

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 2010

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 |
| IN THE COURTS..... | 7 |
| NEWS YOU CAN USE..... | 11 |
| OTHER S.CT ACTION..... | 15 |
| LEGISLATIVE NEWS..... | 18 |
| ACTION ITEMS..... | 20 |
| SAVE-THE-DATE..... | 21 |

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

SUPREME COURT FINDS SEARCH OF OFFICER'S TEXT MESSAGES REASONABLE

By Marielle Dirks¹

In *City of Ontario v. Quon*, No. 08-1332, the U.S. Supreme Court found that a police department's audit of text messages sent and received by a police officer on a pager issued by the department for work-related purposes was reasonable under the circumstances because it was not excessive in scope.

Jeff Quon was employed as a SWAT team member for the City of Ontario Police Department. When Quon was hired, he agreed to the city's "Computer Usage, Internet, and E-Mail Policy," which specified that employees should have no expectation of privacy when using city-owned electronic devices. In October 2001, the police department purchased pagers that could send and receive text messages and distributed them to SWAT team members to help them mobilize and respond to emergencies. The wireless contract for the pagers provided a specific number of characters to be sent and received by the pagers for a flat rate, and any characters over that amount resulted in additional fees.

On the second billing cycle, Quon exceeded his allotted character limit. Steven Duke, the officer responsible for overseeing the pager contract, reminded Quon that the department's privacy policy for e-mail messages also applied to pager messages, and suggested that Quon could reimburse the city for the overage fee in place of Duke's auditing the messages to make sure that they were all government-related, which Quon did. Officer Duke offered the same arrangement to other SWAT team officers who incurred overages. Quon exceeded his character limit several times and reimbursed the city, but after several months, Duke decided that he was tired of "being a bill collector." The police chief decided to evaluate the pager usage of employees who were incurring overages to determine whether the character limit under the contract was too low. The department obtained transcripts of the text messages sent by Quon and another officer who consistently incurred overages, and determined that many of the messages sent while Quon was on duty were personal and sexually explicit. Based on this audit, the department determined the Quon had violated their rules and punished him.

In response, Quon, his wife and his mistress filed suit in the U. S. District Court for the Central District of California, claiming that his Fourth Amendment rights had been violated and the Ontario Police Department had breached both federal and state communications laws. The district court dismissed the claims under federal communications law but heard arguments on the Fourth Amendment claims. The court determined that Quon had a reasonable expectation of privacy in his messages. However, it held that since the purpose of the warrantless search was to determine the sufficiency of the department's pager character limits, there was no Constitutional violation. The Court of Appeals for the Ninth Circuit reversed the district court's decision in part. While the court agreed that there was a legitimate expectation of privacy in the text messages, it found that the search was not reasonable in its scope because the department did not use the least intrusive means possible.

The Supreme Court granted certiorari to the Ontario Police Department on Quon's Fourth Amendment claims. The Court utilized the test for assessing Fourth Amendment claims against government employers established in the *O'Connor v. Ortega*, 480 U. S. 709 plurality opinion. The test has two parts: the first inquires whether or not the realities of the employee's workplace create a reasonable expectation of privacy and, if so, then inquires whether, under the totality of the circumstances, the employer intruded upon that privacy for "noninvestigatory, work-related purposes" or for "investigations of work-related misconduct." The Court declined to make a final decision on the privacy expectation of employer-provided communications devices, reasoning that they are not prepared to elaborate fully on the Fourth Amendment implications on emerging technology until its role in society becomes clearer.

ATTORNEYS GENERAL FIGHTING CYBERCRIME

MULTI-STATE

Twenty-three Attorneys General sent a letter to Internet message board host Topix.com, urging the company to improve consumer protections and eliminate its \$19.99 fee for “priority review” of abusive or inappropriate posts. An initial investigation by the Attorneys General of Connecticut and Kentucky found that the “Forums and Polls” section of Topix is routinely used to post abusive, vulgar and obscene information in violation of Topix’s terms of service. The letter asks Topix to 1) eliminate the \$19.99 fee for “expedited review” of abusive posts; 2) clarify the “feedback” and “flagging” options so consumers understand the process for reviewing flagged and reported posts; 3) reduce the current 7-14 day turnaround time for reviewing abuse reports; and 4) enhance screening technology to block abusive posts. Attorneys General from the following jurisdictions signed the letter: **Arizona, Arkansas, Connecticut, Guam, Illinois, Iowa, Kansas, Kentucky, Maine, Maryland, Mississippi, Montana, Nebraska, New Hampshire, New Mexico, North Dakota, Northern Mariana Islands, Ohio, Rhode Island, South Dakota, Tennessee, Virginia and Washington.**

CONNECTICUT

Attorney General Richard Blumenthal confirmed that Google has used its “Street View” cars to collect data in Connecticut. After Attorney General Blumenthal’s letter of inquiry to Google, the company acknowledged that it had collected data broadcast over unsecured home and business wireless Internet connections such as emails and passwords. Based on the primary response from Google, Attorney General Blumenthal is seeking more answers from the company such as how, when, where, and

The Court found, regardless of the privacy expectation in Quon’s text messages, that the police department’s search was reasonable. At the outset, the search was justified in its inception because it was related to a legitimate work-related purpose. Further, the Court held the scope of the search was reasonable because it was the most efficient, expedited way to determine whether or not the police department needed to invest more money into the pager program. Further, because the police department redacted the text messages sent while Quon was not working and limited their audit to two months, the search was not excessively intrusive. Because the claims by Quon’s wife and mistress suggested that because the search was unreasonable to Quon it was reasonable to them as well, they lost standing once the search was ruled unreasonable to Quon.

Justice Scalia, concurring in the judgment, outlined a different test than the O’Connor test used in the majority’s opinion. He concluded “that the offices of government employees . . . are covered by Fourth Amendment protections as a general matter.” However, he would also have held that searches regarded as reasonable and normal in the private employer context, like those investigating violation of a workplace rule or to retrieve work-related items, do not violate the Fourth Amendment. Under the application of either test, the City of Ontario’s search of Quon’s text messages was reasonable under the circumstances.

¹Marielle Dirx is a summer intern at the National Association of Attorneys General’s (NAAG’s) Cybercrime Project under its contract with the National Center for Justice and the Rule of Law. Marielle will be entering her third year as a law student at the University of Mississippi School of Law this fall.

why the practice of using the Street View cars to collect data happened. Attorney General Blumenthal is also considering the legality of Google's collection practices and is encouraging the state legislature to determine whether state privacy laws need to be clarified or changed.

FLORIDA

Attorney General Bill McCollum announced that Randall Wilson was charged with 10 counts of possession, and one count of promotion, of child pornography. Wilson was arrested after Attorney General McCollum's CyberCrime Unit discovered multiple images of child pornography on his personal computer during a routine investigation. An initial review of Wilson's computer hard drives revealed many pornographic images, some depicting children as young as 10 years old.

ILLINOIS

Attorney General Lisa Madigan cosponsored a statewide Internet safety contest, aimed at raising awareness about potential dangers associated with the Internet. Attorney General Madigan's office encouraged students from first to twelfth grade to submit a poster or electronic project addressing cyberbullying and Internet safety. The seven students who won first place were recognized during a ceremony at the Illinois Governor's Mansion. Illinois law dictates that Internet safety must be taught to students once a year starting in third grade.

IOWA

Attorney General Tom Miller accepted the 2010 Outstanding Service Award from Iowa's Internet Crimes Against Children (ICAC) Task Force. The award recognized the Attorney General's Office's work to amend the Iowa "enticement" statute to make it a felony to entice a person the perpetrator

reasonably believes is a child, even if the person is actually an undercover law enforcement officer. Attorney General Miller's office formulated the amendment to better support undercover investigation of child predators. While accepting the award, Attorney General Miller announced a new website being launched by the Task Force, aimed at helping parents keep their children safe on the Internet.

KENTUCKY

Attorney General Jack Conway announced that a grand jury indicted Terry Henderson on 32 counts of possession, and three counts of distribution, of child pornography. Attorney General Conway's Cybercrimes Unit began their investigation of Henderson after they identified an Internet address suspected of distributing child pornography.

LOUISIANA

Attorney General Buddy Caldwell's High Tech Crime Unit (HTCU) continued their proactive Internet safety education efforts with a presentation for students at West Feliciana Middle School in St. Francisville. The middle school students learned about social networking sites, cyberbullying, and online chat rooms. The HTCU also did a presentation for parents to teach them about what they can do to keep their children safe online afterward. The parents' presentation focused on how predators use the Internet to prey on children, cyberbullying, Internet scams, and the mechanics of social networking sites.

MASSACHUSETTS

Attorney General Martha Coakley announced that a grand jury indicted Raphael Chiu for possessing and distributing child pornography on his computer. Chiu was charged with dissemination or possession of obscene matter, dissemination of child

pornography, and four counts of possession of child pornography. State Police investigators assigned to Attorney General Coakley's office conducted an online investigation of computer systems offering known child pornography images over file sharing networks. The officers noticed a computer distributing child pornography and traced the computer to Chiu. After obtaining a search warrant, investigators determined that Chiu both possessed the pornographic images and distributed them over file sharing networks.

MICHIGAN

Attorney General Mike Cox announced that an undercover Internet child predator sting led to the arrest of Phillip Knowlan, a long haul truck driver, for using the Internet to commit child sexual abusive activity. Knowlan told the undercover investigator he was chatting at home and "from the road." Allegedly, Knowlan engaged in graphic sexual conversation with an undercover persona from Perverted Justice who he thought was a 14-year-old girl. He also, reportedly, solicited the persona to engage in sexual activity. Knowlan was charged with one count of accosting, enticing, or soliciting a child for immoral purposes, four counts of using the Internet to accost a child for immoral purposes, and two counts of using the Internet to disseminate sexually explicit matter to a minor.

MISSISSIPPI

Attorney General Jim Hood announced that Brian Leavitt, an investigator with Attorney General Hood's Cyber Crime Unit, was honored with the "Top Cop" Award for his work with computer forensics and child exploitation cases. Leavitt has been with Attorney General Hood's office for 10 years and in law enforcement for 17 years.

MISSOURI

Attorney General Chris Koster sent a letter to Google asking the company to provide details about the personal information it may have collected from Missourians through its "Street View" program. The letter asked Google to explain to Attorney General Koster's office the nature of the data collected in Missouri, how that data has been used, to whom it has been disclosed, and what protections Google has in place to ensure the data is not put to improper use. The letter also asks Google to preserve the data it collected from Missouri residents until all of the State's questions have been adequately answered and the proper regulatory and investigative agencies have had the opportunity to evaluate the situation.

NEW JERSEY

Attorney General Paula Dow announced that James Haspel, a police officer, was arrested for allegedly exposing himself on a webcam to an undercover officer he believed was a 13-year-old girl. He is also charged with official misconduct because he sent videos of himself from a hotel where he was attending a police training conference and communicated with the "girl" while he was on duty at police headquarters while using a government-supplied computer. Haspel has been a police detective for the past 25 years. The charges against Haspel are official misconduct, attempting to endanger the welfare of a child, and attempting to transmit obscene materials to a person under 16-years-old.

NEW MEXICO

Attorney General Gary King's Internet Crimes Against Children (ICAC) Unit began distributing small, teen-oriented products to all of its affiliates for the purpose of giving them away to teens who participate in Internet safety programs across the

state. The products, which include squeeze stress balls, water bottles, pens and screen cleaners, all display reminders, such as how to report a cyber predator and the Cyber Tipline phone number and web address. Artwork for the items was created in-house by members of Attorney General King's Office.

NEW YORK

Attorney General Andrew Cuomo announced that Friendster, hi5, and isoHunt (a peer-to-peer site) have joined Facebook and MySpace in utilizing Attorney General Cuomo's hash value database, which gives social networking sites the tools to block attempts to share images of children being sexually abused. Attorney General Cuomo's office has compiled 8,000 hash values that are associated with child pornography, and that database can be used to identify images as child pornography before they are posted on the site. The hash values are also used by New York law enforcement agencies to help in investigations of crimes against children.

PENNSYLVANIA

Attorney General Tom Corbett's Child Predator Unit arrested Norman Hutchko in an Internet sex sting. Hutchko allegedly contacted a 15-year-old girl on MySpace, and the girl's mother contacted police with the allegation that a much older man had made inappropriate comments to her teenaged daughter. Attorney General Corbett's Unit began undercover instant message conversations with Hutchko, which quickly became sexually graphic and with Hutchko repeatedly asking the undercover officers to meet for the purpose of having sex. Hutchko was arrested after he arrived at a pre-determined location. Hutchko is being charged with two counts of unlawful contact with a minor and one count of criminal use of a communication facility.

SOUTH CAROLINA

Attorney General Henry McMaster announced that James Vereen was arrested in an undercover Internet sting by the Richland County Sheriff's Office, a member of Attorney General McMaster's Internet Crimes Against Children (ICAC) Task Force. Vereen solicited sex from someone he thought was a minor during online chats. In reality, Vereen was communicating with an undercover sheriff's agent. During the arrest, Vereen's roommate consented to a search of the home which resulted in the seizure of a laptop. Vereen is charged with two counts of criminal solicitation of a minor.

VIRGINIA

Attorney General Ken Cuccinelli joined Neil McBride, U.S. Attorney for the Eastern District of Virginia, to announce that Paul Marlowe was sentenced to 210 months in prison for transporting child pornography, a sentence that was enhanced because of Marlowe's history of sexually abusing children and minors. Marlowe was identified by law enforcement officers during an undercover investigation of individuals trading images of child sexual abuse over the Internet. Agents executed a search warrant at Marlowe's home and seized a computer. A subsequent forensic examination revealed emails from Marlowe with attached child pornography images. Special Assistant U.S. Attorneys Gene Fishel and Tommy Johnstone of Attorney General Cuccinelli's Office prosecuted the case on behalf of the U.S. as part of Project Safe Childhood.

WISCONSIN

Attorney General J.B. Van Hollen announced that the Wisconsin Internet Crimes Against Children (ICAC) Task Force surpassed 150 affiliates by adding the Jefferson County Sheriff's Office and the Lomira Police Department.

IN THE COURTS

COMPUTER FRAUD AND ABUSE ACT: VAGUENESS CHALLENGE

U.S. v. Powers, 2010 WL 1418172 (D. Neb. March 4, 2010). The U.S. District Court for the District of Nebraska found that the Computer Fraud and Abuse Act (CFAA) provides adequate notice of prohibited conduct and does not foster arbitrary enforcement. Chad Powers was charged with intentionally exceeding authorized access to a computer and obtaining information from that computer to further tortious acts of invasion of privacy and intentional infliction of emotional distress. The indictment accuses Powers of violating the CFAA by entering Shaunna Briles' computer and sending partially nude or provocatively posed images of her via email to individuals in her address book. Although Briles had given Powers her email password, the indictment charged Powers with exceeding the purpose for which the password was given. Powers moved to dismiss the indictment on the ground that the CFAA was void for vagueness because it does not provide sufficient warning of what conduct was prohibited, and therefore he was denied due process of law as guaranteed by the Fifth Amendment. The district court found otherwise, noting that the CFAA covers computers used in or affecting interstate communication. The servers that hosted Briles' email account were "protected computers" because they could be used in interstate communication and therefore the statute provided such notice. The motion was denied.

KNOWING POSSESSION OF CHILD PORNOGRAPHY: VIEWING

State of Wisconsin v. Mercer, 2010 WL 1222788 (Wis. Ct. App. April 5, 2010). The Wisconsin Court of Appeals ruled that a person who purposely views digital images of child pornography on the Internet "knowingly possesses" child pornography in violation of state law, even though the images were not found on his computer. Benjamin Mercer, a city human resources director, was charged with deliberately accessing and viewing child pornography online using his city-provided computer. Mercer had deleted the images on his hard drive in a way that made them unrecoverable by forensic analysts. However, monitoring software installed by the city on employees' work computers automatically captured data about the computer's use and created a data log showing every mouse click, keystroke, the words in the browser title bar at the time of the click or keystroke and the time of those actions. Mercer's computer logs showed that he had searched for words that were likely to produce child pornography. Relying on testimony from the software engineer who created the monitoring software and explained its operation, as well as a live demonstration of the software, a jury found Mercer guilty of 14 counts of possessing child pornography. On appeal, the appeals court affirmed the conviction. The court clarified the meaning of possession for purposes of the state statute and established that the State could rely on evidence from monitoring software to convict a person of child pornography possession even when that person successfully deletes the images.

Ed. Note: The trial court case was prosecuted by Assistant Attorney General Michael Schaefer and the appeals court case was argued by Assistant Attorney General Christopher Wren, both with the Wisconsin Department of Justice.

SEARCH WARRANT EXECUTION: STALENESS

U.S. v. Burkhart, 2010 WL 16340151 (10th Cir. April 23, 2010). The 10th Circuit Court of Appeals ruled that the information received from Europol that defendant had received child pornography was not stale, even though two years had elapsed, because possessors of child pornography tend to hoard material. Europol sent the FBI about 10,000 emails between an Italian running a child pornography web site and his U.S. customers. One of the email addresses belonged to William Burkhart, and his emails verified the purchase of child pornography in 2005. The FBI executed a search warrant in May 2008 on Burkhart's home and found more than 400 DVDs with images of child pornography. Burkhart moved to suppress, which the district court denied, and he then pled guilty, reserving the right to appeal the denial of his suppression motion. On appeal, Burkhart argued that over two years had passed since the email from Europol, so the FBI's affidavit contained information "so old as to be stale." The 10th Circuit rejected this argument, pointing out that the offense of possession does not end as long as he has the material. Also, the court noted that the two-year-old email was still within the five-year statute of limitations. According to the court, these facts, coupled with the FBI's testimony regarding the tendency of child pornography collectors to "retain materials for some years," formed a substantial basis for the warrant.

SEARCH WARRANT: PROBABLE CAUSE

U.S. v. Vosburgh, 2010 WL 1542340 (3rd Cir. April 20, 2010). The 3rd Circuit Court of Appeals ruled evidence that the user of a computer with a particular IP address possessed or transmitted child pornography could support a search warrant for the physical premises linked to that IP address. A federal agent obtained an IP address during an operation targeting those accessing child pornography.

He got the physical address of the subscriber connected to the IP address from the Internet service provider, and a local agent received a warrant to search Roderick Vosburgh's apartment. The search uncovered child erotica and pornography. Vosburgh was eventually convicted by a jury of possession of child pornography. On appeal, he argued that the warrant was not supported by probable cause because the basis was only an IP address of a computer that was trying to download a video purporting to be child pornography. The 3rd Circuit disagreed, finding that IP addresses were unique identifiers and, in the instant case, was traceable to Vosburgh's account and physical address. Therefore, the attempts to access the video were criminal activity.

EXPECTATION OF PRIVACY: HARD DRIVE IN SHARED COMPUTER

U.S. v. King, 2010 US App LEXIS 8970 (3rd Cir. April 30, 2010). The 3rd Circuit Court of Appeals found that the owner of a hard drive did not have a reasonable expectation of privacy in its contents after he installed it in a computer shared with another person. Richard King moved in with Angela Larkin, and they both began distributing pornographic pictures of Larkin's two-year-old daughter. A law enforcement investigation led to a search of the residence and Larkin's arrest. Larkin agreed to let police seize her computer, but King objected that he owned and had installed the hard drive. The officers still took the computer, which was found to contain emails and chats between Larkin and King describing sexual acts with the daughter. King later pled guilty to traveling interstate to have sex with a minor, but he argued that the police had violated his Fourth Amendment rights by seizing his hard drive. The U.S. District Court for the Middle District of Pennsylvania rejected this argument, and King appealed. The 3rd Circuit affirmed, holding that the seizure was constitutionally valid because Larkin

had consented. The court explained that King placed his hard drive inside the computer he shared without password protection with Larkin, and he therefore assumed the risk that Larkin would consent to the seizure.

CHILD PORNOGRAPHY CONVICTION: SENTENCING ENHANCEMENTS

U.S. v. Dorvee, 2010 U.S. App. LEXIS 9574 (2nd Cir. May 11, 2010). The Second Circuit Court of Appeals found that the sentence of a defendant convicted of distribution of child pornography was both procedurally and substantively unreasonable and that the defendant would have received a lighter sentence if he had sexually assaulted a child. Justin Dorvee established an online relationship with an undercover officer posing as a 14-year-old boy and sent the “boy” videos of child pornography. He was arrested when he arranged to meet the “boy” for sex. A search of his home and computer uncovered thousands of images of minors engaged in sexually explicit conduct. Dorvee pleaded guilty to distribution of child pornography under 18 U.S.C. §2252A (a)(2)(A), and the Probation Department advised that sentence enhancements applied, including those for distributing material involving prepubescent minors, material intended to get a minor to engage in sexual conduct and material portraying sadistic or masochistic conduct. According to the guidelines, Dorvee’s offense level calculated at 262 to 327 months in prison, but the statutory maximum for his offense was 20 years, or 240 months. Dorvee received the maximum sentence, minus time served on related convictions, for a total of 19 years, five months and 16 days. On appeal, the 2nd Circuit found that the lower court made a procedural error in treating the guideline level range “as though it were a benchmark for any variance,” finding the sentence “substantively unreasonable.”

FREEDOM OF SPEECH: LIBRARY INTERNET FILTERS

Bradburn v North Central Library District, 2010 Wash. LEXIS 434 (May 6, 2010). The Washington Supreme Court ruled that a library’s Internet filter policy does not violate the free speech protections in the State Constitution. The North Central Regional Library District has Internet filters on its computers to block websites and images considered harmful to children. Susan Bradburn and other library patrons as well as the Second Amendment Foundation sued the library for violating federal and state free speech protections. They claimed the library’s filtering policy was overbroad and an impermissible content-based restraint of speech. The U.S. District Court for the Eastern District of Washington certified the question of whether the library’s filtering policy violated the free speech protections in Article 1, Section 5 of the State Constitution to the State Supreme Court. That court concluded that a library has no obligation to provide universal coverage of all constitutionally protected speech, whether it be provided via the printed word or the Internet. Just as a library may exercise discretion in its literary acquisitions, it can also decide what Internet content to provide.

FOURTH AMENDMENT: ADMINISTRATIVE SUBPOENAS

U.S. v. Bynum, 2010 WL 1817763 (4th Cir. May 5, 2010). The Fourth Circuit Court of Appeals held that a Yahoo! subscriber had no reasonable expectation of privacy in his account information, including his IP address, that he provided to Yahoo! in order to access chat boards. Following the investigation of a Yahoo! group to which Marques Bynum had uploaded child pornography, officers searched Bynum’s home and laptop. They uncovered numerous images of child pornography, including those uploaded to the Yahoo! group. Bynum was charged

and convicted of three counts of transporting and one count of possession of child pornography. On appeal, Bynum argued that the government's use of administrative subpoenas to identify him from his Yahoo! group postings, about which he had no knowledge, violated the Fourth Amendment. The court disagreed and affirmed, holding that Bynum had no expectation of privacy in information that he had conveyed and was stored by third parties.

AUTHENTICATION: MYSPACE EVIDENCE

Griffin v State of Maryland, 2010 Md, App. LEXIS 87 (May 27, 2010). In affirming a lower court ruling, the Maryland Court of Special Appeals established the level of authentication necessary to admit print-outs of a social networking profile page. The case involved a murder and alleged witness intimidation. A key State witness changed his story, and in an effort to rehabilitate his testimony, the State hoped to prove that he was being intimidated by defendant Antoine Griffin's girlfriend. The State found what it believed to be the girlfriend's MySpace page with a posting that said, "SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!" Griffin objected to the page's introduction into evidence, arguing that that State could not properly authenticate the document or establish that it was actually his girlfriend's MySpace page, or even if it was, that she posted the message. The trial court found that there was enough information within the printout to meet the threshold requirements of authentication under Maryland Rule 5-901. On appeal, Griffin argued that the trial court erred in admitting the profile as it was not properly authenticated, and its prejudicial effect outweighed its probative value. The appeals court disagreed, finding no reason why social media profiles could not be circumstantially authenticated in the same manner as other forms of electronic communication. It ruled that the document was sufficiently authenticated because 1) the profile picture

was clearly of the girlfriend, 2) the profile stated the girlfriend's actual birthdate, 3) the profile referenced her children, and 4) there was a reference to the girlfriend's admitted nickname for Griffin.

But see the opposite result by the Massachusetts Supreme Court...

Commonwealth of Massachusetts v. Williams, 2010 WL 1999314 (Mass. May 21, 2010). Dwayne Williams was charged in a shooting death and convicted of murder in the first degree primarily on the testimony of two witnesses present at the shooting. During trial, Ashley Noyes, Williams' then girlfriend, testified for the prosecution that Jesse Williams, defendant's brother, had contacted her four times on her MySpace account urging her not to testify against his brother or in the very least to claim a lack of memory. She produced a printout of the messages from her account. The prosecution authenticated the messages through Noyes' testimony that Jesse had a picture of himself on his MySpace account, that his MySpace name was "doit4it," that the messages were sent to her by that MySpace name and bore Jesse's picture and that she replied to the messages and received messages back. On appeal, Williams argued that the trial court erred in admitting the MySpace messages. The Massachusetts Supreme Court agreed that there was insufficient evidence to authenticate the messages and they should not have been admitted. The court noted that there was no testimony regarding how secure the MySpace web page was, about who could access the page, whether codes were needed and whether any one other than Williams could communicate from that web page. However, the court found the admission did not create a substantial likelihood of a miscarriage of justice because Williams was convicted based on the testimony of the two witnesses to the murder.

DATA BREACH CLAIMS: ACTUAL HARM

Ruiz v. Gap, Inc., 2010 U.S. App. LEXIS 10984 (9th Cir. May 28, 2010). The 9th Circuit Court of Appeals affirmed a lower court decision finding that plaintiff's complaint lacked the actual harm necessary to pursue claims resulting from a data breach. This case arose from the theft of two laptop computers from a Gap vendor who processed job applications for Gap. The stolen laptops contained the personal information of applicants who applied for a job at the company. Joel Ruiz, one of the applicants, sued on behalf of the class of applicants on claims of negligence and breach of contract under California law. The U.S. District Court for the Northern District of California rejected the claims because Ruiz failed to show actual injury. The court found that the increased risk of future harm was insufficient to support a negligence claim under California law, and risk of future harm and cost of credit monitoring were not recognizable damages for a breach of contract claim. The Ninth Circuit agreed and affirmed.

NEWS YOU CAN USE

BRAZIL, INDIA SOAR IN CYBERATTACK RANKINGS

Brazil has moved ahead of Germany as the world's number three source of malicious net traffic, and India has risen to number five, according to annual rankings released for 2009 in Symantec's Global Internet Security Threat Report. Still, the U.S. and China remained as first and second, respectively, as the top nations originating cyber attacks. The U.S. accounted for 19 percent of the world's malicious traffic in 2009, down from 23 percent in 2008, and China accounted for eight percent, down from nine percent. Symantec attributes the shift to

the increasing availability of broadband Internet access, especially in emerging nations. The report also shows that: 1) The U.S. is first in five categories, but ranks sixth in delivery of spam; 2) India is second in originating malicious code, and third in delivering spam; 3) Romania is third in developing phishing websites; 4) Spain, Turkey and France are no longer in the top 10 of rankings; and 5) Poland, Romania and Vietnam are rising in cyber attack rankings. The report can be accessed at http://eval.symantec.com/mktginfo/enterprise/white_papers/white_paper_internet_security_threat_report_xv_04-2010.en-us.pdf.

\$51 MILLION AWARDED FOR BROADBAND STIMULUS

The National Telecommunications and Information Administration awarded One Economy Corporation, a nonprofit, and the Broadband Opportunity Coalition, an alliance of civil rights groups, \$28.5 million in broadband stimulus funding – the largest single award ever given for promoting adoption of a technology. In addition, private sector donations from AT&T, Cisco, Comcast, wireless association CTIA, Google and the National Association of Broadcasters will provide an additional \$23 million. The funds will be used for initiatives such as bringing affordable connectivity to 159 housing developments and conducting a national digital literacy awareness campaign targeted at 20 million people. One Economy will also expand its Digital Connectors program, which trains young people in at-risk communities about the Internet and computer technology. The federal funds come from the \$7.2 billion broadband stimulus program.

COURTS SEE INCREASE IN WIRETAP APPLICATIONS

More than 2,370 wiretap applications were filed and granted last year in state and federal courts in the U.S., a 26 percent increase over the previous year, according to a report issued by the Administrative Office of the U.S. Courts. Of that number, 86 percent of the applications targeted drug crimes, with homicide cases the second most prevalent. Federal authorities applied for 663 applications, while state authorities applied for the remaining 1,713. Of the state applications, 71 percent were granted in California, New York and New Jersey. The federal district courts with the most intercept orders were: Arizona (72); Northern District of Illinois (51); Southern District of Texas (37); Northern District of Texas (32); and the Northern District of Georgia (31). No applications were denied in either state or federal court. The wiretap report also examines the average length of wiretaps, the associated costs and the impact in arrests and convictions. The report may be accessed at <http://www.uscourts.gov/wiretap09/2009Wiretaptext.pdf>.

10 COUNTRIES ON COPYRIGHT THEFT WATCH LIST

The U.S. Trade Representative has placed Russia on its list of countries with the worst records of preventing copyright theft for the 13th straight year, with China placed on the list for the sixth consecutive year and Canada for the second. The other nations on the list are Algeria, Argentina, Chile, India, Indonesia, Pakistan, Thailand and Venezuela. While the list carries no sanctions, it aims to shame governments into stopping piracy and updating their copyright laws. The International Intellectual Property Alliance, which represents U.S. copyright industry groups, estimates that U.S. trade losses due to

piracy in more than 36 countries amounted to more than \$15.8 billion in 2009. That figure includes more than \$3.5 billion in China, \$1.9 billion in Russia, \$1.5 billion in India, \$1.1 billion in Italy, \$978 million in Brazil and \$710 million in Canada.

And see...

STUDY: GLOBAL SOFTWARE PIRACY STILL UP IN 2009

While acknowledging progress in stopping the theft of business software, the rate of software piracy grew to 43 percent in 2009, up two percentage points over the previous year, according to a global piracy study by the Business Software Alliance (BSA). The study, conducted for BSA by the International Data Corporation, an IT research firm, attributed much of the increase in piracy to the rise in personal computer users in developing countries, such as Brazil, China and India. For example, the commercial value of pirated software increased in China by \$900 million to \$7.6 billion, the biggest increase of any other country measured in the study. By contrast, the U.S. has the lowest software piracy rate in the world at 20 percent but still has the highest number of computer users. Nevertheless, the commercial value of pirated software in the U.S. was \$8.6 billion in 2009, according to the study. The study also found that the industry made the most progress in combating piracy in Canada, Chile and India, each showing a three percent decline in piracy rates. This study is the seventh BSA piracy report, and for the first time contains the software load by country and the number of software applications believed to be used on each computer. It can be accessed at <http://portal.bsa.org/globalpiracy/2009/index.html>.

SURVEY: EXPERTS CONCERNED ABOUT NETWORK SECURITY

Although 90 percent of private and government security experts believe cyber attacks are a serious threat, they disagree on whether each sector's effort to protect their networks is adequate, according to a survey by the East-West Institute, a nonpartisan think tank. The Institute polled 137 security experts, 34 government officials and 103 private sector security experts from the U.S., China, India, Russia and other countries. Seventy percent of the government officials said that private sector networks were not secure enough, compared with only 30 percent of private sector security officials who believed government networks were not secure enough. The survey found that 43 percent of business security experts and 19 percent of government officials are uncomfortable using online banking. Additionally, a larger 84 percent of private sector officials and 69 percent of government officials are uncomfortable sending personal data, such as Social Security numbers, over the Internet. The results of the survey can be accessed at <http://www.ewi.info/cyber-survey>.

FTC DELAYS "RED FLAGS" ID THEFT RULE

"At the request of several members of Congress," the Federal Trade Commission (FTC) agreed to postpone until the end of the year enforcement of its controversial "Red Flags" rule that would require attorneys, physicians and other professionals to develop written identity theft programs. The rule was developed under the Fair and Accurate Credit Transactions Act, under which Congress directed the FTC and other agencies to develop regulations requiring "creditors" and "financial institutions" to address identity theft. The FTC considers professionals such

as attorneys and physicians to be creditors under the Act, and thus required them to implement programs to detect the warning signs, or "red flags," of identity theft in their daily operations. Last August the American Bar Association filed suit in the U.S. District Court for the District of Columbia, challenging the rule's application to attorneys, and the court agreed, finding the FTC had overreached and applying the rule to attorneys was unreasonable. In May 2010, the American Medical Association sued the FTC, arguing that the rule should not be applied to physicians,

1.2 MILLION PETABYTES FORECAST FOR DIGITAL UNIVERSE

The Digital Universe, which comprises every electronically stored piece of data or file, will reach 1.2 million petabytes this year, according to estimates by IDC, a research and consulting firm. This would be a 62 percent increase, up from 800,000 petabytes, over 2009. The IDC also noted that most of the data is not unique, estimating that 75 percent of it is a copy of some other piece of electronic information. By 2020, IDC estimates that the amount of data will have grown 44 times to 35 trillion gigabytes, with at least 15 percent of it expected to be created, stored and managed in the cloud. However, IDC also cautioned that by 2020 almost one-half of the information in the Digital Universe will require a level of IT-based security that is beyond a baseline level of virus and physical protection. The good news is that staffing and the investment to manage the Digital Universe will only increase modestly between 2010 and 2020, so the cost of managing each byte will drop steadily. A presentation of the IDC data may be accessed at <http://www.emc.com/collateral/demos/microsites/idc-digital-universe/iview.htm>.

STUDY: COLLEGE STUDENTS ADDICTED TO INTERNET

American college students are addicted to cell phones, social media and the Internet and exhibit symptoms similar to drug and alcohol addictions when denied access to these media, according to a study by researchers at the University of Maryland. The researchers asked 200 college students to give up all media for one day, and they observed that after 24 hours many of them showed signs of withdrawal, craving and anxiety, in addition to an inability to function well without their media and social connections. Afterward, many students equated the experience to going without friends or family, with the biggest complaint about the students' need to text and have access to instant messaging. It should be noted that the American Psychiatric Association does not recognize "Internet addiction" as a disorder. A paper on the research may be accessed at <http://www.counseling.umd.edu/Personal/~Kandell/acpbart.htm>.

FCC WIRELESS REPORT SILENT ON COMPETITION

The Federal Communications Commission (FCC) released its annual wireless competition report and, for the first time since 2003, declined to conclude that the wireless marketplace was "effectively competitive." The agency did, however, acknowledge that deciding whether the industry is competitive is complicated. For example, the report notes that competition is dependent on a company's respective position within the market, as well as the dynamics associated with that position. The FCC explained that the mobile wireless ecosystem is sufficiently complex that any analysis of competitive market conditions must consider a large number of factors. As such, the FCC said it decided not to reach an in-

dustry-wide conclusion with respect to whether there is "effective competition." It chose instead to comply with its statutory requirement by providing a detailed analysis of the state of competition that sought to identify areas where market conditions appear to be producing significant consumer benefits and to provide data that can form the basis for inquiries into whether policy changes could result in better outcomes. The report can be accessed at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-81A1.pdf.

And more FCC news...

FCC SURVEY: MOST USERS CLUELESS ON INTERNET SPEED

Eighty percent of Americans do not know the speed of their Internet broadband connections, according to a survey released by the FCC. Nevertheless, 91 percent of broadband users reported they are "very" or "somewhat" satisfied with the speed of their home connections. The FCC polled 1,742 home broadband users in the April-May 2010 time-frame, with a margin of error of plus or minus 2.6 percentage points. To correct this lack of knowledge, the FCC is seeking 100,000 volunteers to participate in a study measuring broadband speeds in which specialized hardware is installed in homes to measure the performance of all major Internet service providers. The tests are designed to help users understand what type of service they are getting from their broadband providers. The survey results may be accessed at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-298516A1.pdf.

POLL: PUBLIC WORRIED ABOUT ONLINE PRIVACY

Eighty-one percent of people said they were “very” or “somewhat” concerned about companies tracking the sites they visit on the Internet and using that information for advertising purposes, according to a poll commissioned by Precursor LLC, a tech and telecom industry research group. In the survey, conducted by Zogby International, 88 percent said it is “unfair” for companies to engage in such tracking without a user’s consent, and 91 percent said it is “unfair” when Internet companies relax their privacy policies after collecting personal information from users. The poll also found that 88 percent thought that consumers should have the same privacy protections online as they have offline, with 79 percent in support of implementing a “do not track” list similar to the “do not call” list which bars telemarketing firms from contacting people on the list. Additionally, 79 percent were in favor of requiring law enforcement to obtain a warrant before tracking a suspect’s Internet activities. It should be noted that only 49 percent felt that government should play a bigger role in protecting online consumer privacy, with 36 percent opposed. The poll included 2,111 adult respondents and had a margin of error of plus or minus 2.2 percentage points. Poll results can be accessed at <http://www.precursorblog.com/files/pdf/topline-report-key-findings.pdf>.

STUDY: PORN SITE USERS FACE EXPLOITATION RISKS

Users who visit pornography sites are at risk for exploitation by cyber criminals, according to a study led by Dr. Gilbert Wondracek of the International Secure System Lab. The researchers analyzed 269,000 websites hosted on the 35,000 pornographic domains, finding that about 3.23 percent of

the sites were booby-trapped with adware, spyware and viruses. Many other sites used “shady” practices to keep users on the site, including javascript catchers which make it hard to leave a page. Other sites use scripts that re-direct visitors to an affiliate site. Researchers also created two adult sites of their own, posted free material on them from pornography producers and spent \$160 to get traffic to view the sites. Analysis of the 49,000 users sent to their sites showed that 20,000 of them were using a computer and browser combination that was vulnerable to at least one known exploit. With many pornographic sites listed in the top 100 most popular web sites on the Internet, there is a potential for large numbers of people being exposed to exploitation. The research team presented their study at the Workshop on the Economics of Information Security at Harvard University in June. The study, “Is the Internet for Pornography? An Insight into the Online Adult Industry,” can be accessed at http://weis2010.econinfosec.org/papers/session2/weis2010_wondracek.pdf.

OTHER SUPREME COURT ACTION

By Marielle Dirkx

Supreme Court Affirms Civil Commitment of Sexually Violent Prisoners

U.S. v. Comstock, 08-1224. The Supreme Court ruled that the federal government, through its powers under Article I of the Constitution, can detain mentally ill, sexually dangerous prisoners through a civil commitment statute beyond the date that the prisoners would have originally been released.

In order to detain the aforementioned prisoners under the federal civil commitment statute, the government must certify that the prisoner has 1.) engaged or attempted to engage in a sexually violent activity or child molestation; 2.) suffers from a serious mental illness, abnormality, or disorder; and 3.) as a result of mental illness, the prisoner is sexually dangerous to others. If the government is able to prove a prisoner is both mentally ill and sexually dangerous, the prisoner is then confined in a suitable federal facility until either the person's mental condition improves to the point where he or she is no longer dangerous, or the state where he or she was tried or domiciled assumes responsibility for his or her care and treatment.

In October and November 2006, the government initiated civil commitment proceedings against five prisoners in the U.S. District Court for the Eastern District of North Carolina. Three of the five had previously pleaded guilty to possession of child pornography, and another pleaded guilty to sexual abuse of a minor. The fifth respondent was charged with sexual abuse of a minor, but was found to be mentally incompetent to stand trial. In response, all five prisoners moved to dismiss the proceedings on the grounds that the federal civil commitment statute was unconstitutional because, in passing it, Congress exceeded its powers under the Constitution, including the Commerce Clause and the Necessary and Proper Clause.

The district court granted the prisoners' motion to dismiss, finding the civil commitments exceeded Congress' legislative power. On appeal, the Fourth Circuit upheld the district court's holding under Article 1. Since the Fourth Circuit ruled on the case, two other circuits have found that the statute is within Congress's legislative power, creating a circuit split.

The Supreme Court, in an opinion authored by Justice Breyer, focused upon the statute as it relates to the realm of Congress' power under the Necessary and Proper Clause. Under the Necessary and Proper Clause, Congress' enumerated powers are supplemented with the broad power to enact laws that are convenient, useful or beneficial to Congress' exercise of the enumerated powers. The statute must be related on a rational basis to the constitutionally enumerated power. The Court found that the relationship between the federal commitment statute and Congress' enumerated powers was not too attenuated, and the statute was not too sweeping in its scope. Furthermore, the federal civil commitment statute is only a minor addition to pre-existing laws governing prison-related mental health issues. Congress had already enacted a commitment statute, which allowed for mentally ill prisoners to be committed after the time they would have been released if, after a hearing, it is established that the person's release would "create a substantial risk of bodily injury to another person or the property of another." Notably, under the iteration of the federal commitment statute at issue in this case, many candidates would have easily been eligible for commitment under the alternative, less controversial, version of the statute. Therefore, the statute is not significantly different from other federal civil commitment statutes except for its focus on criminals who are "sexually dangerous." Moreover, the federal government is the custodian of its prisoners. As such, the federal government has the responsibility to protect people and communities from the dangers the prisoners may impose.

The Court further found that the commitment statute is in accordance with the Tenth Amendment, because the Tenth Amendment only delegates to the states the "powers not delegated to the federal government." The powers delegated to the federal government include those enumerated as well as those granted to the government under the Neces-

sary and Proper Clause. Without regard to any other Constitutional provisions, the Supreme Court held that Congress has the power to enact measures that can be utilized to civilly commit mentally ill, sexually violent offenders, even after the end of their prison sentences.

Supreme Court to Hear Violent Video Game Case

The Supreme Court granted a writ of certiorari to *Entertainment Merchants Ass'n v. Schwarzenegger*. The case raises two constitutional questions regarding California Civil Code sections 1746-1746.5, a ban on the sale or rental of violent video games to children under the age of 18. The first question presented is whether the First Amendment prohibits states from regulating the sale of violent video games to children. If the Constitution prevents states from restricting a minor's purchase of violent video games, and the standard of review is strict scrutiny, then the second issue on appeal is whether the state is required to demonstrate a direct causal link between the video games and physical and psychological harm to children before the state can issue a ban.

The California Code forbids selling or renting violent video games depicting the killing, maiming, dismembering, and sexual assault of a human being to children under the age of 18 when a reasonable person, taking the game as a whole, would find that the game appeals to the morbid or deviant interests of minors; is patently offensive according to community standards; and lacks serious literary, artistic, scientific, or political value. Of note, the Act does not constrain the child's parent or guardian from purchasing or renting violent games for them. When considering the law, the California Legislature examined numerous studies that established a correlation between playing violent video games and increased

aggressiveness, antisocial behavior, and desensitization to violence. In response, the Entertainment Merchants Association (EMA)¹, an association of companies within the video game industry, brought suit against California Governor Arnold Schwarzenegger and other state officials facially challenging the law.

The U.S. District Court for the Northern District of California held that, absent sexual content, violence alone cannot be considered constitutionally unprotected speech. Further, the district court found that as a content-based speech restriction, the law was subject to strict scrutiny review. While the court found the physical and psychological well being of children to be a compelling state interest, it asserted that the State failed to establish a sufficient causal connection between playing violent video games and the harm sought to be avoided by the Act. Finally, the lower court found that it was not the least restrictive means available to the State. The Ninth Circuit affirmed the lower court's ruling, rejecting California's argument that the Act only covers speech that should not be protected under the First Amendment and should be reviewed under the flexible standard that applies to the sale of sexually explicit materials to minors established by *Ginsberg v. New York*, 390 U.S. 629 (1968).

In its appellate brief, the State asserts that excessively violent material, just like sexually explicit material, deserves no First Amendment protection with regard to minors because it has no essential part in the exposition of ideas and very little social value. Furthermore, California argues that allowing states to impose special protection for minors against extremely violent material would uphold the longstanding tradition of providing special government protections for children. Finally, the State claims that even if First Amendment protections apply to video games, the lower courts applied the

LEGISLATIVE NEWS

Cyberbullying

wrong standard for the quantum of evidence required to restrict protected speech by requiring empirical evidence of a direct causal link between video games and harm to children. The proper standard outlined in *Turner Broadcasting System, Inc. v. F.C.C.*, 512 U.S. 622 (1994) is deference to the legislature's predictive judgments as long as the legislature has drawn reasonable inferences based on substantial evidence.

Conversely, EMA emphasizes in its appellate brief that the Act is a typical content-based speech restriction, which properly invokes First Amendment protection and strict scrutiny review. EMA further argues that, while restrictions on video games for violence have been politically popular, two other circuit courts and six other district courts have held that obscenity, with regard to its relationship with the First Amendment, cannot be stretched to encompass violence. Moreover, EMA maintains that a heightened level of causation, more than a tenuous or speculative connection, between physiological and psychological harm to children and violent video games needs to be shown under strict scrutiny review. Further, EMA asserts that even if state legislatures have the right to regulate the sale of violent video games to children, California's statute is unconstitutionally vague.

¹The original plaintiffs in the case were the Video Software Dealers Association (now the EMA) and the Entertainment Software Association.

GEORGIA. ENACTED. On May 27, Governor Sonny Perdue signed into law Senate Bill 250, Georgia's comprehensive anti-bullying law. It specifically includes intimidation, harassment, and threats communicated on a school's computer, computer system, computer network, or other electronic technology that belongs to the school system. The law requires all school districts to adopt anti-bullying policies and requires students guilty of three acts of bullying in one year be sent to an alternative school.

MASSACHUSETTS. ENACTED. On May 3, Governor Deval Patrick signed into law Senate Bill 2404, which aims to eradicate school bullying and was passed unanimously by the Legislature. It prohibits students from cyberbullying, defined as bullying their classmates through the use of technology or electronic means. The law includes within its prohibitions harassment, intimidation, and threats through emails, Internet communications, instant messages, faxes, the creation of a website or blog where the bully impersonates another person, and posting messages online assuming the identity of someone else. The technology used to cyberbully another student does not have to be owned by the school if the bullying creates a hostile environment in school for the victim.

NEW HAMPSHIRE. ENACTED. On June 15, 2010, Governor John Lynch signed into law House Bill 1523, an amendment to the Pupil Safety and Violence Prevention Act. The Law seeks to eliminate bullying from New Hampshire schools and specifically includes cyberbullying. Cyberbullying, under the new Law, is harassing conduct through the use of electronic devices, such as cellular phones, com-

puters, pagers, email, instant messaging, text messaging, and websites. The Law punishes cyberbullying that takes place off school property if the conduct interferes with a student's educational opportunities or substantially disrupts the orderly operations of the school or school-sponsored activity or event.

Internet Gambling

NEW JERSEY. PASSED SENATE COMMITTEE. On June 3, Senate Bill 490, which would allow New Jersey residents to place wagers on the Internet with Atlantic City casinos, was passed favorably by the State Government, Wagering, Tourism & Historic Preservation Committees. The bill would allow all games that can be played at casinos, such as poker, baccarat, blackjack, slot machines, and all of their variations, to be offered for online wagering. All equipment used to conduct Internet wagering, on the part of the casinos, would have to be housed in a secure location, inaccessible to the public and within the city limits of Atlantic City. All casino profits on Internet gambling would be subject to a 20 percent state tax. Casinos would have to fulfill registration and licensing requirements to legally offer online gambling services.

Cybersecurity

INTRODUCED. On June 10, Senator Joseph Lieberman (I-CT) introduced S. 3480, a bill that would mandate continuous monitoring of cybersecurity and create a new cyber office at the White House. The bill would also reform the recruitment, hiring and training of government cybersecurity personnel and require federal agencies to develop cybersecurity workforce plans. The bill was referred to the Committee on Homeland Security and Government Affairs.

PASSED COMMITTEE. On May 20, H.R. 4900, sponsored by Representative Diane Watson (D-CA), was amended and passed by a voice vote in the House Committee on Oversight and Government Reform. The bill seeks to amend the Federal Information Security Management Act of 2002 (Public Law 107-296; 116 Stat. 2135) and create a National Office for Cyberspace. At a minimum, the National Office for Cyberspace will create information security policies and procedures to provide for Government-wide protection of Government-networked computers against common computer attacks and provide protection for all federal agencies against risks, threats, and vulnerabilities of information within individual agencies. Individual federal agencies will be responsible for assessing the risk of harm of unauthorized access or use of information managed or collected by that agency and complying with cybersecurity standards promulgated by the National Office for Cyberspace. The companion Senate bill, S.921 has had no action since it was introduced by Senator Thomas Carper (D-DE).

Mobile Device Identification

INTRODUCED IN SENATE. On May 26, Senator Charles Schumer (D-NY) introduced SB 3427, also known as the Pre-Paid Mobile Device Identification Act. The bill, which has been assigned to the Committee on Commerce, Science, and Transportation, requires resellers of pre-paid mobile phones and SIM cards to collect the full name, address, and date of birth of the purchaser. It also compels resellers to verify the collected information with identification provided by the purchaser, make a record of the sale, and transmit the record to the purchaser's wireless carrier in order to comply with record-keeping protocol. The purpose of this law is to make it harder for criminals and terrorists to plan their crimes anonymously.

ACTION ITEMS

Proposed Sex Offender Registration Guidelines

The Department of Justice published proposed Supplemental Guidelines for Sex Offender Registration and Notification in the Federal Register and may be accessed at http://www.ojp.usdoj.gov/Smart/pdfs/FR_SORNA_051401.pdf. The deadline for public comment is July 13, 2010.

Crime Victims' Service Awards

Nominations are being accepted for the 2011 National Crime Victims' Service Awards, and may be entered at <http://ovcnvrvw.ncjrs.gov/awards/preparation.html>. The deadline for submissions is September 15, 2010.

FREE TRAINING TO ATTORNEYS GENERAL OFFICES

BEST PRACTICES IN CYBERSECURITY

SAVE-THE-DATE

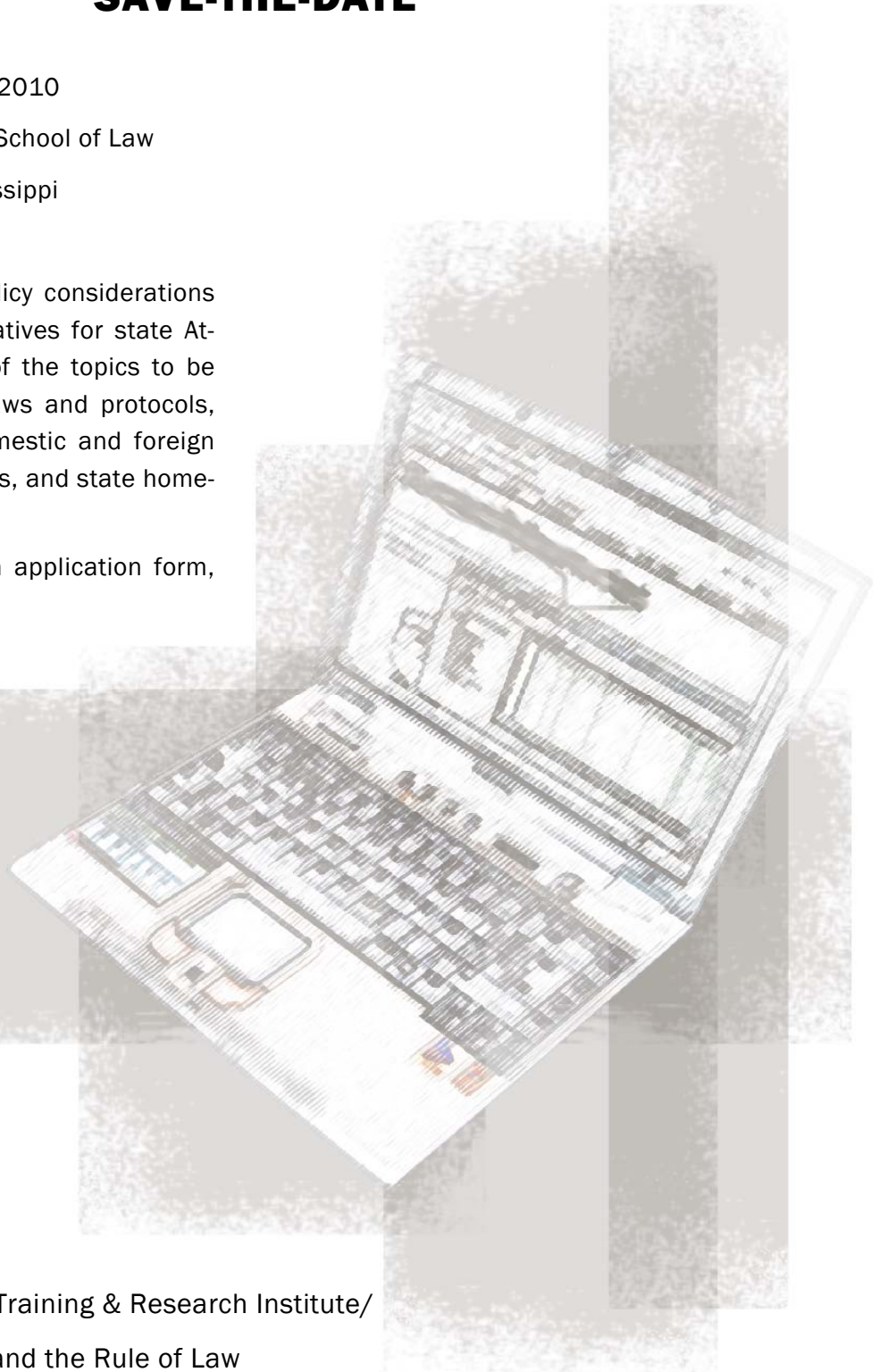
October 26–28, 2010

University of Mississippi School of Law

University, Mississippi

This training will focus on policy considerations in developing cyber security initiatives for state Attorneys General offices. Some of the topics to be covered include cyber security laws and protocols, digital intelligence gathering, domestic and foreign offenders, types of hacking attacks, and state homeland security.

Further details, as well as an application form, will be released shortly.



National Attorneys General Training & Research Institute/
National Center for Justice and the Rule of Law