

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

NOVEMBER-DECEMBER 2009

TABLE OF CONTENTS

FEATURES.....	1
AG'S FIGHTING CYBERCRIME.....	3
IN THE COURTS.....	7
LEGISLATIVE NEWS.....	9
NEWS YOU CAN USE.....	10
REPORTS YOU CAN USE.....	14

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

SUPREME COURT TAKES 4TH AMENDMENT TEXTING CASE

The U.S. Supreme Court agreed to decide whether a police department violated the constitutional privacy rights of an employee when it inspected personal text messages sent and received on a government pager. The case opens "a new frontier in Fourth Amendment jurisprudence," according to a three-judge panel of an appeals court that ruled in favor of the employee. The following is a summary of the case written by Dan Schweitzer, Supreme Court Counsel at NAAG.

City of Ontario v. Quon, 08-1332. At issue is whether a city police department violated the Fourth Amendment rights of a police officer when it read the transcripts of text messages the officer sent while on duty on a department-issued text-messaging pager. The City of Ontario, California had

a written policy advising employees that use of City-owned computer-related services for personal purposes was forbidden, that the City reserves the right to monitor “all network activity including e-mail and Internet use, with or without notice,” and that “[u]sers should have no expectation of privacy or confidentiality when using these resources.” When the City Police Department obtained text-messaging pagers for its SWAT team officers, it told the officers that the e-mail policy applied to pager messages. The City, however, had to pay extra when a pager went above its monthly character limit. The officer in charge of the administration of the pagers, Lieutenant Steve Duke, adopted an informal agreement that he would not audit pagers that went above the monthly limit if the officers agreed to pay for any overages. Eventually, Lieutenant Duke became tired of collecting bills. That prompted the Chief of Police to order a review of the pager transcripts for the two officers with the highest overages to determine whether the monthly character limit was insufficient to cover business-related messages. One of those officers was respondent Sergeant Jeff Quon. After initial Department review, the matter was referred to internal affairs to determine whether Sergeant Quon was wasting time with personal matters while on duty. Internal affairs discovered that, during the month under review, Sergeant Quon sent and received 456 personal messages while on duty, some to his wife, some to his mistress, many sexually explicit in nature. Sergeant Quon, his wife, and his mistress (collectively, respondents) filed a §1983 action against the City, the Police Department, and others (the “City”), alleging Fourth Amendment violations. A jury found that the Chief of Police’s purpose in ordering review of the transcripts was to determine the character limit’s efficacy

The district court ruled that that was reasonable under the circumstances, and therefore constitutional under *O’Connor v. Ortega*, 480 U.S. 709 (1987) (plurality). The Ninth Circuit reversed, hold-

ing that respondents were entitled to summary judgment in their favor. 529 F.3d 892.

The Ninth Circuit held as a threshold matter that respondents possessed a reasonable expectation of privacy in their text messages. The court found that the City’s general non-privacy policy was overridden by Lieutenant Duke’s informal policy of not auditing pagers so long as the officers paid any overages. Because Duke was in charge of administering the pagers, and Quon’s messages had never previously been reviewed, Quon had a reasonable expectation of privacy in the text messages. The court next held that the search was not reasonable. The court applied *O’Connor*, in which the plurality stated that, “[g]iven the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis” that looks to “[t]he operational realities of the workplace.” The court found that the search was not reasonable in scope because the government could have accomplished its objectives through “less intrusive methods” — such as “warning Quon that for the month of September he was forbidden from using his pager for personal communications,” “ask[ing] Quon to count the characters himself,” or “ask[ing] him to redact personal messages and grant permission to the Department to review the redacted transcript.” Seven judges dissented from the denial of rehearing en banc.

The City argues that the Ninth Circuit’s opinion “undermines the ‘operational realities of the workplace’ standard” of *O’Connor* by “erroneously holding that a police lieutenant’s informal policy creates a reasonable expectation of privacy in text messaging on a police department pager in the face of the Department’s explicit no-privacy policy and potential disclosure of the messages as public records.” The City further argues that the Ninth Circuit erred in

applying a “less intrusive means” test to assess the reasonableness of the search. The City cites *Skinner v. Ry. Labor Executives’ Ass’n*, 489 U.S. 602, 629 n.9 (1989), as stating that the Court has “repeatedly” rejected the “existence of alternative ‘less intrusive’ means” as a basis for evaluating the reasonableness of government searches and seizures. According to the City, the court should instead have “balance[ed] [the search’s] intrusion on the individual’s Fourth Amendment interests against its promotion of legitimate governmental interests” (citation omitted). Respondents assert that the Ninth Circuit did not, in fact, adopt a “less intrusive means” test, but rather held that the search “was excessively intrusive in light of the noninvestigatory object of the search.” Respondents further contend that O’Connor mandated a “case-by-case” fact-intensive inquiry, which necessarily limits this case to its facts, such as the precise authority of Lieutenant Duke.

ATTORNEYS GENERAL FIGHTING CYBERCRIME

MULTI-STATE

Thirty-two Attorneys General announced a consumer protection settlement with Vonage, a company providing Voice over Internet Protocol (VoIP) telephone services. The settlement follows an investigation into complaints about the marketing of Vonage services, including advertisements about “free” services, money back guarantees and trial periods, as well as inability to cancel services. The Assurance of Voluntary Compliance (AVC) requires Vonage to issue refunds to consumers who filed valid complaints and those who file new complaints within 120 days. The AVC also requires Vonage to make clear and conspicuous disclosures about

“free” service promotions, money back guarantees and trial periods, as well as the use of paid incentives to customer service representatives who prevent customers from cancelling their Vonage services. The investigation was led by the Attorneys General of **Connecticut, Illinois, Michigan, Oregon, Pennsylvania, Texas** and **Wisconsin**. Also participating in the agreement are the Attorneys General of **Alabama, Arizona, Arkansas, Florida, Hawaii, Idaho, Indiana, Kansas, Kentucky, Louisiana, Maine, Missouri, Montana, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Ohio, South Carolina, South Dakota, Tennessee, Vermont, Washington** and **West Virginia**.

Twelve states are members of a special committee convened by the National Association of Attorneys General (NAAG) to address intellectual property theft. The co-chairs are **Attorneys General Jim Hood of Mississippi and Rob McKenna of Washington**, who were appointed by NAAG President and Nebraska Attorney General Jon Bruning. The other committee members are the Attorneys General of **Delaware, Hawaii, Illinois, Kentucky, Louisiana, Michigan, Montana, New Mexico, Ohio** and **Tennessee**.

DELAWARE

Attorney General Beau Biden announced that the state Child Predator Unit, established by Attorney General Biden’s Office and the State Police, has been awarded \$1,105,000 in federal grant funding to continue and expand its efforts. The funding is comprised of three separate grants: (1) \$437,000 in federal Recovery Act funds (four year grant); \$200,000 in renewable Internet Crimes Against Children funds (one year grant); and \$468,000 in Community-Oriented Policing Services funds (two year grant). The funds will be used to hire additional

staff to support child predator investigations, train first responders and other law enforcement personnel on procedures for addressing 911 calls reporting child predator offenses, assist State Police in tracking down fugitives who use Delaware as a safe haven and/or have failed to register as sex offenders as required by law and pay equipment needs and operational expenses.

FLORIDA

Attorney General Bill McCollum's CyberCrime Unit law enforcement officers arrested Robert Candella on 10 charges of child pornography possession which will be enhanced to second-degree felonies. Images of child pornography were found during an undercover investigation, and investigators traced the images to Candella's computer. A search warrant was executed at his home and two computers, an external hard drive and other digital media were seized. An initial review of the images revealed images of children appearing to be no more than nine years old. The seized equipment will undergo additional forensic analysis. Candella admitted to possessing the images during the investigation. The Orange County Sheriff's Office and the Winter Garden Police Department, both members of Attorney General McCollum's CyberCrime Task Force, as well as the FBI, assisted in the arrest.

ILLINOIS

Attorney General Lisa Madigan's High Tech Crimes Bureau initiated the investigation and obtained a federal search warrant that led to the arrest of Roger McCarty by Bureau investigators, Macomb police and the U.S. Immigration and Customs Enforcement on federal child pornography charges. A search of McCarty's residence had revealed per-

sonal computer equipment containing more than 300 files of child pornography allegedly sent and received over the Internet. The U.S. Attorney's Office charges McCarty with one count of possession of child pornography, which carries a statutory penalty of up to 10 years in prison, and one count of receipt of child pornography, which carries a mandatory minimum statutory penalty of five, and up to 20, years in prison. If the defendant has a prior conviction, the statutory penalty is enhanced to 15 up to 40 years in prison. Both offenses carry terms of supervised release of up to life following imprisonment.

MASSACHUSETTS

Attorney General Martha Coakley received the 2009 National White Collar Crime Center (NW3C) Agency Award for Excellence. The award is presented to an agency whose accomplishments "most exemplify support of the NW3C's mission which is to provide training, investigative support and research to agencies involved in the prevention, investigation and prosecution of economic and high-tech crimes." Attorney General Coakley's Office provided this training program to more than 5,000 law enforcement officers in the state.

MICHIGAN

Attorney General Mike Cox was awarded the Cable's Leaders in Learning Policymaker Award for his work in protecting kids from Internet sex predators with the Michigan Cyber Safety Initiative (Michigan CSI), an in-classroom educational program. The program is offered free of charge to any academic institution providing K-8 education in the state. The award, founded by Cable in the Classroom, the cable industry's national education foundation, is

given to a federal, state or local elected official whose exceptional vision and/or action has dramatically expanded or enhanced learning opportunities for children and youth in their local community, state or region.

MISSISSIPPI

Attorney General Jim Hood's Cyber Crime Unit investigators arrested Stephen Risher, who is charged with five counts of possession of child pornography. The penalty for possession is five to 40 years imprisonment per count. The Lauderdale County Sheriff's Office, part of Mississippi's Internet Crimes Against Children (ICAC) Task Force, assisted with the arrest.

NEBRASKA

Attorney General Jon Bruning announced that Kevin Fullerton pleaded no contest to an online enticement charge. Fullerton believed he was communicating with two underage girls while he committed lewd acts in front of a webcam, but the "girls" were actually investigators from Attorney General Bruning's Office. Online child enticement is a Class IV felony punishable by up to five years in prison, a \$10,000 fine or both. Assistant Attorney General Bill Tangeman handled the case.

NEW JERSEY

Attorney General Anne Milgram announced that Angelo Crocco was charged in a state grand jury indictment for allegedly distributing child pornography over the Internet. Crocco was charged with two counts of second-degree distribution of child por-

nography and one count of fourth-degree distribution of child pornography. The indictment alleges that Crocco used emails to distribute multiple images of child pornography from his America Online account. The State Police Digital Technology Investigations Unit coordinated the investigation. Deputy Attorney General Lee Schaer presented the case to the state grand jury.

NEW MEXICO

Attorney General Gary King's Office distributed more than \$100,000 in specialized computers to state Internet Crimes Against Children (ICAC) affiliates for use in child exploitation cases. The funding for the computers comes from a federal grant which Attorney General King's Office received from the Office of Juvenile Justice and Delinquency Protection.

NEW YORK

Attorney General Andrew Cuomo announced that 13 additional social networking companies, including those owned by Google. Yahoo and AOL, have agreed to remove New York sex offenders from their sites after receiving letters from Attorney General Cuomo. That makes a total of 15 social networking companies that have agreed to use New York's Electronic Securing and Targeting of Online Predators Act (e-STOP), authored by Attorney General Cuomo, which requires all registered sex offenders to register their email accounts, screen names and other Internet identifiers with the state Division of Criminal Justice Services, which then makes the information available to social networking sites. Information about the accounts will be shared with law enforcement.

PENNSYLVANIA

Attorney General Tom Corbett's Child Predator Unit agents arrested Robert Finkenscher, an Ohio high school chemistry teacher, who is accused of using the Internet to sexually proposition what he believed was a 13-year-old girl, as well as sending sexually explicit webcam videos to the "girl." Finkenscher allegedly used Internet chat rooms and instant message programs to approach the "girl," who was actually a Unit undercover agent. Finkenscher is charged with five counts of criminal attempted unlawful contact with a minor (related to obscene or sexually explicit material) and one count of criminal use of a computer, all third-degree felonies each punishable by up to seven years in prison and \$15,000 fines. Fickenscher will be prosecuted by Deputy Attorney General William Caye II of the Unit. The Lake County, Ohio Sheriff's Department and the FBI assisted in the investigation.

SOUTH CAROLINA

Attorney General Henry McMaster's Office arrested Richard Lipkin during an undercover Internet sting on one count of Criminal Solicitation of a Minor and one count of Dissemination of Obscene Material to a Minor, both felony offenses each punishable by up to 10 years imprisonment. A search warrant was executed on Lipkin's home, and four computers were seized. The Richland County Sheriff's Office, a member of Attorney General McMaster's Internet Crimes Against Children (ICAC) Task Force, assisted with the arrest.

TEXAS

Attorney General Greg Abbott filed two enforcement actions against Intercept, L.L.C. and Everyprice.com, Inc., which operate "price-comparison" web sites, charging them with unlawfully misleading online shoppers about the reliability and trustworthiness of several Internet merchants. Although both sites claim independent web site comparisons, Attorney General Abbott's investigators uncovered a cash-for-ratings scheme in which online retailers paid for higher ratings. Intercept, L.L.C., which operates several web sites, including Shopcartusa.com, Diduprice.com, FlyingPrices.com, Digitalsaver.com and Pricingdepot.com, entered into an agreement judgment with Attorney General Abbott after he filed suit, promising to correct its unlawful practices and either pay a \$300,000 civil penalty or cease doing business. In the suit against Everyprice.com, Inc, which operates Everyprice.com and Lowpricedigital.com, the state seeks civil penalties of up to \$20,000 per violation of the Deceptive Trade Practices Act, attorney's fees and restitution where necessary.

UTAH

Attorney General Mark Shurtleff joined Governor Gary Herbert, state Senate President Michael Wadouds and Speaker of the House David Clark to unveil an Internet safety program which will be provided free to state parents, teachers and law enforcement officers. The program, "Wired for Wisdom," was created by the Entertainment Software Association and Web Wise Kids to help educate parents about keeping their children safe online.

VIRGINIA

Attorney General William Sims announced a partnership with Enough is Enough, The Family Foundation and the Virginia Interfaith Center to promote an Internet safety program, "Internet Safety 101: Empowering Parents," that will equip the faith-based community to teach Internet safety. The reproduction and distribution of Internet safety kits to churches, synagogues and mosques was funded by Attorney General Mims' Youth Internet Safety fund with contributions from AOL and News Corp. Enough is Enough produced the program in partnership with the U.S. Department of Justice, AOL, MySpace and other partners. The Virginia Interfaith Center and the Family Foundation will distribute the program to their network of faith-based partners in Virginia.

WASHINGTON

Attorney General Rob McKenna testified before the U.S. Senate Committee on Commerce, Science and Transportation to encourage getting tough on companies that engage in deceptive online sales tactics. Attorney General McKenna's five-page statement describes how certain marketing methods have been purposefully used to deceive consumers into paying monthly membership fees for services they didn't want.

WEST VIRGINIA

Attorney General Darrell McGraw, Jr. filed two suits against Internet payday lenders and their collection agencies. The first suit is against FFD Resources, a group of interconnected corporations and individuals that jointly operates four web sites making usurious payday loans. The suit alleges that FFD

companies have refused to comply with Attorney General McGraw's investigative subpoenas and have continued to collect their unlawful loans in violation of a court order. The second suit asks the court to order collection agencies Capital Collections, L.L.C.; Cairns Investigators of America; Crime Monitoring Center; and Premier Recovery Group to comply with his investigative subpoenas and to stop collecting Internet payday loans.

WISCONSIN

Attorney General J.B. Van Hollen announced that the Merrill Police Department joined the Wisconsin Internet Crimes Against Children (ICAC) Task Force. As part of the Task Force, the Department is eligible for reimbursement to help fund ICAC-related expenses, priority for ICAC-related training, investigative assistance from trained ICAC investigators and computer forensic analysts, access to the national ICAC email group and recognition on Attorney General Van Hollen's web site.

IN THE COURTS

ADMISSIBILITY: MYSPACE PAGES

Clark v. State, 2009 WL 3319674 (Ind. October 15, 2009). The Indiana Supreme Court found that defendant's MySpace page was properly admitted into evidence by the trial court. Ian Clark was charged with murdering his fiancée's two-year-old daughter. At trial, he testified in his own defense, claiming he had acted recklessly, not intentionally, and should be found guilty of reckless homicide, not murder. During his testimony, the prosecution entered Clark's MySpace page, in which he bragged about his ability to get away with it. Clark was found guilty of murder and appealed to the Indiana Su-

preme Court. He argued that the entry of his MySpace page was inadmissible character evidence admitted in violation of Ind. R. Evid. 404(b), which precludes the admission of evidence intended to demonstrate the defendant's propensity to commit the crime charged. The court found the rule inapplicable because the evidence was comprised of Clark's own statements, not prior acts. The court also found that the trial court did not err in admitting the evidence, since Clark's own testimony raised the issue of his character. The verdict was affirmed.

Ed. Note: J.T. Whitehead, Deputy Attorney General in the Office of the Attorney General of Indiana, represented the State.

PROBABLE CAUSE: SUBSCRIPTION TO WEB SITE

U.S. v. Frechette, 583 F.3d 374 (6th Cir. October 8, 2009). The 6th Circuit Court of Appeals reversed the suppression of evidence by the district court, finding that in a crime involving child pornography, 16 months between the affidavit and the time of a subscription to a web site featuring child pornography did not make the information stale. ICE agents learned that Douglas Frechette, a registered sex offender, paid for a one-month subscription to a web site they knew contained child pornography in January 2007 and opened an investigation. In April 2008, an agent presented an affidavit to search the residence to a magistrate, recounting what was learned about Frechette's subscription and stating that based on his experience, evidence of the storage of child pornography is often present on the computer hard drives of consumers of child pornography. The magistrate determined that probable cause existed that evidence could be found at Frechette's residence and issued a search warrant. Upon execution of the warrant, agents recovered child pornography from Frechette's computer. A federal grand jury indicted him on receipt and posses-

sion of child pornography. Frechette moved to suppress the evidence, challenging the sufficiency of the affidavit supporting the search warrant, and the U.S. District Court for the Western District of Michigan agreed, finding the allegations in the affidavit to be stale because there was a 16 month lapse between the subscription and the affidavit and there was no link between the factual basis and the conclusion that there was a fair probability that evidence would be found at Frechette's residence. The government appealed, and a divided 6th Circuit reversed and remanded, finding that possessors of child pornography often kept the images for a long time so the images had an "infinite lifespan."

FIRST AMENDMENT: VIRTUAL TOWN

Estavillo v. Sony Computer Entertainment America, Inc., 2009 U.S. Dist. LEXIS 86821 (N.D. Cal. September 22, 2009). The U.S. District Court for the Northern District of California found that the First Amendment does not apply to an ouster from a virtual town because the online network was neither a state actor nor a "company town." Erik Estavillo was banned from Sony's Playstation 3 network for violating network use terms. He sued Sony for \$55,000 in damages, alleging that the First Amendment's guarantee of free speech precluded Sony from removing him from the network. Sony moved to dismiss for failure to state a claim, which the district court granted. In order to implicate the First Amendment in a restriction on action, the court must perceive that state action has taken place. In the instant case, the court held that because Sony was not a state actor for First Amendment purposes, nor a "company" town (an exception to the state action requirement of the First Amendment), Estavillo could not maintain an action against Sony for infringement of free speech rights.

POSSESSION OF CHILD PORNOGRAPHY: JURY VIEWING OF CLIPS

U.S. v. Caldwell, 2009 WL 3425074 (5th Cir. October 26, 2009). The 5th Circuit Court of Appeals upheld defendant's conviction on possession of child pornography, finding that the showing of child pornography clips to the jury was necessary to allow them to "form a narrative" of the illegal behavior. Arkon Caldwell was charged and convicted of knowingly possessing child pornography in the U.S. District Court for the Western District of Texas. At trial, the prosecution was allowed to show the jury brief clips from three of the child pornography videos found on Caldwell's computer. In order to show that Caldwell was fully aware he was downloading pornography, the prosecution also showed the jury two adult pornographic videos from the computer, one of which featured bestiality. On appeal, Caldwell argued that the trial court erred in allowing the jury to view the clips, because he had admitted, and the jury knew, that the videos contained pornography. Therefore, he argued, showing the videos was unnecessary and prejudicial, and the showing of the adult pornography was irrelevant. The 5th Circuit disagreed, finding that the clips allowed the jurors to form an opinion as to whether Caldwell was guilty and that the jury expected to see such clips in a child pornography case. As to the showing of adult pornography, the court found it to be harmless error in light of the overwhelming evidence against Caldwell.

LEGISLATIVE NEWS

DATA SECURITY

PASSED SENATE COMMITTEE. On November 5, S. 1490, a bill sponsored by Senator Patrick Leahy (D-VT), passed the Senate Committee on the Judiciary. The bill adds intentionally accessing a com-

puter without authorization to the definition of racketeering activity, imposes a fine and/or a prison term of up to five years for intentionally concealing a security breach involving sensitive personal information causing economic harm to at least one person and imposes requirements for a data privacy and security program on business entities that maintain personally identifiable information in electronic or digital form on 10,000 or more persons. The bill also requires any agency or business entity with personally identifiable information to notify any person affected of a breach without unreasonable delay. The bill preempts state regulation of data brokers and state laws relating to safeguards for the protection of sensitive personally identifiable information. It allows state Attorneys General to bring a civil action in a U.S. district court for violation of security breach notification requirements.

PASSED BY THE HOUSE. On December 8, the House passed H.R. 2221, a bill sponsored by Representative Bobby Rush (D-IL), which would require the Federal Trade Commission (FTC) to establish regulations requiring each person engaged in interstate commerce who possesses electronic data containing personal information to establish security policies and procedures. It also requires information brokers to submit their security policies to the FTC with a security breach notification or on request. The bill would preempt state information security laws. It was referred to the Senate Committee on Commerce, Science and Transportation.

INTERNET SAFETY

INTRODUCED IN HOUSE. On November 6, Representative Bart Stupak (D-MI) introduced H.R. 4059, a bill that would require age verification by the operator of any web site carrying out a financial transaction involving a product or service in which sale or access is unlawful to persons under a certain age. The bill was referred to the Committee on Energy

and Commerce.

PEER-TO-PEER USE

INTRODUCED IN HOUSE. On November 17, Representative Edolphus Towns (D-NY) introduced H.R. 4098, a bill which would require the Office of Management and Budget to issue guidance on the use of peer-to-peer file-sharing software and would prohibit its personal use by federal employees. The bill was referred to the Committee on Oversight and Government Reform.

PASSED BY THE HOUSE. On December 8, the House passed H.R. 1319, a bill sponsored by Representative Mary Mack Bono (R-CA), which makes it unlawful to induce a user to make files available to another user through the use of peer-to-peer software or to prevent a computer user from blocking the installation or functioning of a peer-to-peer software program. The bill was referred to the Senate Committee on Commerce, Science and Transportation.

CYBERSECURITY

PASSED HOUSE COMMITTEE. On November 18, the House Committee on Science and Technology passed H.R. 4061, a bill sponsored by Representative Dan Lipinski (D-IL), to advance cybersecurity research, development and technical standards.

NEWS YOU CAN USE

CRIMES AGAINST CHILDREN CENTER GETS \$2 MILLION GRANT

The Crimes Against Children Research Center (CCRC) of the University of New Hampshire received more than \$2 million in U.S. Department of Justice funding to further its research into Internet crimes against children (ICAC). Under the grant, the CCRC will conduct three studies: (1) an evaluation of Internet child safety materials used by ICAC task forces in schools and communities, (2) the third Youth Internet Safety Survey and (3) the third National Juvenile Online Victimization Study. In (1) above, according to principal investigator Dr. Lisa Jones, the project will produce a standardized toolkit to rate victimization prevention programs. It will also determine whether the way prevention messages are currently being delivered coincides with what is known to work for other at-risk behaviors, such as drugs and alcohol. In (2) above, a nationally representative sample of 10- to 17-year-olds will be interviewed via phone about their experiences with technology over the past year. According to lead researcher Dr. Kim Mitchell, this is the same methodology used in the previous two studies to allow comparison and discovery of trends. In (3) above, investigators and prosecutors involved with more than 1,000 crimes will be interviewed in-house to determine which investigative strategies appear to be working, how law enforcement is responding to cases and changing trends from the first two studies. According to lead researcher Janis Wolak, the project also seeks to determine how increased training and undercover operations have affected arrests.

ICANN TO HAVE INTERNATIONAL OVERSIGHT

The Internet Corporation for Assigned Names and Numbers (ICANN) and the U.S. Department of Commerce agreed to set up international oversight of the domain name system organization, allowing it greater independence and giving more countries oversight. The agreement sets up reviews of ICANN's performance every three years with ICANN members, the Department of Commerce, independent experts and others on the review team. However, the agreement does not change the Department's contract with ICANN to perform the functions of the Internet Assigned Numbers Authority (IANA), which is responsible for the global coordination of the domain name system (DNS) Root, IP addressing and other Internet protocol resources. Additionally, the Department stated that it does not endorse ICANN's efforts to allow an unlimited number of new generic top-level domains, such as .food and .basketball. A copy of the agreement can be accessed at <http://icann.org/en/announcements/announcement-30sep09-en.htm>.

And more ICANN news...

ICANN TO ALLOW NON-LATIN DOMAIN NAMES

ICANN voted to allow domain names in non-Latin script, including Arabic and Chinese. The decision will pave the way for the Internet's Domain Name System (DNS) to be changed so it can recognize and translate non-Latin characters. The complicated technical feature allowing Internationalized Domain Names (IDNs) would represent the biggest change to the coding that underlies the Internet since it was invented. Conceivably, the first IDNs could be in use

as early as next year. It is likely that the first IDNs to be approved will be in Chinese and Arabic, with Russian to follow. Although some countries, such as China and Thailand, have introduced workarounds, these solutions are neither internationally approved nor do they work on all computers.

REPORT: CONCERN OVER SMART GRID VULNERABILITIES

A cybersecurity task force at the National Institute of Standards And Technology released a report assessing security and privacy requirements for the U.S. Smart Grid, as well as strategies needed to address them. The report looks at vulnerabilities that can arise during the operation of a smart grid, as well as problems such as authenticating and authorizing users to substations, key management for meters and intrusion detection for power equipment. It also considered vulnerabilities arising from inadequate patching; configuration and change management processes; weak access controls; and lack of risk assessment, audit, management and incident response plans. The report also noted that vulnerabilities associated with bad software coding practices, including input validation errors and user authentication errors, can pose a risk to the grid's integrity. The real-time, two-way communication between consumers and suppliers in a smart grid also raises privacy concerns, and the report explained that there must be more of an understanding of how collected data will be distributed throughout the smart grid system. The report may be accessed at http://www.nist.gov/public_affairs/releases/smartgrid_inoperability.pdf.

SURVEY: 93% SUPPORT TEXTING WHILE DRIVING BAN

A national survey conducted by Penn, Schoen & Berland Associates on behalf of Ford Motor Company found that 86 percent of U.S. drivers described handheld texting while driving as very dangerous, with 93 percent supporting a nationwide ban on such texting. However, only 42 percent of those surveyed believed drivers would stop if the practice were banned. This number increased to 75 percent if hands-free or voice-activated technologies were widely available. In fact, the survey found that 67 percent of drivers believed voice-activated technology to be a safe alternative to texting, and 76 percent said it would be an appealing feature in a car. Currently, 18 states have enacted bans on handheld cell phones and/or texting while driving, although nearly 40 percent of drivers in those states indicated they were unaware of the ban,

And more on texting while driving...

SURVEY: ONE-THIRD OF TEENS TEXT WHILE DRIVING

One-third of cell phone users aged 16 and 17 admitted to texting while driving, despite increased publicity over the dangers of doing so, according to a survey by the Pew Research Center. The survey also reported that 48 percent of teens admitted they have been in a car while the driver was texting. Forty percent reported being in a car when the driver used a cell phone in a way that put them in danger. The survey report noted that some teens do not understand the risk and even flaunt laws enacted to prohibit while driving. The report can be accessed at <http://pewresearch.org/assets/pdf/teens-and-distracted-driving.pdf>.

LAW SCHOOLS TO EXPAND SUPREME COURT DATABASE

Four law schools and two undergraduate universities received an \$874,000 National Science Foundation grant for a four-year project to expand an online U.S. Supreme Court database to go back to the court's first recorded decision in 1792. The project will add 19,675 cases to the database that now extends from the court's 1953 term through 2008. The project intends to post 4,400 cases by summer 2010. The schools involved are Northwestern University School of Law, the University of Pennsylvania Law School, Washington University Law School, Michigan State University College of Law and the political science departments at Princeton University and Stony Brook University. The database was created by Harold Spaeth, professor emeritus at Michigan State, during the 1980s for research. The schools redesigned it last year with updated technology to make it more user-friendly. The site also tracks dissents and lets users analyze statistics in graphs and tables.

FREECREDITREPORT.COM AWARDED 1,017 DOMAIN NAMES

The National Arbitration Forum published an historic domain dispute decision, awarding 1,017 cybersquatting domain names to FreeCreditReport.com. The complaint was filed by ConsumerInfo.com, owner of FreeCreditReport.com, through a process known as the Uniform Domain-Name Dispute-Resolution Policy (UDRP), and is believed to be the largest case in the 10 years since the UDRP was enacted. FreeCreditReport.com was represented by CitizenHawk, Inc., which is not a law firm, but which specializes in the automated creation of UDRP complaints using proprietary software. The disputed domain names were all slight misspellings of Free-

CreditReport.com or included the name spelled correctly within a larger domain, such as 1-800-freecreditreport.com. The respondent in the case was Netcorp LLC, which argued that the disputed domain names were common, descriptive and therefore generic names.

ABA SITE LISTS TOP APPEALS COURT DECISIONS

The American Bar Association's Standing Committee on Federal Judicial Improvements launched a web site that will summarize some of the most interesting or newsworthy recent decisions and pending cases before federal appeals courts. Currently the project covers the Third, Fifth and Ninth Circuits, with the rest rolling out in future months. The case selection and summaries are being done by Temple University Beasley School of Law for the Third Circuit, the University of Texas School of Law for the Fifth Circuit and the University of Arizona James E. Rogers College of Law for the Ninth Circuit. The site was developed to help the media expand coverage of the federal courts, and reporters and others can sign up to receive alerts about new cases. The site can be accessed at <http://www.abanet.org/SCFJI/Pages/MediaAlertsOnFederalCircuitCourts.aspx>.

CYBERSECURITY RESEARCH CONSORTIUM FORMED

Three universities with established cybersecurity programs joined with Northrop Grumman Corp. to form a cybersecurity research consortium seeking solutions to the increase in network-based spying and computer hacking. The consortium of Carnegie Mellon, the Massachusetts Institute of Technology and Purdue University was established under a five-year, multi-million dollar a year grant program un-

derwritten by Northrop Grumman, which provides cybersecurity technology and monitoring services. Each university will use the grants to increase efforts in three or four research projects in areas of their expertise and will collaborate with each other and Northrop Grumman. The project's consortium members will pursue include efforts to better protect computers and networks from attacks, to allow quicker recognition of intrusions and to develop better forensics to analyze the nature of attacks and their impact.

SURVEY: ONE-THIRD OF YOUTHS ENGAGE IN SEXTING

Nearly one-third of youths admit engaging in sexting-related activities that involved either e-mailing a photo or video of themselves in the nude or being the recipient of such images, according to a survey conducted by MTV and the Associated Press. Of those who admitted to distributing suggestive images of themselves, about 61 percent reported that they were pressured by someone to send the image. The survey further found that girls were more likely to share a naked image of themselves than boys. It also found that those who are sexually active were much more likely to send an image than those who were not. Most of the respondents sent the image to a significant other or a person of romantic interest to them. However, 29 percent said they shared naked images of themselves with someone they knew only online. The survey is part of "A Thin Line," a multi-year campaign launched by MTV with numerous partners to educate teens and college-age students about safe and appropriate digital behavior. The survey findings can be accessed at <http://www.athinline.org/MTV-AP-Digital-Abuse-Study-Full.pdf>.

WHITE HOUSE NAMES CYBER CORRDINATOR

The White House has tapped Howard Schmidt, president and CEO of the Information Security Forum, a nonprofit international consortium that conducts information security research, as cyber security coordinator. Schmidt has served as chief security officer for Microsoft and as cyber security chief for eBay. His 40-year career includes 31 years in local and federal government service, including serving as vice chairman of the Critical Infrastructure Protection Board in the Bush administration. He has also served as an advisor to the FBI and has worked at the National Drug Intelligence Center.

Ed. Note: Howard Schmidt was the keynote speaker at the first cybercrime training held under the NAAG-NCJRL partnership.

“Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition”

This publication by the National Institute of Justice is designed to assist state and local law enforcement and other first responders who may be responsible for preserving an electronic crime scene and for recognizing, collecting and safeguarding digital evidence. It also describes different types of electronic devices and explains how to secure, evaluate and document the scene. It can be accessed at <http://www.ncjrs.gov/pdffiles1/nij/219941.pdf>.

REPORTS YOU CAN USE

“Peer-to-Peer File Sharing: Pandora’s Box of Child Porn?”

This paper discusses the proliferation of child pornography through P2P and highlights the legislation advanced to Congress to contain it as well as the efforts by law enforcement and industry leaders to combat it. It can be accessed at http://stopchildpredators.org/pdf/SCP_on_P2P_File_Sharing_Pandoras_Box_of_Child_Pornography_1109.pdf.