gave people the right to know all the information web sites had about them. The study can be accessed at <http://graphic8.nytimes.com/backpages/pdf/business/20090929-Tailored-Advertising.pdf>.

FREE ONLINE SAFETY RESOURCE FOR YOUR USE

The Federal Trade Commission (FTC) recently released *Net Cetera: Chatting with Kids About Being Online*, a guide for parents with practical tips to help kids navigate the online world. The guide is designed to be a comprehensive vehicle to help parents in your state raise these important issues with their kids – and it's available to you **in bulk – and for free.**

Net Cetera focuses on helping parents talk with their kids: encouraging parents to reduce online risks by talking to kids about how they communicate – online and off – and helping kids engage in conduct they can be proud of. *Net Cetera* covers what parents need to know, where to go for more information, and issues to raise with kids about living their lives online.

The guide addresses a variety of topics, such as:

- **Social networking.** Socializing online can help kids connect with friends, and even their family members, but it's important for children to learn how to navigate these spaces safely. Net Cetera offers tips to help parents talk to their children about applying real-world judgment and sense when socializing online, which can help minimize these downsides.
 - **Sexting.** Net Cetera suggests that parents talk to their kids about not doing it – emphasizing the risk to their reputation and their friendships. It also discusses how kids could be breaking the law if they create, forward, or even save this kind of message.
 - **Cyberbullying.** It can happen in an email, a text message, an online game or comments on a social networking site. It might involve rumors or images posted on someone's profile or passed around for others to see, or creating a group or page to make a person feel left out. Net Cetera gives parents practical suggestions for spotting and stopping this kind of harassment.
- **Mobile Phones.** Many kids these days have powerful computers...in their pockets. The rise of smart phones means that parents and kids need to understand how they can stay safe in a mobile environment.
- **Protecting your family's computer.** Net Cetera offers tips for recognizing and protecting computers from malware, software that monitors or controls computer use, or can install viruses, be used to send unwanted pop-up ads, or record keystrokes. Net Cetera also highlights the importance of keeping security software, operating systems, and web browsers all up-to-date.

You can review the full publication at OnGuardOnline.gov, the FTC's online safety website. Like all the FTC's consumer education resources, *Net Cetera* is in the public domain and is available for free. You can order free copies to distribute at conferences, in schools or at a PTA meeting – anywhere parents or educators might gather. There's even room for a sticker on the back to let people know it came from your office. You can put a Net Cetera button on your website, include sections in a newsletter or on your website, link to it, or even reprint it with your own seal.

To order free copies of *Net Cetera*, visit bulkorder.ftc.gov (please allow 2-4 weeks for delivery). To find out more about reprinting the guide or working with the FTC to spread the word, contact Jennifer Leach: jleach@ftc.gov.

JOB OPENING: SENIOR COUNSEL / VISITING PROFESSOR

The National Center for Justice and the Rule of Law, a program at the University of Mississippi School of Law, has an opening for the position of Senior Counsel / Visiting Professor. The Center may fill that opening on either a temporary basis, as a one or two year visitor, or as a permanent position. The position is non-tenure track and is dependent on the Center's ability to obtain continued funding.

The successful candidate will have visiting faculty status at the law school and will teach advanced criminal law and procedure classes. A second focus of the position is to help develop national conferences and to lecture at those conferences. The Center has two initiatives that produce approximately 12 conferences each year.

The Center's *Cyber Crime Initiative* develops educational programs targeting computer-related crime. To implement this initiative, the Center allies with other national organizations. In partnership with the National Association of Attorneys General (NAAG), the Center has a cyber-crime training program for Attorney General offices from all 50 States. The Center also develops unique and nationally important projects to further the goals of this initiative.

The Center's *Fourth Amendment Initiative* promotes awareness of search and seizure principles through conferences, judicial and prosecution training, and support for selected publications. The Center has an annual symposium focused on the Fourth Amendment and sponsors the James Otis Lectures, both of which attract noted scholars. The Center associates with the National Judicial College, located in Reno, NV, to provide educational programs for state trial and appellate judges regarding search and seizure principles. Through its partnership with NAAG, the Center offers training about the search and seizure of computers to state Attorney General offices. The Center also has computer search and seizure conferences for trial and appellate judges.

Applicants must have a J.D. degree from an ABA-accredited school and be admitted to the bar. Preferred accomplishments include substantial knowledge of either cyber crime or search and seizure principles, strong interpersonal skills, a record of academic achievement, and advanced writing, oral, and editing skills..

Informal inquiries may contact Professor Thomas K. Clancy, Director, National Center for Justice and the Rule of Law, University of Mississippi, School of Law, P.O. Box 1848, University, MS 38677-1848, tclancy@olemiss.edu. For more information about the Center, please visit our website at www.NCJRL.org. The University of Mississippi is an EEO/AA/Title VI/Title IX/Section 504/ADA/ADEA employer. All applicants must formally apply on line at <https://jobs.olemiss.edu/>. Applicant must submit a cover letter, resume, and writing sample. The position will remain open until filled.