

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

JULY-AUGUST 2009

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

This project is supported by grants provided by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the authors and do not represent the official position of the United States Department of Justice.

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

In the interest of making this newsletter as useful a tool as possible for you, we ask that you keep us informed of your efforts. Additionally, we would

TABLE OF CONTENTS

FEATURES.....	1
AG'S FIGHTING CYBERCRIME.....	6
IN THE COURTS.....	11
SUPREME COURT UPDATE.....	14
LEGISLATIVE NEWS.....	16
NEWS YOU CAN USE.....	17
TOOLS YOU CAN USE.....	19
FREE TRAINING.....	20
EMPLOYMENT.....	21

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

“THE PERFECT STORM: THE COLLISION OF ELECTRONIC HEALTH RECORDS AND IN-ADVERTENT PEER TO PEER FILE SHARING”

*By Catie Ashburn**

Introduction

Watching the health care debate brings to mind a meteorologist's map during coverage of an impending weather event; as the storm approaches the mainland, winds pick up speed, the radius grows larger, and the soon-to-be affected population braces for the impact. Rebuilding of multiple aspects of the medical field is on the horizon, ranging from a potential shift from curative medicine to pre-

ventive medicine down to the billing of practitioner's services.¹ Amidst the details involved in this expansive reorganization, a move away from traditional paper files towards electronic health records ("EHR") seems inevitable and, in most regards, a necessary step in reforming the current system.²

When the foreseeable upheaval of conversion to an EHR system hits the U.S. health care world, the possibility of collision with the already existing peer-to-peer file sharing storm creates truly dangerous conditions for privacy and security of patients' confidential information. As discussed in more detail below, peer-to-peer file sharing protocols are popular for the sharing of media files across an open network, however abuse of these networks concerns legislators and law enforcement alike.³ As just one example, a recent study found thousands of sensitive medical records accessible through simple searches on peer-to-peer networks.⁴

Partially funded by the Department of Homeland Security and working in conjunction with the peer-to-peer intelligence service company Tiversa, M. Eric Johnson, the director of the Center for Digital Strategies at Dartmouth, presented the study's results at the Financial Cryptography and Data Security Conference in February 2009.⁵ Johnson's findings included access to an online "fill-in-the-blank" template prescription pad, psychiatric evaluations from mental health centers in multiple states, and a 1,718-page document that included Social Security numbers, insurance information and treatment codes for over 9,000 patients.⁶ The potential harm resulting from identity theft, insurance and Medicaid fraud, and abuse of prescription medication is all too real.

This article first looks at what characterizes a high-performing EHR system and the pros and cons of the implementation of such a system. The article

focuses on privacy as the primary concern with EHR systems and the potential for breaches through abuse of peer-to-peer file sharing protocols. In conclusion, the article provides a summary of recommendations for state action related to the possible overlap of EHR and file sharing.

Defining an EHR System

EHR appeared on the national policy podium in April 2004 when former President George W. Bush revealed plans to create a National Health Information Network (NHIN), intended to computerize most health records within ten years.⁷ In 2008, the State Alliance for E-Health released their first annual report analyzing the future of health information technology and the states' roles in implementing and navigating these systems.⁸ Most recently, President Barack Obama signed the American Recovery and Reinvestment Act of 2009 ("Recovery Act") which provides \$20 million to the Department of Health and Human Services for the development of standards research for the security and interoperability of EHR.⁹ Over the past several years, scholars, both within the law and biotechnical fields, have studied and debated the positive and negative aspects of EHR, with an eye on the regulations needed for control of a yet untested program.

An ideal EHR system functions on multiple different levels, above and beyond simple record keeping. The core elements include the ability to display health information and data related to a patient, manage results of tests and procedures to enhance detection of abnormalities, computerize prescriptions and reduce mistakes due to poor handwriting, and provide a means of electronic communication for a patient's entire medical team across the nation.¹⁰ These elements, working at their peak efficiency, will improve a patient's medical treatment by making information critical to a comprehensive treatment and wellness plan available to the multi-

ple providers a patient will come into contact with through a lifetime.¹¹

Interoperability, or “the ability for systems to exchange data and to operate in a coordinated, seamless manner,”¹² is the biggest key to meeting this level of performance. A patient’s medical records would be available for access by providers in different cities, in different fields, and in different physician networks.¹³ Currently, some hospitals and clinics enter patient information into an internal electronic network, but an NHIN envisions a uniform, centralized system allowing access to a patient’s complete medical history, allergies, and current prescribed medications.¹⁴

Concerns with EHR Systems

The benefits of an EHR system outweigh the risks if the system is designed to anticipate every possible breakdown. Imagine a storm wall or levy system guaranteed to protect a city’s population from a level 5 hurricane; there is no doubt that such a system could be built, but the “wait-and-see” aspect of testing its strength creates much anxiety. Scholars raise questions of potential errors in the system and the tremendous effect such errors will have on patients, whether the errors result from breakdowns in the technology itself or as a result of human interaction with the system through data input.¹⁵ Training providers, converting existing paper records to electronic, and installation of the system nationwide are but three of the factors playing a role in a cost, burden, and time assessment; there is little doubt that the cost of implementing an NHIN will be significant.¹⁶

Privacy and security concerns cause the greatest and most realized fear to date, especially for the states.¹⁷ In light of the trepidations related to breaches of patient privacy, the U.S. Department of

Health and Human Services promulgated the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and Security Rule.¹⁸ These rules are criticized for their narrow application to electronic records, their lack of a private cause of action, and vague language which frustrate compliance efforts.¹⁹ State privacy laws will also play a large role in the development of the NHIN. Because HIPAA creates a baseline privacy standard, states with more lenient laws are preempted by HIPAA.²⁰ A different distress focuses on outsiders to the health care industry breaching patient records with the intent of committing identity theft and fraud; the frequent and widespread use of peer-to-peer file sharing protocols opens the door to inadvertent sharing of secure files from EHR systems.²¹ Like the inevitable storm of conversion to an EHR system, the use of peer-to-peer file sharing can no longer be avoided or ignored.

When Two Storms Collide

File sharing protocols, such as Lime Wire, KaZaA, and BitTorrent, allow multiple users to gain access to information on other computers linked into the network.²² Often, individuals use the protocols to share media files, such as music and film downloads. These protocols are frowned on for promoting copyright infringement and exposing unsophisticated users to inadvertent file sharing.²³ For example, a home computer user may be listening to music using a Lime Wire protocol, but because of setting selections made in the process of installing Lime Wire on their computer, other users may be able to access thousands of files on the home user’s computer, including downloaded bank statements, saved tax returns, and personal images of family and friends.²⁴

Taking this example a step further and into the future, envision a hospital employee listening to music on their work computer while inputting data from

saved EHR into the theoretical NHIN. Although the NHIN may be a more secure closed network,²⁵ the chance of exposing insurance data, confidential medical diagnoses, prescriptions, and billing information remains a real possibility given the need for transfer of the data from an insecure data file to the closed NHIN system.²⁶

Several congressional hearings have taken place regarding the dangers of peer-to-peer file sharing protocols.²⁷ Until recently, Congress, in the spirit of self-regulation, permitted these companies to fix their protocols' security omissions through updates to their respective networks.²⁸ Currently, the mood is changing on the national level and two pieces of legislation provide for oversight capabilities by the Federal Trade Commission (FTC). H.R. 1319, introduced by Rep. Mary Bono Mack (R - CA) and referred to the Committee on Energy and Commerce, aims to prevent inadvertent disclosure of files by requiring file sharing programs to provide "clear and conspicuous notice" of items that will be shared through installation and use of the program.²⁹ H.R. 2221, introduced by Rep. Bobby Rush (D - IL) and also referred to the Committee on Energy and Commerce, calls for the FTC to promulgate regulations requiring FTC approval of electronic information brokers' security policies.³⁰ The bill also creates a national breach notification law for any person or company involved in interstate commerce.³¹

Although these bills bring a serious security issue to a national level, the states are better equipped and more capable of handling the breaches occurring through peer-to-peer file sharing.³² Especially in cases relating to health records when medical providers and patients reside in the same state, individual victims stand a greater chance of relief and vindication through prosecution on the state level.³³ State Attorneys General and local prosecutors have several options in protecting

the privacy of their state's citizens and maintaining state-level control of prosecutions involving privacy breaches.

States' Roles in Protection from the Storm

Often when facing an impending obstacle, the best defense is a good offense. The State Alliance for E-Health takes this approach by encouraging states to promote and play an active role in the development of EHR systems.³⁴ A creation of the National Governors Association Center for Best Practices and composed of executive-level state elected and appointed officials, the State Alliance released their first annual report in 2008.³⁵ The report represents a compilation of testimony, research, and in depth deliberations that concludes in a set of recommendations.³⁶ These consist of, inter alia, "consolidating and updating relevant [state] privacy and security laws" in addressing health information privacy and participation "in national certification and standards-setting processes."³⁷ Support and action by the states should also include an alignment of "policies and laws to support intra- and interstate data exchange among public programs."³⁸ State created models put into practice in state supported programs, such as Medicaid, can serve as templates for the eventual extension of EHR systems to the private sector.³⁹ By taking an affirmative role in the creation and implementation of EHR systems, states will have a clearer grasp on the technology's future impact in their particular region.

A second option for states centers on corrective action after a breach occurs. In 45 of 50 states, a breach notification law requires companies that suffer a data breach to give written notice to customers if the customer's personal information is leaked.⁴⁰ The specifics vary slightly from state to state, but in general, the laws contain notification guidelines about how soon a company must notify its customers, penalties for failure to disclose,

whether a private right of action is available to customers, and what kinds of breaches are exempt from the notification requirements.⁴¹ A company, including hospitals and medical clinics, has little to no incentive to comply with breach notification laws if no enforcement occurs. For the laws to be effective enforcement by states must become the norm; hopefully, this will result in a trickle down effect whereby companies move towards greater security of their internal network, more workforce training, and less opportunity for breach through peer-to-peer file sharing protocols.

States should take the lead in education and awareness endeavors, teaching government agencies and private companies the best methods of securing their customers' personal information. In seeking medical attention, patients entrust their most confidential information to health care providers; the development and implementation to EHR systems will have long-term positive effects, as long as short-term efforts are made to guard against possible break downs. Federal breach notification laws and regulation of peer-to-peer file sharing networks seem on the horizon, but state enforcement actions today will result in constituent confidence in the rising use of EHR systems.

*Catie Ashburn was a NAAG summer intern from the University of Mississippi School of Law.

1 See Summary of the White House's Position on Health Care Reform, <http://www.healthreform.gov> (last visited August 5, 2009).

2 Steve Lohr, How to Make Electronic Medical Records a Reality, N.Y. TIMES, March 1, 2009, at BU3.

3 See *Hearing on Inadvertent File Sharing Over Peer-to-Peer Networks: How it Endangers Citizens and Jeopardizes National Security Before the H. Comm. On Oversight and Government Reform, 111th Cong.* (2009) (opening statement of Rep. Edolphus Towns, Chairman).

4 M. Eric Johnson, *Data Hemorrhages in the Health-Care Sector*, LECTURE NOTES IN COMPUTER SCIENCE (forthcoming 2009), available at [http://mba.tuck.dartmouth.edu/digital/Research/Research Projects/JohnsonHemorrhagesFC09Proceedingd.pdf](http://mba.tuck.dartmouth.edu/digital/Research/Research%20Projects/JohnsonHemorrhagesFC09Proceedingd.pdf).

5 *Id.*

6 *Id.*

7 Sharona Hoffman & Andy Podgurski, *Finding a Cure: The Case for*

Regulation and Oversight of Electronic Health Record Systems, 22 HARV. J.L. & TECH. 103, 106 (2008).

8 STATE ALLIANCE FOR E-HEALTH, *Accelerating Progress: Using Health Information Technology and Electronic Health Information Exchange to Improve Care* (2008), available at <http://www.nga.org/Files/pdf/0809EHEALTHREPORT.PDF>.

9 See Summary of American Recovery and Reinvestment act of 2009, <http://www.recovery.gov> (last visited Aug. 5, 2009).

10 Hoffman & Podgurski, *supra* note 7, at 108-09.

11 *Id.* At 112.

12 *Id.* (quoting from BIOMEDICAL INFORMATICS: COMPUTER APPLICATIONS IN HEALTH CARE AND BIOMEDICINE 937 (Edward H. Shortliffe & James J. Cimino eds., 3d Springer 2006) (1990)).

13 Hoffman & Podgurski, *supra* note 7, at 109.

14 *Id.* Three out of four of U.S. doctors practice in small offices, which tend to see less benefit from converting to HER systems. Only about 17% of the nation's physicians are using computerized patient records. Lohr, *supra* note 2.

15 Hoffman & Podgurski, *supra* note 7, at 120-21.

16 *Id.* at 123-24.

17 Robert Pear, *Privacy Issue Complicates Push Link to Medical Data*, N.Y. TIMES, Jan. 18, 2009, at A16.

18 45 C.F.R. §§ 160.101-534 (2009).

19 See Sharona Hoffman & Andy Podgurski, *Securing the HIPAA Security Rule*, J. INTERNET L., Feb. 2007.

20 *Id.*

21 *Hearing, supra* note 3, (statements of Thomas D. Sydnor, II, Director, Center for Study of Digital Property and Robert Roback, CEO Tiversa, Inc.).

22 Sean T. McLaughlin, *Pandora's Box: Can HIPPA Still Protect Patient Privacy Under a National Health Care Information Network?*, 42 GONZ. L. REV. 29, 35-36 (2006).

23 *Hearing, supra* note 3, (statements of Thomas D. Sydnor, II, Director, Center for Study of Digital Property and Robert Roback, CEO Tiversa, Inc.).

24 For further explanation of this example see Thomas D. Sydnor, II, *Inadvertent File-Sharing Re-Invented: The Dangerous Design of LimeWire 5* (PFF July 2009), available at <http://pff.org/issuespubs/pops/2009/pop16.14-inadvertent-file-sharing-reinvented-limewire-5.pdf>.

25 McLaughlin, *supra* note 22, at 36-37.

26 *Id.*

27 *Hearing, supra* note 3.

28 *Id.*

29 Informed P2P User Act, H.R. 1319, 111th Cong. (2009).

30 Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009).

31 Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009).

32 See *Hearing on H.R. 2221, the Data Accountability and Trust Act and H.R. 1319, the Informed P2P User Act Before the H. Comm. On Energy and Commerce*, 111th Cong. (2009) (statements of David M. Sohn, Senior Policy Council, Center for Democracy and Technology, and Marc Rotenberg, Executive Director, Electronic Privacy Information Center).

33 *Id.*

34 STATE ALLIANCE FOR E-HEALTH, *supra* note8, at Preface.

35 *Id.*

36 *Id.*

37 *Id.* at 27, 30.

38 *Id.* at 31.

39 *Id.* at 29-32.

40 For a complete list of states' breach notification laws, see compilation table created by the National Conference of State Legislatures, available at <http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx> (last visited Aug. 6 2009).

41 Scott Berinato, *Data Breach Notification Laws, State by State*, CSO SECURITY AND RISK ONLINE, Feb. 12, 2008 (updated July 28, 2008), http://www.csoonline.com/article/221322/CSO_Disclosure_Series_Data_Breach_Notification_Laws_State_By_State.

ATTORNEYS GENERAL FIGHTING CYBERCRIME

MULTI-STATE

Forty-one states reached a \$9.75 million settlement with Massachusetts-based TJX Companies, Inc., resolving allegations that the massive breach of consumer information was caused because TJX ignored flaws in the configuration of its computer network and failed to take sufficient steps to protect customer information. Those failures allowed hackers to access its unsecured network and operate undetected for more than one year, leaving millions of consumers vulnerable to identity theft. The settlement requires TJX, the parent company of the T.J. Maxx and Marshalls discount clothing chains and HomeGoods stores, to upgrade and carefully test its

security systems and to regularly report the results of their security testing to the Attorneys General. It also creates a \$2.5 million national fund to investigate future data security breaches and help develop new ways to protect consumer information. States participating in the agreement are: Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Hawaii, Idaho, Illinois, Iowa, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Vermont, Washington, West Virginia, Wisconsin and the District of Columbia.

ALABAMA

Attorney General Troy King announced that former police chief Clifford Yetter Jr. pled guilty to two counts of unauthorized use of a computer to obtain criminal records of individuals through the Law Enforcement Tactical System (LETS) under false pretenses. He was sentenced to two concurrent sentences of one year, to be suspended for a term of two years probation, and fined \$2,000 plus court costs and fees. Yetter also pled guilty to nine counts of willfully obtaining or seeking to obtain criminal records through LETS under the false pretense that it was for official law enforcement purposes. He will enter a pretrial intervention program for five years. Yetter also surrendered his Alabama Peace Officers Standards and Training Commission certification and agreed not to seek future law enforcement employment. The case was prosecuted by Assistant Attorneys General Ben Baxley and James Rutter of Attorney General King's Public Corruption and White Collar Crime Division, and by former Deputy Attorney General Joseph Fitzpatrick.

DELAWARE

Acting Attorney General Richard Gebelein's Office hosted Internet safety presentations to help educate kids about ways to protect themselves online. The presentations were held at Boys & Girls Clubs in six cities in the State.

FLORIDA

Attorney General Bill McCollum's CyberCrime Unit officers arrested Joseph Bullock on charges of possession of child pornography. Unit investigators and the Plant City Police Department discovered the child pornography during a routine online undercover investigation and traced the images back to Bullard's computer. A search warrant was executed at his residence, and a computer and two external hard drives were seized. A preliminary search of the computer revealed numerous images, and Bullard admitted to possession during the investigation. The equipment will undergo additional forensic analysis for additional images. Bullard will be charged with 20 counts of possession of child pornography, a third-degree felony which will be enhanced to a second-degree felony. The Plant City Police Department, Florida Department of Law Enforcement, Hillsborough County Sheriff's Office and the U.S. Immigration and Customs Enforcement participated in the arrest.

HAWAII

Attorney General Mark Bennett announced that his office now provides a free service which allows the public to subscribe to receive email alerts when sex offender registration information in their geographic area is added or updated. Users of the service will receive alerts regarding registered offenders who live or work within a selected zip code or within up to a three-mile radius of a specified address.

ILLINOIS

Attorney General Lisa Madigan announced that Jimmy Dill was arrested and charged with five counts of Possession of Child Pornography, a Class 3 felony. Investigators from Attorney General Madigan's High Tech Crimes Bureau assisted the Huntley Police Department in executing a search warrant at Dill's residence resulting in the seizure of computers and hard drives believed to contain child pornography. The Bureau had earlier identified that Dill was offering child pornography over the Internet.

INDIANA

Attorney General Greg Zoeller's Office held a series of Continuing Legal Education (CLE) classes on Identity Theft. The sessions were designed to train attorneys on the legal ramifications of dealing with identity theft.

LOUISIANA

Attorney General James "Buddy" Caldwell's High Tech Crime Unit (HTCU) conducted an Internet training for 11 Baton Rouge area law enforcement agencies. Mike Johnson, HTCU Director, and Ashley Borel led the session, which trained 25 officers. The training was also an undercover sting operation which resulted in two arrests. Hugh Passerini of North Carolina and Jermei Reifer were each charged with one count of computer-aided solicitation of a juvenile and one count of indecent behavior with a juvenile.

MASSACHUSETTS

Attorney General Martha Coakley joined legislators and district attorneys in sponsoring An Act to Combat Economic Crime. Among the areas the bill updates is the state wire interception statute, including adding a definition for "electronic communi-

cation” and designating new crimes eligible for the use of a lawful interception. The bill would also extend the amount of time that a lawful interception can remain open from 15 to 30 days to account for the breadth and complexities of criminal investigations. It also allows lawful, court-approved one-party consent monitoring and recording of conversations of certain crimes.

MICHIGAN

Attorney General Mike Cox joined six state legislators to announce Internet child protection legislation consisting of three bills. The bills would ban registered Internet child sex predators from social networking web sites, with a felony penalty for violations; mandate that Internet child sex predators be placed on the Michigan Sex Offender Registry; and increase sentencing for possession and distribution of child pornography.

MISSISSIPPI

Attorney General Jim Hood announced that Branden Henley was arrested and charged with possession of child pornography. Attorney General Hood’s Internet Crimes Against Children (ICAC) Unit led the investigation and was assisted in the execution of a search warrant by the Lamar County Sheriff’s Office and the Hattiesburg FBI. Possession of child pornography is a felony offense with a penalty of five to 40 years in the state penitentiary and, upon conviction, is a lifetime registerable sex offense.

NEW JERSEY

Attorney General Anne Milgram’s Division of Criminal Justice obtained a superseding indictment that charges former state assemblyman Neil Cohen with an additional count of fourth-degree possession of child pornography. The charge is in connection with multiple images of child pornography he alleg-

edly possessed on a computer seized from his law office. The indictment repeats all four counts of the prior indictment, charging Cohen with official misconduct (2nd degree), reproduction of child pornography (2nd degree), distribution of child pornography (2nd degree) and possession of child pornography (4th degree). Second-degree crimes carry a maximum sentence of 10 years in state prison and a \$150,000 fine, while fourth-degree crimes carry a sentence of up to 18 months in prison and a \$10,000 fine. The official misconduct charge carries a mandatory minimum sentence of five years without parole. The charges are the result of an investigation by the Division’s Corruption Bureau and the New Jersey State Police. Deputy Attorney General and Bureau chief Anthony Picione and Deputy Attorney General Robert Rowbotham II presented the case to the grand jury.

NEW MEXICO

Attorney General Gary King’s Internet Crimes Against Children (ICAC) unit special agents executed a search warrant at Norman Elquest’s home and subsequently took him into custody on 25 counts of Sexual Exploitation of Children. During an earlier undercover investigation, Unit Special Agent Lois Kinch discovered evidence leading to an investigation of Elquest. The search of his home revealed illicit images of children in sexual acts on his computer.

NEW YORK

Attorney General Andrew Cuomo announced a settlement with cosmetic surgery company Lifestyle Lift over the publishing of fake consumer reviews on the Internet. Lifestyle Lift published positive reviews and comments about the company to trick web-browsing consumers into believing that satisfied customers were posting their own stories. In reality, the company was engaging in “astroturfing,”

a practice in which employees pose as independent consumers to post positive reviews and commentary to web sites and Internet message boards about their own company. Internal e-mails discovered in the investigation show that Lifestyle Lift gave employees specific instructions to engage in this illegal activity, which constitutes deceptive commercial practices, false advertising and fraudulent and illegal conduct under New York and federal consumer protection law. Under the settlement, Lifestyle Lift will stop publishing anonymous positive reviews about the company, and its employees will no longer pose as consumers. The company will not promote its services on the Internet without clearly and conspicuously disclosing that they are responsible for the content. They will also pay \$300,000 in penalties and costs to the State. The investigation was handled by Chief of the Internet Bureau Justin Brookman and investigator Vanessa Ip, under the direction of Deputy Attorney General for Economic Justice Michael Berlin.

NORTH CAROLINA

Attorney General Roy Cooper announced that Internet sales companies iMergent, Inc. and StoreOnline, Inc., both of which had entered into an agreement over their misleading sales practices, have been ordered to comply with the agreement and pay the promised refunds to state consumers. The contempt order stated that the two Internet companies, which claim to help people build web sites and create online stores, failed to comply with the consent judgment because they did not provide refunds to the 221 state consumers who filed applications with Attorney General Cooper's Consumer Protection Division.

OKLAHOMA

Attorney General Drew Edmondson announced that Stephen Lewis pleaded guilty to seven counts of unfair or deceptive trade practices related to his online business sales. Lewis sold trailers, fencing panels, metal storage sheds and ceramic insulation materials through numerous companies including Cowboy and Company, USA Cowboy, Arieyl Trailer and Pioneer Builders Supply and Services. According to the state, Lewis placed the items for sale in online auctions and in online advertisements. The state alleges Lewis accepted payment for, but failed to deliver, many items. An investigation by Attorney General Edmondson's Consumer Protection Unit found he scammed consumers from 13 states, including Oklahoma. Lewis was ordered to pay almost \$57,000 in restitution and agreed to stop doing online business in the State. He also received a five-year deferred sentence on each count to run concurrently.

OREGON

Attorney General John Kroger joined Jefferson County District Attorney Steven Leriche to announce the sentencing of Richard Pickett, a former county building and maintenance employee, to more than 38 years in prison for sexually abusing a girl for eight years and possessing child pornography. Pickett was convicted of five counts of first-degree sodomy, 10 counts of first-degree sexual abuse, nine counts of first-degree encouraging child sexual abuse, nine counts of second-degree encouraging child sexual abuse and two counts of using a child in a display of sexually explicit conduct. Pickett was arrested following an online investigation by Attorney General Kroger's Internet Crimes Against Children (ICAC) unit. A child pornography tip led to additional evidence that Pickett had also sexually abused a child.

PENNSYLVANIA

Attorney General Tom Corbett's Child Predator Unit agents arrested Orlando Inoa, a graduate student from Ohio, and Michael York, a photographer, who are accused of using the Internet to sexually proposition what they believed were 13-year-old girls and traveling to have sex with them. The "girls" were actually Unit undercover agents who were using the profiles of children. Inoa is charged with one count of attempted unlawful contact with a minor (related to involuntary deviate sexual intercourse), a first-degree felony punishable by up to 20 years in prison and a \$25,000 fine. He is also charged with four counts of unlawful contact with a minor (related to explicit sexual material), two counts of sexual abuse of children (related to child pornography) and two counts of criminal use of a computer, all third-degree felonies punishable by up to seven years in prison and \$15,000 fines. The Cranberry Township Police Department assisted in the investigation. Inoa will be prosecuted by Deputy Attorney General William Caye II of the Unit. York is charged with one count of attempted unlawful contact with a minor (related to involuntary deviate sexual intercourse), one count of unlawful contact with a minor (related to statutory sexual assault), a second-degree felony punishable by up to 10 years in prison and a \$25,000 fine and one count of criminal use of a computer. The Lower Providence Township Police Department assisted with the investigation. York will be prosecuted by Deputy Attorney General Michael Sprow of the Unit.

SOUTH CAROLINA

Attorney General Henry McMaster's Internet Crimes Against Children Task Force arrested Tyrone Horton in an undercover sting on one count of Criminal Solicitation of a Minor, a felony offense punishable by up to 10 years in prison. Arrest warrants allege that Horton solicited sex on the Internet from an individual he believed to be a 13-year-old girl, but

actually was an undercover investigator in Attorney General McMaster's Office. A search warrant was executed on Horton's residence, and a computer and cell phone were seized. The Kershaw County Sheriff's Office, a Task Force member, assisted with the case. Horton will be prosecuted by Attorney General McMaster's Office.

TEXAS

Attorney General Greg Abbott joined with the Texas Cable Association and the Internet Keep Safe Coalition to launch a video that teaches children and parents about online safety. Cable service providers will make the video available to their subscribers for the next four months through on-demand cable services across the State. The video describes risks associated with the Internet and teaches parents how to protect their children online.

VERMONT

Attorney General Bill Sorrell settled claims that New York-based Habana Cigar Shop sold tobacco products in Vermont via its web site in violation of state law. In documents approved by a court, Habana agreed to pay \$2,500 for the sale of one pound of roll your own tobacco, which cost \$25. Vermont's ban on Internet sales and delivery of tobacco products became effective in July 2008.

WASHINGTON

Attorney General Rob McKenna entered into an agreement with StoresOnline which requires StoresOnline and its parent company, Imergent, Inc. of Utah, to pay up to \$75,000 in restitution to customers in the state, as well as \$25,000 in civil penalties and \$75,000 in attorney's fees and costs. The state's complaint accused the businesses of violating the state Consumer Protection Act by misrepresenting services and omitting facts during sales

presentations, using high pressure sales tactics and having an unfair refund policy. The company's invitations promised a free meal and gift for attending a 90-minute presentation on how to make money on the Internet. Consumers who bought an "Express license" for \$50 after the presentation were invited to a second workshop promoted as a free training but was actually a sales pitch for more expensive services, such as purchasing six web sites for \$6,000. The agreement also extends refund rights to ensure that all consumers have at least a full weekend to examine the product, with seniors getting 15 days to rescind.

WISCONSIN

Attorney General J.B. Van Hollen announced that Alexander Combs, a volunteer youth counselor at a summer camp, was arrested as part of an ongoing child exploitation investigation originating in another state. According to the criminal complaint, child pornography was recovered during a preview of the hard drive of Combs' computer. The Madison Police Department and the Dane County Sheriff's Office, both members of Attorney General Van Hollen's Internet Crimes Against Children (ICAC) Task Force, participated in the operation in conjunction with the Minnesota ICAC Task Force and the Mount Pleasant, South Carolina Police Department. Combs is charged with one count of Possession of Child Pornography.

IN THE COURTS

FIRST AMENDMENT: BLOG RETRIBUTION

Richerson v. Beckon, 2009 U.S. App. LEXIS 12870 (9th Cir. June 16, 2009). Providing a setback to blogger's First Amendment rights, the 9th

Circuit Court of Appeals ruled that a teacher's blog, which attacked her co-workers, the union and the school district, was not protected speech, and therefore she was not unlawfully demoted as a result. Washington state teacher Tara Richerson was transferred out of her coaching position after school officials discovered her blog. Richerson came under fire for blog entries such as the one in which she allegedly attacked a teacher and union negotiator, who complained to school officials. Richerson filed suit, arguing that her blog was protected free speech, that it was a matter of "public concern," and that she was unlawfully demoted. The U.S. District Court for the Western District of Washington concluded that Richerson's blog was instead "racist, sexist and bordered on vulgar." On appeal, the 9th District Court of Appeals affirmed, finding that the blog was disruptive, eroded work relationships and interfered with her job performance, justifying her transfer.

Ed. Note: On a related, and closer to home, note, the California Bar Journal reports that Frank Wilson of San Diego was suspended from practice for 18 months in part over comments he made on his blog about a trial. The moral: be careful what you blogeth.

WIRE FRAUD: BOGUS CHARITABLE WEBSITE

U.S. v. Stephens, 2009 U.S. App. LEXIS 12662 (5th Cir. June 10, 2009). The 5th Circuit Court of Appeals affirmed the convictions of Bartholomew and Steven Stephens on charges of conspiracy to commit and aiding and abetting wire fraud and aggravated identity theft. The Stephens brothers created a bogus charitable website to collect fraudulent Hurricane Katrina relief donations. The evidence showed that the online donations had been deposited in their personal accounts and that those accounts had been created in other names and identification numbers and were used to commit wire

fraud. It also showed that the brothers exchanged emails about the “fake socials,” and they carefully tracked the names associated with each account and the money in each. They were convicted in the U.S. District Court for the Southern District of Texas and appealed, arguing insufficiency of evidence and prosecutorial misconduct. As to the insufficiency of evidence, the brothers argued that the prosecution did not subpoena any witness, but that claim was quickly put away by noting that neither did the defense. The brothers also argued that the prosecution’s statement in opening argument that the brothers took advantage of the generosity of people who wanted to help was unfairly prejudicial, but the court found otherwise and affirmed.

GPS TRACKING: STATE RIGHT AGAINST UNREASONABLE SEARCH

People v. Weaver, 2009 NY Slip Op 03762 (NY May 12, 2009). A divided New York Court of Appeals reversed the conviction of Scott Weaver, finding that police needed a warrant to attach a GPS device to his car. Very early in the morning, a state police investigator placed a GPS tracking device inside the bumper of burglary suspect Scott Weaver’s street-parked van. The device monitored the position of the van continuously, although the same investigator had to replace its battery during another nocturnal visit. All of the surveillance was conducted without a warrant. The GPS reading was later admitted into evidence at Weaver’s burglary trial. Weaver was found guilty after a jury trial, and the Appellate Division, Third Department, upheld his conviction, 3-1. Weaver appealed, claiming his constitutional rights under N.Y. Const. art. I, § 12 to be free of unreasonable searches and seizures were violated by the warrantless placement and use of the GPS device. In an internally controversial 4-3 decision, the New York Court of Appeals found that the privacy expectation that Weaver had in his vehicle was adequate to support his claim of a constitu-

tional violation. It found the search to be illegal because it was executed without a warrant and without justification under any exception to the warrant requirement. Weaver’s conviction was reversed and a new trial ordered.

Ed. Note to our readers: The Wisconsin Court of Appeals reached the opposite conclusion in State v. Sveum, 2009 Wisc. App. LEXIS 343 (May 7, 2009), as reported in the May-June 2009 issue of this e-newsletter.

E-MAIL INTERCEPTION: AUTO-FORWARDING

U.S. v. Szymuszkiewicz, 2009 U.S. Dist. LEXIS 60755 (E.D. Wis. June 30, 2009). The U.S. District Court for the Eastern District of Wisconsin denied defendant’s motion for acquittal, leaving in place his jury conviction. David Szymuszkiewicz, an IRS revenue officer, created a “rule” on his supervisor’s computer that auto-forwarded all of her e-mail to him. His “rule” was discovered during a routine training session, and Szymuszkiewicz was charged with three counts of violating § 2511(1)(a), which makes it a federal crime to intercept the contents of electronic communications. According to the statute, the term “intercept” means to acquire the contents of any electronic communication through the use of any electronic, mechanical or other device. A jury convicted him, and Szymuszkiewicz moved for an acquittal. He argued that the government had failed to prove beyond a reasonable doubt that he used a “device” to intercept the e-mails. However, he could not cite any cases holding that using two computers to intercept communications does not satisfy the statute’s requirements, so the court found the government had carried its burden.

FIRST AMENDMENT: IDENTIFY THEFT BY HACKING

State v. Baron, 2009 WI 58 (June 23, 2009). The Wisconsin Supreme Court upheld a lower court ruling finding that stealing another's identity for the purpose of harming that person's reputation is not constitutionally protected speech, even if the victim is a public official. Christopher Baron, an EMT technician, hacked into the work computer of his boss and found several emails which suggested that his boss was using a government-owned apartment to conduct an extramarital affair. Baron forwarded those emails to 10 other people in a manner suggesting that they came from the boss himself. Wisconsin § 943.201 (2) © prohibits the intentional use and distribution of any personal identifying information of an individual while posing as that individual to harm the reputation of the individual. Baron was charged with six criminal counts, including a charge of identity theft alleging that Baron used his boss' identity without his consent and with the intent to harm his reputation. Baron moved to dismiss that charge, arguing that he had a First Amendment right to disseminate truthful information about a public official, even if it did harm that person's reputation. The trial court agreed, and dismissed the charge. On appeal, the Court of Appeals reversed, and the Supreme Court agreed to review the case. The court held that while the statute, as applied to Baron's conduct, constituted a content-based regulation of his speech, the statute was constitutional because it was narrowly tailored to promote the State's compelling interest in preventing identity theft. The statute did not chill Baron's right to free speech because he could have disseminated the information about his boss without pretending to be his boss.

Ed. Note: The State was represented at the Supreme Court by Assistant Attorney General Jeffrey Kassel of the Wisconsin Department of Justice.

ONLINE CHILD ENTICEMENT: USE OF INTERMEDIARY

U.S. v. Nestor, 2009 U.S. App. LEXIS 16220 (3rd Cir. July 23, 2009). The Third District Court of Appeal affirmed a lower court judgment that a defendant who solicited sex online through an intermediary was guilty of attempting to entice a child to engage in sexual activity. Brian Nestor posted an advertisement seeking "family fun" on a website. A police officer suspected that he was really looking for a parent willing to make a child available for sex, so he responded to the ad using an alias. Through emails and phone conversations, Nestor proposed to engage in sexual activity with the alias and the alias' underage stepson and arranged a meeting at Nestor's home, where he was arrested. Nestor was convicted under 18 U.S.C. S. § 2422(b) and moved for a judgment of acquittal. The U.S. District Court for the Western District of Pennsylvania denied the motion and sentenced him. Nestor appealed, contending that he never spoke to a child or anyone whom he believed was a child, so he could not be convicted under the statute. The 3rd Circuit noted that Nestor demonstrated his intent to violate the statute in his emails and phone conversations. Although Nestor never communicated directly with a child, he was guilty because he took substantial steps calculated to put him in direct contact with a child so that he could carry out his intent to entice the child into sexual activity.

INTERNET ENTICEMENT STATUTE: CONSTITUTIONALITY

State of Utah v. Gallegos, 2009 UT 42 (July 21, 2009). In a case of first impression, the Utah Supreme Court held that Utah's Internet Enticement Statute is not unconstitutionally vague and affirmed the lower court's decision. James Gallegos solicited an undercover Internet Crimes Against Children (ICAC) agent over the Internet and was arrested af-

ter he arrived at the pre-arranged meeting place. He was charged with two felony counts of enticing a minor over the Internet in violation of Utah Code section § 76-4-401 (2008). At trial, Gallegos moved to dismiss on the grounds that the statute was unconstitutionally vague, which the trial court denied. On appeal, Gallegos again raised the constitutionality argument, as well as other arguments that will not be addressed here. The court noted that “A statute is impermissibly vague if it either (a) ‘fails to provide people of ordinary intelligence a reasonable opportunity to understand what conduct it prohibits’ or (b) ‘authorizes or even encourages arbitrary or discriminatory enforcement.’” *Hill v. Colorado*, 530 U.S. 703, 732 (2000). As to the first prong, Gallegos argued that a person of ordinary intelligence cannot know which act is sufficient for the offense – when the person meets the minor, takes any step to meet the minor or the “chat” by itself. The court easily dismissed that argument, finding that the likelihood that anyone would not understand the common words of the statute was quite remote. As to the second prong, Gallegos argued that the statute could be arbitrarily applied since many other individuals also contacted the ICAC agent but were not arrested. The court disagreed, finding that the decision of whom to arrest depended on resource allocation and the difficulty of proving intent. The court concluded that any variation in enforcement of the statute may occur because it is simply easier to prosecute individuals who arrange a meeting with a minor, not because the statute is impermissibly vague.

Ed. Note: Jeffrey Gray and Paul Amann, Assistant Attorneys General in the Office of the Attorney General of Utah, represented the State.

SUPREME COURT UPDATE

On June 22, the Supreme Court granted certiorari in *United States v. Comstock*, No. 08-1224, to determine whether Congress’ newly enacted sexually violent predator statute 18 U.S.C. § 4248 (2006), a part of the Adam Walsh Child Protection and Safety Act, exceeds Congress’ enumerated powers. The statute allows the federal government to place “sexually dangerous” persons in indefinite civil commitment for the purpose of treatment. In 2007, the U.S. District Court for the Eastern District of North Carolina found the statute unconstitutional. The Fourth Circuit Court of Appeals upheld the district court’s ruling, finding Congress exceeded its constitutional authority by enacting this portion of the Act. The government argued that Congress properly passed the legislation under the Necessary and Proper Clause and the Commerce Clause of the Constitution. The court rejected the government’s Necessary and Proper Clause assertion because the clause simply allows Congress to enact laws that are needed for the execution of enumerated constitutional powers. In examining the Commerce Clause argument, the court relied on the Supreme Court’s decisions in *U.S. v. Lopez*, 514 U.S. 549 (1995) and *U.S. v. Morrison*, 529 U.S. 598 (2000), which limited Congress’ Commerce Clause power to three specific areas: (1) the channels of interstate commerce, (2) instrumentalities of or persons and things in interstate commerce, and (3) activities that “substantially affect” interstate commerce. The court found that enactment of Section 4248 did not fall within any of these areas and therefore did “not constitute a valid exercise by Congress of its Commerce Clause power.”

The Supreme Court denied review of *Cable News Network v. CSC Holdings Inc.*, No. 08-448, on June 29. The U.S. District Court for the Southern District of New York held that Cablevision System Corp.’s

proposed remote-storage DVR violated copyright laws by storing data in data buffers, copying programs onto server hard disks, and transmitting the stored data to its customers as a response to a “playback” request. On appeal, the Second Circuit Court of Appeals reversed the district court’s judgment; the court held that Cablevision’s technology did not create a fixed copy of the material being stored; the act of copying was actually performed by Cablevision’s customers, and the playbacks were not distributed to the public. Based on this reasoning, the Second Circuit found that Cablevision’s technology did not violate the Copyright Act.

United States v. Comstock, 08-1224. At issue is whether Congress has the authority to provide for court-ordered civil commitment of mentally ill, “sexually-dangerous” persons in federal custody who have either been found incompetent to stand trial or have been convicted but are nearing the end of their sentences. In 2006, Congress enacted 18 U.S.C. §4248 as part of the Adam Walsh Child Protection and Safety Act. The statute authorizes the federal government to seek civil commitment of persons in the custody of the Bureau of Prisons who are “sexually dangerous,” *i.e.*, who suffer from a mental illness that results in “serious difficulty in refraining from sexually violent conduct or child molestation if released.” The standards for commitment were modeled after the standards approved by the Court in *Kansas v. Hendricks*, 521 U.S. 346 (1997), and *Kansas v. Crane*, 534 U.S. 407 (2002): they allow the district court to order a psychiatric examination; require the Government to prove at a hearing by clear and convincing evidence that the inmate is a “sexually dangerous person”; provide counsel to the inmate; and allow the inmate to testify, present evidence, and subpoena, confront, and cross-examine witnesses. In this case, a number of federal prisoners who were due to be released, and one who was found incompetent to stand trial, offered a facial challenge to the constitutionality of

§4248, moving to dismiss civil commitment proceedings initiated against them by the Government. The district court granted the motions to dismiss, holding §4248 unconstitutional. The Fourth Circuit affirmed, holding that §4248 is unconstitutional because Congress lacks the authority “to confine a person solely because of asserted ‘sexual dangerousness’ when the Government need not allege (let alone prove) that this ‘dangerousness’ violates any federal law.” 551 F.3d 274.

The United States argues in its petition that it possesses a different relationship to persons in federal custody than to members of the general public, and that the ability to pursue civil commitment of persons in federal custody is “a rational incident” to its undisputed powers to enact criminal laws and imprison those who break them. It contends that it has a legitimate interest in protecting the public from persons already lawfully in federal custody, and that that interest is unaffected by whether the danger comes from conduct that constitutes a violation of federal law. The United States also contends that the statute involves only minimal intrusion on states’ traditional sphere, noting the frequency of “supervised release” to show that former federal prisoners are rarely turned over to the primary authority of the states on their release. Moreover, §4248 provides for continued federal custody of committed persons only when the states decline to take them. Respondents argue that §4248 cannot be justified as a “rational incident” to Congress’ authority to enact criminal laws because it applies broadly to all persons in federal custody, not just those who have violated federal criminal law. Nor can §4248 be justified as a “rational incident” to the federal government’s custodial responsibility for persons who violate its criminal laws because such custodial authority “necessarily ends” when the inmate is no longer lawfully in the custody of the Bureau of Prisons, for example, at the end of his sentence. Relying on the Court’s recent Commerce

Clause cases — *United States v. Lopez*, 514 U.S. 549 (1995), and *United States v. Morrison*, 529 U.S. 598 (2000) — respondents argue that §4248 is an attempt to regulate an activity that does not substantially affect interstate commerce and therefore exceeds Congress' authority under the Commerce Clause.

SUPREME COURT WILL HEAR MAJOR COPYRIGHT CASE

On February 23rd, 2009, the U.S. Supreme Court granted certiorari to hear an appeal by a group of publishers seeking to reinstall a settlement with freelance writers, effectively reversing the Second Circuit's decision that federal courts lacked jurisdiction in the instant case. Initially, the writers had sued publishers and electronic database services, arguing that their contract did not allow publishers a license for others to electronically produce their work. The settlement was reached in 2005 and was approved by a federal judge. This settlement was subsequently thrown out by a U.S. Appeals Court panel because the panel reasoned that the federal judge lacked jurisdiction over infringement claims arising from unregistered copyrights. In accepting review, the Supreme Court stated the only question it would consider was whether the law restricted federal court jurisdiction over copyright infringement actions. Arguments in the case will take place during the court's upcoming term in October. The brief for the petitioners can be found at http://www.abanet.org/publiced/preview/briefs/pdfs/07-08/08-103_Petitioner.pdf

LEGISLATIVE NEWS

Broadband Services

On July 22, **New Hampshire** Governor John Lynch signed SB 159 into law, a bill intended to bring broadband and advanced telecommunications services to the state, especially in underserved areas. The measure establishes a director of broadband technology planning and development, to be paid for with federal stimulus funds. The main duties of the director's position will be to work with the Telecommunications Planning and Development Advisory Committee and the Department of Resources and Economic Development to grow technology services by utilizing federal grants and public-private enterprises.

On July 14, Senator Kay Bailey Hutchinson (R-TX) introduced S. 1447, a bill designed to expand broadband coverage in the U.S., in part by amending the tax code to provide tax credits for investments in broadband infrastructure. It was referred to the Finance Committee.

Sexting

A package of bills in response to sexting were introduced in the **New Jersey** legislature. A-4069 and its comparable Senate bill, S-2926, propose an alternative to criminal prosecution by creating a diversionary program under which minors who are charged with the creation, distribution or exhibition of nude photos can avoid prosecution by completing a course focusing on the consequences of such acts. The bills also call for the Attorney General's office to develop a sexting curriculum in cooperation with the judiciary. The course would focus on legal consequences of transmitting explicit photos as well as nonlegal consequences, such as the effect on relationships and the loss of job opportunities. Also

covered would be the long-term consequences of sharing of sexually explicit materials and the link between bullying and the sharing of such materials. Another bill, A-4068, and its Senate counterpart, S-2923, would require schools to annually disseminate, by whatever means they deem appropriate, information to students in grades six through 12 on the hazards of electronic dissemination of sexually explicit images. A third bill, A-4070, and its Senate version, S-2925, would require stores selling cell phones or phone contracts to provide brochures about sexting to purchasers.

Internet Safety

On July 15, Representative Debbie Wasserman Schultz (D-FL) introduced HR 3222, a bill that would provide grants to develop an Internet safety program that encourages safe and responsible Internet use. It would require the use of such programs to educate children, parents and communities on how to prevent or respond to problems. The bill was referred to the Committee on Energy and Commerce.

Texting While Driving

On July 29, Senator Charles Schumer (D-NY) introduced S. 1536, a bill that would reduce the amount of federal highway funding available to states that do not enact a law banning the writing, sending or reading of text messages while operating a motor vehicle. The measure provides that states would have two years to enact such legislation or lose 25 percent of their highway funding each year. The bill was referred to the Committee on Environment and Public Works.

Caller ID Spoofing

On August 5, the Senate Commerce, Science and Transportation Committee approved S. 30, a bill sponsored by Senator Bill Nelson (D-FL) that would

make it unlawful to cause any caller Identification service to transmit inaccurate or misleading caller ID information. The bill provides for civil and criminal penalties and authorizes enforcement by states. The companion bill in the House is HR 1258, sponsored by Representative Eliot Engel (D-NY).

NEWS YOU CAN USE

SURVEY: CONSUMERS STILL DOWNLOADING ILLEGALLY

Eight percent of consumers in Great Britain, France, Germany and the United States readily admit to downloading video illegally from the Internet, according to a survey by Futuresource Consulting, a research and consulting firm based in Great Britain. It found that two-thirds of those surveyed in Great Britain often or sometimes watched TV, movies and video on their PC or laptop computer, with U.S. consumers close behind, but of those, 15 percent did so illegally. The survey, conducted online of more than 2,500 people, found that 90 percent of those who watched video content online had never paid to watch news or recently-missed shows. Over one-half had never paid to watch new movies, although most said they would or might be willing to pay in the future. Less than one percent said that an advertising reel placed before, during or after an old movie or TV show spoiled their online viewing, with 30 percent saying it had no impact and nearly one-half saying it put them off.

MICHIGAN COMES DOWN ON GADGET-HAPPY JURORS

The Michigan Supreme Court has banned all electronic communications by jurors during trial, including tweets on Twitter, text messages and Google searches. The ruling, which becomes effective on September 1, will require Michigan judges for the

first time to instruct jurors not to use any hand-held devices, such as iPhones or Blackberrys, while in the jury box or during deliberations. The ruling comes in response to prosecutors' complaints that jurors were getting distracted by their cell phones, smart-phones and PDAs and, in some cases, texting during trial or researching their own information about a case and potentially tainting the jury process. According to the National Center for State Courts, a recent questionnaire sent to court administrators across the country found that many other courts are addressing the problem of potential juror misconduct through hand-held devices.

“SCREENSAVERS” IS RISKIEST SEARCH TERM

McAfee, a network security provider, issued a report highlighting some of the Internet's most dangerous search terms. First on that list was the term “screensavers” with a maximum risk of 59.1 percent. Additionally, search terms that include lyric keywords or that use the word “free” have the next highest risk of exposing users to malware or fraudulent web sites. The safest were those regarding health-related terms or terms about the recent economic crisis. The report can be accessed at http://us.mcafee.com/en-us/local/docs/most_dangerous_searchterm_us.pdf.

CRITERIA FOR RURAL BROADBAND FUNDING ANOUNCED

The administration announced the criteria to be used to award billions of dollars in stimulus money to develop the infrastructure for delivering broadband Internet access to underserved areas or areas without access. The U.S. Departments of Commerce and Agriculture will consider projects that provide wired or wireless access starting at low-end DSL speeds, but will give priority to those promising higher speeds. A geographical area will be consid-

ered “underserved” by broadband, and thus eligible for grants, if one-half or fewer of the households can get wired broadband today, among other criteria. Applicants began applying on July 14, with the first round of funding to be awarded in September. Besides providing funds to create the infrastructure, funding can also be awarded for training people to use the Internet. All money must be awarded by September 2010. As yet, none of the largest U.S. broadband providers, including Verizon Communications, AT&T Corp. and Comcast, have expressed interest in applying for the funds, based upon concerns about the bureaucratic “red tape” and possible restrictions that might be applied to lines built with taxpayer dollars.

FINALLY! A ROYALTY AGREEMENT FOR MUSIC STREAMING

After a two-year battle, record labels and online radio stations agreed on new royalty rates to cover music streaming. In 2007, a federal royalty board ruled that all webcasters had to pay a fee, which was set to increase to 19 cents per song each time they streamed a song for a listener. Webcasters claimed the fees were so high they were being forced out of business. The new agreement treats sites differently depending on their size and business model. It applies to companies that make most of their money from streaming music, so webcasters such as CBS Radio, which runs online music services for AOL and Yahoo, are not covered. The agreement covers the period from 2006 through 2015 for big sites and 2014 for small sites. Webcasters with significant advertising revenue, such as Pandora or Slacker, will pay the greater of 25 percent of revenue or a fee each time a listener hears a song, starting at eight cents for songs streamed in 2006 and increasing to 14 cents in 2015. Small sites with less than \$1.25 million in revenue, such as AccuRadio, Digitally Imported or RadiolO, will pay 12 to 14 percent of it in royalties. All stations will

be required to pay an annual minimum fee of \$25,000, which they can apply to royalty payments. Webcasters also agreed to give more detailed information about the songs they play and how many people listen to them to SoundExchange, a nonprofit organization that collects and distributes digital royalties on behalf of artists and labels.

CALIFORNIA DATA BREACHES RISE AFTER TOUGH LAW ENACTED

Health care organizations in California filed over 800 reports of breaches this year after a new law became effective, according to a report in the August issue of the Journal of the American Health Information Management Association. Senate Bill 541 and its counterpart, Assembly Bill 211, which passed last year, require health care organizations to begin reporting any unauthorized access to records to the California Department of Public Health (CDPH). According to the report, CDPH received 823 breach incident reports from January 1 to May 31. Of those cases, 122 have received a full investigation, with 116 confirmed as breaches. There were 232 cases that had ongoing investigations, and 469 reported breaches were pending investigation. One factor cited for the unexpected volume of breach reports is that the new law changed the definition of a breach to include any inappropriate data access. The article can be accessed at <http://journal.ahima.org>.

TOOLS YOU CAN USE

Advanced Radio Technology for Law Enforcement

“Smart Radio for Police,” a National Institute of Justice publication, describes two related developments in radio technology software-defined radio

and cognitive radio. It can be accessed at <http://www.ncjrs.gov/pdffiles1/nij/224253.pdf>.

Protecting Mobile Computing Devices

The National Association of State Chief Information Officers released an issue brief, “Security on the Edge – Protecting Mobile Computing Devices,” highlights the risks associated with the uncontrolled use of mobile devices and targets the standards and procedures and controls that allow states to better secure them. It can be accessed at <http://www.nascio.org/publications>.

Bullying

“Bullying in Schools,” a guide published by the U.S. Department of Justice’s Office of Community-Oriented Policing Services (COPS), provides information about the causes and extent of bullying in schools and includes recommendations for developing practices and policies that promote student safety.

FREE TRAINING TO AG OFFICES

TECHNOLOGY-BASED CRIMES AGAINST CHILDREN: CUTTING EDGE ISSUES

October 13–15, 2009

University of Mississippi School of Law

University, Mississippi

Registration Deadline: September 21, 2009

(application on back pg 22)

This course will address the more complex issues that arise when addressing technology-based crimes against children. It will cover such topics as approaches to sexting, dealing with defense experts and Fourth Amendment issues related to warrants in child pornography cases. The course will also address the creative use of statutes to prosecute child offenders, such as sex offender failure to register prosecutions and the use of the Adam Walsh Act anti-grooming statute. Attendees will receive CLE credit, and there is no registration fee for Attorney General Office attendees. Travel scholarships are available.

National Association of Attorneys General/

National Center for Justice and the Rule of Law

JOB OPENING: SENIOR COUNSEL / VISITING PROFESSOR

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

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

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

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

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

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

CYBERCRIME NEWSLETTER ■ JULY-AUGUST 2009

**NATIONAL ASSOCIATION OF ATTORNEYS GENERAL
TECHNOLOGY-BASED CRIMES AGAINST CHILDREN: CUTTING EDGE ISSUES**

October 13-15, 2009

University, MS 38677

NOMINATION FORM - RETURN BY SEPTEMBER 18, 2009

****PLEASE NOTE: THIS FORM IS NOT AN AUTOMATIC APPROVAL TO ATTEND THE TRAINING.
APPROVAL NOTICE WILL BE SENT UNDER SEPARATE COVER****

MEETING ID NO. 0910_TBCAC

Please use one form per registrant/nominee. Complete all sections.

Please return form to: National Association of Attorneys General, Attn: Marland Holloway, Cyberspace Law Project Assistant, 2030 M Street, N.W., 8th Floor, Washington, DC 20036 or **Fax to (202) 785-0287.**

Name (as it should appear on badge):

Full Mailing Address:

Title: _____

Phone Number: _____

Fax Number: _____

E-mail: _____

Attorney General Office: _____

Travel By (Check one): Air _____ Rail _____ Car _____

State Bar registration number(s)

State _____ Number _____

(For CLE credit)

State _____ Number _____

Dietary Restrictions? If so, describe: _____

Special Requests If you require special services or auxiliary aids to assist you while attending the meeting and events during the Clean Water Act Training, such as sign-language interpreters, note-takers, large print materials or Braille materials, please contact Marland Holloway, Cyberspace Law Project Assistant, at 202-326-6262 or by email at mholloway@naag.org. NAAG will make suitable arrangements.