ATTORNEYS GENERAL TO TRAIN INTERNATIONAL PROSECUTORS THROUGH U.S. DEPARTMENT OF STATE

On February 24, the National Association of Attorneys General (NAAG) and the U.S. Department of State, Bureau of International Narcotics and Law Enforcement Affairs (INL), signed an agreement establishing an international partnership to train foreign criminal justice personnel. The Memorandum of Understanding means INL will request that NAAG members or the National Attorneys General Research and Training Institute (NAGTRI) conduct trainings, serve as mentors, participate in assessments or speak at conferences. The Attorneys General of Rhode Island, Delaware and New Mexico also recently signed similar INL agreements.

ATTORNEYS GENERAL FIGHTING CYBERCRIME

MULTI-STATE

Sixteen Attorneys General sent a letter to both chambers of Congress urging them to consider the policy implications of a recent reversal of the U.S. Department of Justice interpretation of the federal Wire Act as it pertains to Internet gambling. The letter notes that although the federal government has consistently interpreted the Wire Act to prohibit all
forms of gambling involving interstate wire transmissions, the U.S. Department of Justice’s Office of Legal Counsel issued a legal opinion stating the Act only bans sports betting and does not apply to Internet gambling. The letter was authored by Missouri, Nebraska and South Carolina and additionally signed by Arizona, Florida, Guam, Hawaii, Kansas, Michigan, Montana, North Dakota, South Dakota, Texas, Utah, Vermont and Wyoming.

ARIZONA

Attorney General Tom Horne announced the sentencing of Roger Forney to 15 years in prison after Forney entered into a plea agreement to one count each of Sexual Exploitation of a Minor and Dangerous Crimes Against Children and Sexual Exploitation of a Minor, both Class 2 felonies. Responding to a citizen’s tip, the Maricopa County Sheriff’s Office (MCSO) located a destroyed laptop computer left for garbage at the scene. MCSO salvaged the hard drive and conducted a computer forensic examination of its content, finding hundreds of images of child pornography and identifying Forney as the computer owner. MCSO executed a search warrant at Forney’s residence, finding another computer with child pornography. Forney was indicted by the State Grand Jury on 10 counts of Sexual Exploitation of a Minor, a Class C felony. Upon release, Forney will be placed on lifetime probation and required to register as a sex offender. Assistant Attorney General Joseph Waters handled the case.

ARKANSAS

Attorney General Dustin McDaniel’s Cyber Crimes Unit agents arrested Don Cox on two counts of possession of child pornography, a Class C felony. The agents executed search warrants at Cox’s residence and workplace and seized a desktop computer, laptop and other electronic evidence, which will be analyzed at the Cyber Crimes Unit Forensic Lab. Special Agent Mike Lett began investigating Cox after suspecting the possession of child pornography at his residence. The Saline County Sheriff’s Office assisted in the investigation.

CALIFORNIA

Attorney General Kamala Harris’ eCrime Unit agents joined the Rohnert Park Department of Public Safety and the Tulsa Police Department to arrest Casey Meyerling of Oklahoma, the alleged owner and operator of a revenge porn website which facilitated the posting of more than 400 sexually explicit photos and extorted victims for as much as $250 each to remove the illicit content. Attorney General Harris’ Office is seeking a Governor’s warrant for Meyerling’s extradition to California. Meyerling has been charged with five felony extortion counts. According to court documents, Meyerling owned WinByState.com, which solicits the anonymous public posting of private photographs of individuals without their permission, usually obtained by the poster during a prior relationship or through stealing or hacking and known as revenge porn. WinByState.com allegedly required victims to pay via a Google Wallet account named TakeDownHammer to remove the photographs. Agents purchased a “takedown” and traced the funds to Meyerling’s bank account. Attorney General Harris’ Office is working with GoDaddy.com to suspend the website pending the investigation and identification of additional victims.

COLORADO

Attorney General John Suthers’ Office settled a lawsuit against several South Dakota Internet lenders and their principal, Martin “Butch” Webb, for making unlicensed, high cost loans. The lenders include Western Sky Financial, LLC; Payday Financial, LLC, doing business as Lakota Cash and Big Sky Cash; Great Sky Finance, LLC; Green Billow, LLC, doing business as Four Seasons Cash; and Red Stone Financial, LLC. Webb and his companies made more than 16,000 loans to Colorado consumers with interest rates of from 90 percent to over 500 percent, with some as high as 10,000 percent. The settlement permanently prohibits Webb and his companies from making or collecting loans to or from Colorado consumers and requires defendants to
pay $565,000 to the State.

**CONNECTICUT**

Attorney General George Jepson’s Office and the Federal Trade Commission entered into a settlement with LeanSpa LLC, NutraSlim LLC and Nutraslim U.K. Ltd. and their owner, Boris Mizhen, providing restitution to consumers harmed by the companies’ alleged deceptive and unfair Internet marketing and sales practices to sell dietary supplements. Deceptive practices used included fake news and testimonials; “free” trials if consumers paid for shipping and handling, but then charging consumers for the trial; billing of unauthorized charges; failure to disclose preconditions for cancellations; and failure to provide refunds. The settlement includes a monetary judgment of $32,725,453, which is suspended in part due to evidence defendants were unable to pay the full amount. The settlement requires a court-appointed receiver to sell real estate owned by Mizhen and his wife, and requires the liquidation of other assets to make partial payment. The settlement also enjoins deceptive practices and requires greater oversight over affiliate programs and compliance reporting measures for the next 20 years. Assistant Attorneys General Jonathan Blake, Matthew Fitzsimmons, José René Martinez and Philip Rosario, head of the Consumer Protection Department, assisted in the case.

**DELAWARE**

Attorney General Beau Biden announced the arrest of Jeremy Fiske on 25 counts of Dealing in Child Pornography following an undercover online investigation conducted by the Delaware Child Predator Task Force, assisted by the Middletown Police Department, a Task Force member agency. The Task Force, police detectives and a DSP Troop #9 Trooper executed a search warrant at Fiske’s residence and seized multiple computers and other evidence. A forensic preview of the evidence revealed multiple files of child pornography.

**GEORGIA**

Attorney General Sam Olens announced a jury found Faiz Al-Khayyal, a former Georgia Institute of Technology professor, guilty of all 76 counts of possession of child pornography. While Al-Khayyal was on a teaching assignment in China, Georgia Tech found child pornography on his computer and notified Attorney General Olens’ Office. An investigation by the Georgia Bureau of Investigation (GBI) revealed child pornography on Al-Khayyal’s office computer, and he was detained upon his return and his laptop seized. Assistant Attorney General Laura Pfister prosecuted the case, and the GBI investigation was headed by former Agent Vaughn Estes.

**ILLINOIS**

Attorney General Lisa Madigan’s investigators, with assistance from the Freeport Police and the Stephenson County State’s Attorney’s Office, arrested John Fernandez on seven counts of possession, and three counts of dissemination, of child pornography, all Class X felonies each punishable by six to 30 years imprisonment. A search of Fernandez’ residence was also conducted.

**KENTUCKY**

Attorney General Jack Conway’s Cybercrimes Unit arrested Gordon Bowers, an environmental scientist at the Department for Natural Resources Division of Mine Reclamation and Enforcement, on multiple counts of possession of child pornography, a class D felony punishable by one to five years in prison on each count. The arrest resulted from an investigation revealing Bowers, using a file sharing software program, downloaded child pornography images and saved them to his state office computer. Unit investigators executed a search warrant at Bowers’ office and discovered Bowers was actively downloading such images.

**LOUISIANA**

Attorney General Buddy Caldwell announced the arrest of David Hall on charges of aggravated incest, molestation of a juvenile and 20 counts of producing child pornography. The arrest resulted from a joint
investigation involving Attorney General Caldwell’s High Technology Crimes and Fugitive Apprehension Units and the St. Tammany Parish Sheriff’s Office. Investigators had executed a search warrant on Hall’s residence for possession of child pornography, but a subsequent forensic examination on evidence seized confirmed Hall also produced child pornography. If convicted, Hall faces up to 99 years in prison on both the aggravated incest and the molestation charges, and up to 20 years on each count of producing child pornography.

MASSACHUSETTS

Attorney General Martha Coakley announced the arraignment of David Linnehan on two counts of Production of Child Pornography, Attempted Production of Child Pornography, eight counts of Dissemination of Child Pornography, 11 counts of Possession of Child Pornography, 13 counts of Unauthorized Access to Computer Systems, Unlicensed Possession of a Firearm and Unsecured Storage of a Firearm. State Police assigned to Attorney General Coakley’s Office learned about an email account linked to a residence believed to be involved in trading of child pornography, and they executed a search warrant on that residence and arrested Linnehan on possession of child pornography. Further investigation revealed Linnehan allegedly stored thousands of images and videos of child pornography on computers and storage media at his home and workplace and also distributed the images via email. Linnehan also used his position as IT administrator at Springfield College to gain unauthorized access to students’ computers and email accounts, copying and downloading private photographs. Attorney General Coakley’s Office has worked with the College to identify and notify affected students. The case is being prosecuted by Assistant Attorney General Timothy Wyse of Attorney General Coakley’s Cyber Crime Division. Attorney General Coakley’s Computer Forensics Lab, the State Police Internet Crimes Against Children Task Force, Homeland Security Investigations agents and the Granby Police Department assisted with the case.

MICHIGAN

Attorney General Bill Schuette co-hosted Google’s Good to Know Roadshow, an interactive event highlighting the importance of cyber safety to middle school students and parents. The session included such topics as creating a memorable password, tips to identifying phishing scams and considering the consequences of shared content on social media.

MISSOURI

Attorney General Chris Koster’s Office sued Stadia Studio, LLC and Michael Allton for failing to provide website design, development and hosting services after receiving down payments from clients. According to the lawsuit, Stadia Studio solicited clients for website services, often through Craigslist. The company required an “initial retainer” of 50 percent of the total contract price before work began, but failed to provide contracted web design services for at least 11 clients who paid a total of $12,000 and ceased communicating with them when they requested refunds. Attorney General Koster alleges Alton operates a similar web design and hosting firm named Social Media Hat, failing to register it as a business as required under State law. The lawsuit seeks full restitution for consumers and an order preventing Alton from advertising or engaging in any website design or development services in the State. Attorney General Koster is also asking the court to impose fines for making false promises and misrepresentation.

NEW JERSEY

Acting Attorney General John Hoffman announced a guilty plea was entered by Max Melis to one count of second-degree distribution of child pornography and one count of fourth-degree possession of child pornography. Melis was among 27 defendants arrested as a result of “Operation Watchdog,” a multi-agency investigation led by the State Police and the Division of Criminal Justice targeting offenders who distribute known images and videos of child pornography. The State will
recommend a sentence of five years in State prison, and Melis will be required to register as a sex offender upon release. Deputy Attorney General Anand Shah prosecuted the case and took the guilty plea for the Division’s Computer Analysis & Technology Unit. Melis admitted he knowingly used Internet file sharing software to make multiple files of child pornography readily available to download from a designated shared folder on his computer. A State Police detective downloaded child pornography from that folder. State Police executed a search warrant at Melis’ home and arrested him, and a forensic examination of his computer revealed he possessed at least 84 files of child pornography and shared at least 37, including 29 videos.

NEW MEXICO
Attorney General Gary King’s Communications Division presented an Internet safety workshop to parents at a Rio Rancho high school. The workshop was intended to ensure the safety of students on the Internet.

NEW YORK
Attorney General Eric Schneiderman’s Office reached a settlement with Western Sky Financial, LLC; CashCall, Inc.; WS Funding, LLC; and their owners, Martin Webb and J. Paul Reddam, for violations of the State’s usury and licensed lender laws relative to personal loans they made over the Internet. Under the settlement terms, the companies and their owners will cease collecting interest on outstanding loans made by Western Sky to State consumers, provide refunds to State borrowers who paid back more than the principal of their loan plus the interest rate of 16 percent and pay $1.5 million in penalties. The companies charged New Yorkers annual rates of interest ranging from 89 percent to more than 355 percent, far exceeding the maximum rate allowed under State law, which is limited to 16 percent for most lenders. None of the companies, which are located in South Dakota and California, were licensed in New York. The settlement also creates a settlement fund to distribute refunds to eligible State consumers. The companies and their owners are also required to stop their illegal lending practices and stop lending in New York until they comply with State law and are properly licensed. The case was handled by Assistant Attorneys General Jordan Adler and Clark Russell, under the supervision of Bureau of Consumer Frauds and Protection Chief Jane Azia and Executive Deputy Attorney General for Economic Justice Karla Sanchez.

OHIO
Attorney General Mike DeWine’s Crimes Against Children Unit agents joined Fairfield Police Department officers to arrest Brent King, a registered sex offender, pursuant to a child pornography investigation. A search warrant was executed at King’s home, and agents seized electronics believed to contain child pornography. King was convicted in Indiana on a child molestation charge in 2007. The Ohio Adult Parole Authority took King into custody on a parole violation.

OKLAHOMA
Attorney General Scott Pruitt announced the sentencing of Aaron Howk to 35 years in prison after pleading guilty to five counts of distributing child pornography and one count each of sexual abuse of a child and manufacturing child pornography. The guilty plea and sentencing resulted from an investigation by Attorney General Pruitt’s Internet crimes agent and the State Internet Crimes Against Children Task Force. The Attorney General’s investigators received a cybertip from both the National Center for Missing and Exploited Children and the FBI alleging Howk was distributing child pornography on an online photo sharing site. Task Force members from Attorney General Pruitt’s Office, the State Bureau of Investigation ICAC and Computer Crimes Units and the Edmond, Guthrie and Tulsa Police Departments executed a search warrant at Howk’s residence. Howk must serve at least 85 percent of his 35-year prison term before becoming eligible for parole.
OREGON

Attorney General Ellen Rosenblum announced the sentencing of Thomas Noah to 96 months in prison after pleading guilty to 22 counts of possession and distribution of child pornography. Noah’s sentence resulted from an investigation by the Department of Justice’s Internet Crimes Against Children (ICAC) Task Force. ICAC Special Agents and detectives located the residence distributing the pornographic images and executed a search warrant, finding child pornography images on a computer, in printed format and on other electronic storage devices. Noah later admitted to being involved in the possession and distribution of the images.

PENNSYLVANIA

Attorney General Kathleen Kane’s agents arrested Brian Vandruff on nine counts of distribution of child pornography, six counts of possession of child pornography and one count of criminal use of a communications facility. Agents conducting an online investigation discovered files of suspected child pornography allegedly downloaded to Vandruff’s computer. They executed a search warrant, seizing the computer and external hard drives, which had hundreds of video files of suspected child pornography and will be analyzed by Attorney General Kane’s Computer Forensics Unit. Vandruff will be prosecuted by Deputy Attorney General Anthony Marmo of Attorney General Kane’s Child Predator Section.

SOUTH CAROLINA

Attorney General Alan Wilson announced the Internet Crimes Against Children (ICAC) Task Force arrested Xavier Fulwood on 20 counts involving child pornography. The Task Force received information from the Berkeley County Sheriff’s Office and the Columbia Police Department, both Task Force members, about child pornography images being disseminated from an account traced to Fulwood’s residence. A search warrant was executed by the Clarendon County Sheriff’s Office and Task Force special investigators, and computers and electronic media were seized for analysis. Fulwood admitted to downloading child pornography and was charged with 20 counts of Sexual Exploitation of a Minor second degree, a felony offense punishable by up to 10 years on each count. The case will be prosecuted by Attorney General Wilson’s Office.

TEXAS

Attorney General Greg Abbott’s Internet Crimes Against Children (ICAC) Task Force hosted a training conference for law enforcement agencies affiliated with the program. Law enforcement personnel from the Department of Public Safety and the Austin Police Department also attended. Task force officers provided basic investigative instruction about uncovering online exploitation crimes and discussed ICAC operational standards. The new affiliates also received information about grant funding, federal law and obtaining search warrants for child exploitation crimes.

VERMONT

Attorney General William Sorrell announced the arrest of Mark Zielinski on five felony counts of Promoting Child Pornography. The charges stem from a shared investigation between Attorney General Sorrell’s Office, the Vermont Internet Crimes Against Children Task Force and the State Police. According to court documents, Zielinski distributed child pornography over the Internet using peer-to-peer file sharing programs.

WISCONSIN

Attorney General J.B. Van Holle’s Division of Criminal Investigation (DCI) special agents, with assistance from the Oak Creek and Milwaukee Police Departments, arrested two suspects for Trafficking of a Child. The suspects allegedly arranged for a 16-year-old female to meet with men in Milwaukee and Chicago for sexual activity. Investigators also found narcotics and a firearm during the execution of a search warrant at the suspects’ residence.
NEVADA, DELAWARE SIGN ONLINE POKER AGREEMENT

On February 25, Nevada and Delaware signed the Multi-State Gaming Agreement, establishing a legal framework for the first authorized interstate Internet gambling. The agreement seeks to expand the marketplace for online poker in smaller states without significant populations for Internet gambling to flourish. Nevada has legalized poker-only online for players logging on within the State, while Delaware has approved online slots, blackjack, roulette and poker. No date was given for interstate poker to go live, as technology providers must harmonize site platforms in both states.

FCC TO DOUBLE $$ FOR BROADBAND IN SCHOOLS, LIBRARIES

The Federal Communications Commission (FCC) announced it will double the amount of funding for high-speed Internet connections in schools and libraries over the next two years. Financing for the increased funding will come from restructuring the $2.4 billion E-Rate program, which provides money for “advanced telecommunications and information services” using the proceeds of fees paid by telecommunications users. The proportion to fund broadband service in schools and libraries will increase to $2 billion a year from $1 billion. The E-Rate program is part of the Universal Service Fund, which also provides funds to connect rural areas and low-income people to phone and Internet service through fees on consumers’ phone bills. Most of the redirected spending in 2014 will come from funds remaining from previous years, but in 2015 much of the funding will be from changes to the E-Rate program, including the elimination of programs paying for outdated technologies, such as paging services, dial-up Internet connections and email programs available for free elsewhere. The spending will be used to increase available broadband speeds and provide wireless networks to schools.

U.S. ISSUES CYBERSECURITY FRAMEWORK

On February 12, the U.S. Department of Commerce’s National Institute of Standards and Technology (NIST) issued “Framework for Improving Critical Infrastructure Cybersecurity,” a management tool designed to enable organizations to improve the security of their critical infrastructure. The project resulted from a year-long collaboration between NIST and more than 3,000 “stakeholders” from the public and private sectors. On February 14, the “NIST Roadmap for Improving Critical Infrastructure Cybersecurity,” a companion piece to the framework, was issued. It identifies key areas for cybersecurity development, alignment and collaboration, including the development of better identity and authentication technologies, automated indicator sharing, conformity assessments, data analytics and the cybersecurity workforce. The Framework may be accessed at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. The Roadmap may be accessed at http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

FTC SEEKS COMMENT ON FANTAGE.COM SETTLEMENT

The Federal Trade Commission (FTC) is seeking public comment on a proposed settlement with the website Fantage.com, a virtual world for children. The consent agreement would resolve allegations Fantage.com misrepresented its status as a current participant in the U.S.-EU Safe Harbor Framework, when in fact its certification had lapsed. The Safe Harbor framework allows U.S. companies to transfer data outside the EU in a manner consistent with EU law. In order to join the framework, companies must self-certify to the U.S. Department of Commerce their compliance with a set
of principles and requirements to protect privacy, including notice, choice, onward transfer, security, data integrity, access and standards. The Department maintains a public database of the companies taking these steps. The FTC alleges Fantage renewed its self-certification when in fact its website was not in compliance. Comments on the settlement may be filed online by March 13, 2014 at https://ftcpublic.commentworks.com/ftc/fantageconsent and will be made public, including names and states, on the FTC website. An analysis of the settlement may be accessed at https://www.federalregister.gov/articles/2014/02/19/2014-03532/fantagecom-inc-analysis-of-proposed-consent-order-to-aid-public-comment.

The Ninth Circuit Court of Appeals launched live streaming Internet coverage of its en banc oral arguments in San Francisco, the first such effort by a federal appeals court. The arguments can be accessed from the court’s website at http://www.ca9.uscourts.gov.

Casetext, a website created by attorneys Jake Heller and Joanna Huey, offers crowdsourced legal research using contributions from groups of people to create or enhance content. Essentially, the site provides a database for researching case law, but it seeks to enhance the cases by encouraging users to add descriptions, tags, annotations and documents, as well as links to secondary sources. Other users can vote up or down on those additions. The right half of the web page will show the most popular annotations, secondary sources and related cases, and selecting any one of those categories will show the full list of user-added items. The site is free and is accessed at https://casetext.com.

Constituteproject.org, a new searchable database of 189 worldwide constitutions, is now available. It was developed by constitutional scholars Zachary Elkins of the University of Texas, Tom Ginsburg of the University of Chicago Law School and James Melton of University College London pursuant to a grant from Google Ideas. Users can locate relevant passages on a particular subject based on searchable terms, such as “right to privacy,” and can filter searches by country or date.

McAfee Labs released its seven threat predictions to cybersecurity in 2014, revealing a plethora of dangers to try to avoid. The report predicts the following concerns: 1) mobile malware targeting Android devices; 2) ransomware attacks on virtual currencies; 3) new attack technologies against security software, such as sandbox-aware attacks and return-oriented programming attacks; 4) attacks using the features of social networks to gather data about users; 5) attacks exploiting vulnerabilities above and below operating systems; 6) sophisticated advance evasion technique attacks which may be thwarted by Big Data analytics; and 7) exploitation of cloud-based corporation applications. The full report may be accessed at http://mcafee.com/utjz4.

Microsoft Corp. signed memorandums of understanding with the Organization of American States and Europol during its first annual Cybercrime Enforcement Summit to collaborate against cybercrime. The summit
included more than 60 officials and experts from law enforcement, academia and the private sector who shared solutions to the global cybercrime problem.

IN THE COURTS

FOURTH AMENDMENT: PRIVATE SEARCH EXCEPTION

U.S. v. Goodale, 2013 U.S. App. LEXIS 25756 (8th Cir. December 30, 2013). The Eighth Circuit Court of Appeals found the private search exception to the warrant requirement applied. The 13-year-old male victim showed his mother a history of child pornography sites on the laptop of Michael Goodale, who was staying with them. They took the laptop to police, showing police the same history, and the victim also described how Goodale had sexually abused him and his young cousin. The police interviewed Goodale and, over his objection, seized his laptop pending a search warrant, which they shortly thereafter obtained. A grand jury indicted Goodale, who was subsequently convicted in the U.S. District Court for the Northern District of Iowa on two counts of aggravated sexual abuse, two counts of interstate transportation of a minor with intent to engage in criminal sexual activity and one count of accessing child pornography. Goodall appealed, arguing the district court erred in denying his motion to suppress the evidence obtained from his laptop because it was obtained based on a warrantless search in violation of the Fourth Amendment. The appeals court disagreed, finding the private search exception to the warrant requirement was applicable, noting the search was performed by the victim and his mother, and was neither instigated nor performed at the request of police. The court ruled when the government re-examines materials following a private search, it may intrude on an individual’s privacy expectations without violating the Fourth Amendment, provided the government’s examination goes no further than the private search. The judgment was affirmed.

FIFTH AMENDMENT: CUSTODIAL INTERROGATION

State v. Beasley, 2013 Mo. App. LEXIS 1540 (December 24, 2013). The Missouri Court of Appeals, Eastern District, Division 4, found the error in admitting defendant’s statements did not result in manifest injustice. Leland Beasley, Jr. was convicted of three counts of child molestation in the first degree, four counts of statutory sodomy in the first degree, one count of attempted statutory sodomy in the first degree, one count of attempted statutory sodomy in the second degree, one count of promoting child pornography in the first degree and three counts of possession of child pornography. He appealed, arguing the trial court erred in denying his motion to suppress statements he made to police regarding ownership of a black box in which police found evidence of child pornography. Beasley argued the statements violated his right to counsel and privilege against self-incrimination because the statements were obtained during a custodial interrogation before police gave him Miranda warnings and without his counsel present. The court found the statements were illegally obtained in violation of the Fifth Amendment, but their admission at trial did not result in manifest injustice given the overwhelming evidence of Beasley’s guilt. The judgment was affirmed.

PROBABLE CAUSE: SEARCH WARRANT AFFIDAVIT

State v. Aguilar, 2013 Tenn. Crim. App. LEXIS 1101 (December 18, 2013). The Tennessee Court of Criminal Appeals at Nashville found the affidavit in support of the search warrant application was sufficient to support a finding of probable cause. Jared Aguilar was convicted of six counts of sexual exploitation of a minor. He appealed, arguing among other claims that the trial court erred in denying his motion to suppress evidence seized pursuant to a search warrant because the affidavit in support of the warrant applica-
tion did not contain sufficient facts to establish probable cause. The court disagreed, finding the 27-page warrant detailed the investigator’s extensive training and experience and showed how images were found on a computer at Aguilar’s address through the use of a file-sharing program, refuting the claim Aguilar had an expectation of privacy in the files viewed and the claim the affidavit failed to show a nexus between the files viewed by the investigator and Aguilar’s residence. The court found the affidavit contained facts sufficient to support a finding of probable cause and affirmed the judgment. Ed. note: Assistant Attorney General Kyle Hixson represented the State.

**RELEVANCE: WEBSITE HISTORY**

**IDENTIFICATION**

State v. Botelho, 2013 N.H. LEXIS 138 (December 24, 2013). The New Hampshire Supreme Court ruled any error in admitting information about the website was harmless due to the overwhelming evidence of defendant’s guilt. Jessica Botelho left her young sons unattended in the bathtub while she visited an Internet site on breast implants, and one of the sons nearly drowned and later died of brain damage. Forensic evidence demonstrated nearly continuous online activity for almost 40 minutes, and the water level in the bathtub indicated the two children spent an extended period of time there. Botelho was convicted of manslaughter, negligent homicide and reckless conduct. She appealed, arguing the trial court erred in admitting identifying information about the website she visited because it was not relevant, and even if it was, any probative value was outweighed by the danger of unfair prejudice. The New Hampshire high court noted the evidence related to the website was limited to web addresses and short descriptions, and the State had emphasized the site’s networking features and Botelho’s interest in it, rather than the site’s content. Further, the court found Botelho’s guilt rested upon the length of her computer use, not the particular websites she visited. The court decided any error in admitting identifying information about the website was harmless because the evidence of Botelho’s guilt was overwhelming. The judgment was affirmed.

**FIRST AMENDMENT: BLOGGER DEFAMATION**

Obsidian Finance Group, LLC v. Cox, 2014 U.S. App. LEXIS 948 (9th Cir. January 17, 2014). The Ninth Circuit Court of Appeal determined the blogger could not be held liable for defamation unless she acted negligently. Obsidian Finance Group, a firm providing advice to financially distressed companies, was retained by Summit Accommodators in connection with their pending bankruptcy. The bankruptcy court then appointed Kevin Padrick, a principal at Obsidian, as the Chapter 11 trustee. Since Summit had misappropriated clients’ funds, Padrick’s main task was to marshal those funds on behalf of the clients. After Padrick’s appointment, Crystal Cox, who had a history of making allegations and seeking payoffs for retractions, published several blog posts accusing Padrick and Obsidian of fraud, corruption and money laundering in connection with the bankruptcy. Padrick and Obsidian sent Cox a cease and desist letter, but when she persisted, they sued for defamation. The U.S. District Court for the District of Oregon found all but one of Cox’s blog posts were constitutionally protected because they used figurative language and did not assert facts. The single defamation claim proceeded to trial, and the jury found in favor of Padrick and Obsidian, awarding them $1.5 million and $1 million, respectively, in compensatory damages. Cox moved for a new trial, which was denied, and she appealed. Obsidian and Padrick cross-appealed, arguing the jury should have been allowed to hear their defamation claims on the other blog posts. The appeals court found the allegations against Padrick and Obsidian were a matter of public concern, noting First Amendment protections do not depend on whether the defendant was a trained journalist. Therefore, the court reversed and remanded for a new trial. The court also affirmed the district
Knowing Possession: Sufficiency of Evidence

U.S. v. Smith, 2014 U.S. App. LEXIS 651 (5th Cir. January 13, 2014). The Fifth Circuit Court of Appeals ruled there was sufficient evidence of “knowing” possession of child pornography because the file names clearly indicated their contents. James Smith was charged with knowing possession of child pornography. At trial in the U.S. District Court for the Northern District of Mississippi, the prosecution produced uncontroverted evidence showing someone intentionally downloaded videos of child pornography to Smith’s computer during the period when Smith and two roommates, his girlfriend Elizabeth Penix and friend Joshua Jolly, were the exclusive users of the computer. Employment records eliminated Penix as a suspect, and Jolly denied any knowledge of the files. Smith did not testify. Expert testimony established the files were explicitly named, so an individual downloading them would know of their content. A jury found Smith guilty, and he moved for a new trial and a verdict of acquittal. The district court denied the motion for a new trial but entered a judgment of acquittal, finding the evidence was insufficient to sustain the verdict and it was just as likely Jolly downloaded the files as Smith. The government appealed, and the appeals court reversed, finding the prosecution presented sufficient evidence to enable the jury to find, without a reasonable doubt, that Smith downloaded the files and knew what he was downloading. The decision was reversed and the case remanded for sentencing.

Shared Files: Suppression Motion

Rideout v. Commonwealth, 2014 Va. App. LEXIS 22 (February 4, 2014). The Court of Appeals of Virginia found defendant was not entitled to suppression of the evidence. Pursuant to an investigation of peer-to-peer sharing of child pornography, police obtained a search warrant for Marvin Rideout’s residence, seizing privacy in the cell site location information (CSLI), and therefore the warrant requirement applied. Shabazz Augustine was a suspect in the murder of his girlfriend, who had gone missing on August 25, 2004. Police obtained call logs for the victim’s and Augustine’s cell phones, including the date, time, duration and incoming and outgoing telephone numbers on August 24 and 25, 2004. An ADA subsequently filed an application for a §2703(d) order, supported by a trooper’s affidavit of the investigation, to obtain from Sprint, Augustine’s cell phone provider, certain records for Augustine’s cell phone, including CSLI, for a 14-day period beginning August 24, 2004. The order was issued, and the Commonwealth received at least 64 pages of SCLI related to Augustine’s cell phone. Seven years later, Augustine was indicted for the murder. He filed a motion to suppress the evidence of his CSLI, arguing it violated his Fourth Amendment rights. The court agreed there was a search and the evidence should be suppressed. The Commonwealth appealed, and the state Supreme Court held even though the CSLI was a Sprint business record, Augustine had a reasonable expectation of privacy in it, so therefore the warrant requirement applied. The court further noted because only reasonable suspicion, not probable cause, was required to issue a §2703(d) order, the Commonwealth could on remand seek to establish the affidavit in support of its application for that order also demonstrated probable cause for the order to provide the CSLI records. The allowance of Augustine’s motion to suppress was vacated and the case remanded to motion court.
several electronic devices which forensic analysis found to contain child pornography. Rideout filed a pretrial motion to suppress the files discovered by police in their initial search, claiming he had a reasonable expectation of privacy in the files and he had inadvertently activated file sharing on his computer, allowing police to view the files. The motion was denied, and Rideout entered a conditional guilty plea to 20 counts of possession of child pornography, then filing an appeal. He argued the trial court erred in denying his motion to suppress the evidence pursuant to the Fourth Amendment. The appeals court disagreed, finding Rideout was not entitled to suppression because, by downloading a program designed to facilitate the sharing of files, he opened his files to any other person, including law enforcement. The court found a police officer viewed those files and then properly obtained and executed a search warrant at Rideout’s home, where more incriminating evidence was located. The judgment was affirmed.

**STATUTE INTERPRETATION: READING CELLPHONE MAPS AND DRIVING**

*The People v. Spriggs*, 2014 Cal. App. LEXIS 190 (February 27, 2014). The California Court of Appeal, Fifth Appellate District, decided the Legislature intended to prohibit only the use of a wireless telephone to engage in conversation while driving. While stopped in heavy traffic, Steven Spriggs accessed his cell phone to check a map application for a way to avoid the congestion. A patrol officer saw him and issued him a traffic citation for violating Vehicle Code § 23123, subdivision (a), prohibiting drivers from “using a wireless telephone unless that telephone is specifically designed and configured to allow hands-free listening and talking, and is used in that manner while driving.” Spriggs contested the citation, but was found guilty and ordered to pay a $165 fine. He appealed, arguing the only use of a wireless phone prohibited by the code is listening and talking on the phone if doing so requires the driver to hold the telephone in his or her hand. The lower court affirmed Spriggs’ conviction, concluding the statute was designed to prohibit all “hands-on” use of the wireless phone while driving. Spriggs sought review, and the appellate court concluded, based on the statute’s language, legislative history and subsequent legislative enactments, the statute means what it says and only prohibits a driver from holding a cell phone while conversing on it. Spriggs’ conviction was reversed.

*Ed. Note: Assistant Attorney General Michael Farrell and Deputy Attorneys General Daniel Bernstein and Doris Calandra of the California Department of Justice represented the People.*

**LEGISLATIVE UPDATE**

**INTERNET GAMBLING**

NEW JERSEY. On January 27, S980 was introduced, a bill which would allow the State to enter into reciprocal agreements with other states or countries with legalized gambling to allow their residents to access the 15 gambling websites operated by the Atlantic City casinos. It would compel payment processors to obtain a casino industry service license, requiring background checks, to encourage financial institutions to allow credit cards used in online gambling. The bill has been referred to the State Government, Wagering, Tourism and Historic Preservation Committee.

**DATA COLLECTION**

CALIFORNIA. On January 30, the Senate passed SB 383, a bill limiting the information online retailers can collect from consumers to their billing addresses and ZIP codes, with the proviso that such information be securely destroyed when no longer needed for fraud detection. The bill would impose a penalty of $250 for the first violation and $1,000 for each subsequent violation. The bill has been sent to the Assembly.
SUPREME COURT UPDATE

The U.S. Supreme Court has granted review of two cases involving the search of a cell phone after arrest. Below is a synopsis of both cases written by Dan Schweitzer, NAAG Supreme Court Counsel.

Riley v. California, 13-132. The Court will decide whether the Fourth Amendment permits a warrantless search of the contents (including photos and video) of an individual’s cell phone seized from him incident to his lawful arrest. In 2009, petitioner David Riley was pulled over by police for driving with expired registration tags. Upon learning that Riley was also driving with a suspended license, the police impounded his car and conducted an inventory search to document the car’s contents. During that search, police discovered two firearms hidden under the hood and arrested Riley for carrying concealed and loaded weapons. The police seized Riley’s “smartphone” during the arrest, and performed two separate warrantless searches. Police initially scrolled through the phone’s contents at the scene, at which point they noticed suspicious words in text messages and contacts, possibly indicating that Riley was involved with a particular street gang. Two hours later, after conducting an interrogation in which Riley was unresponsive, police conducted a more thorough search of his phone. During the second search, police found photos and video of Riley and others, further suggesting that he was part of a gang. They also found a photo of Riley in front of a red Oldsmobile that police suspected had been used in a prior shooting. After ballistic testing revealed that the firearms seized during Riley’s traffic stop were used in that shooting, Riley and two others were charged with shooting at an occupied vehicle, attempted murder, and assault with a semiautomatic firearm. Prior to trial, Riley moved to suppress all of the evidence seized from his cell phone. The trial judge denied the motion, finding that the searches were legitimate searches incident to arrest. Riley ultimately was convicted on all three charges. While Riley’s case was proceeding to trial, the California Supreme Court decided People v. Diaz, 244 P.3d 501 (2011), in which it held that the Fourth Amendment’s search-incident-to-arrest doctrine permits police to search a cell phone (even some time later at the stationhouse) whenever the phone was “immediately associated with the arrestee’s person” at the time of arrest. Applying Diaz, the California Court of Appeals affirmed petitioner’s convictions in an unpublished opinion. The California Supreme Court denied review without comment.

Riley notes that federal and state courts are openly divided over whether the Fourth Amendment permits police officers to search the digital contents of an arrestee’s cell phone incident to arrest. He attributes the divide, in part, to disagreement over the qualitative differences between cell phones and traditional physical containers that might be seized incident to arrest. Riley argues that the Fourth Amendment forbids cell phone searches incident to arrest because once a cell phone is securely under police control neither of the rationales for searches incident to arrest — to locate weapons or prevent the destruction of evidence — applies. He also argues that the profound privacy concerns attendant to modern cell phone use make it unreasonable for police officers to search digital content. The State of California argues, consistent with Diaz, that while the Fourth Amendment prohibits warrantless delayed searches of items that merely had been within the arrestee’s control at the time of the arrest, it permits such searches of the “person of the arrestee” and of the personal property “immediately associated with the person of the arrestee.” United States v. Robinson, 414 U.S. 218 (1973); United States v. Edwards, 415 U.S. 800 (1974). It is the lawful arrest and the resulting diminished expectation of privacy, California argues, that establish the authority to conduct such searches.

United States v. Wurie, 13-212. This case is similar to
Riley v. California, but involves an old-fashioned “flip phone” and a narrower search. In 2007, Boston police arrested respondent Brima Wurie for drug distribution after they observed him making an apparent drug sale out of his car. Five to ten minutes after Wurie arrived at the station, officers noticed that one of his two cell phones—a flip phone—was receiving calls from a caller identified as “my house” on the phone’s external screen. Officers opened the phone, pressed one button to navigate the call log, and then pressed a second button to obtain the phone number for “my house.” They also saw the “wallpaper” on the phone’s internal screen, a picture of a women holding a baby. Police ultimately located the address for “my house,” found a mailbox labeled with Wurie’s name, and observed the woman pictured on Wurie’s phone through a window. They then obtained and executed a search warrant for the apartment, and seized drugs, cash, and a firearm. Wurie was charged with being a felon in possession of a firearm and with possession and distribution of crack cocaine. Wurie moved to suppress the evidence obtained from the apartment, arguing that it was the fruit of the unconstitutional search of his cell phone’s call log. The district court denied the motion, and Wurie was convicted on all charges. A divided panel of the First Circuit reversed the district court’s denial of the motion to suppress. 2013 WL 2129119 (not yet published).

ABC, Inc. v. Aereo, Inc., 13-461. The Court will decide whether a company violates the Copyright Act when it retransmits a television program to paid subscribers over the Internet. Again, here is Dan Schweitzer’s summary below.

Aereo subscribers can watch programs on their computers or other Internet-connected devices while the programs are being broadcast (with a slight delay) or record them to watch at a later time. A number of holders of copyrights in broadcast television programs, including petitioners, filed copyright infringement actions against Aereo in federal district court. They sought a preliminary injunction barring Aereo from transmitting their programs over the Internet while the programs are still airing, arguing that those transmissions infringe their exclusive right to publicly perform their works. The district court denied the motion, concluding that petitioners were unlikely to prevail on the merits. The Second Circuit affirmed in a 2-1 decision. 712 F.3d 676.

Relying on its decision in Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121 (2008) (Cablevision), the Second Circuit focused on the “transmit clause” of the Act’s definition of what it means to perform or display a copyrighted work publicly. 17 U.S.C. §101. The Court reasoned, as it did in Cablevision, that the transmit clause requires examination of the potential audience of a particular transmission, as “private” performances are generally exempt from copyright liability. Because Aereo’s system creates a unique digital copy of a program for each subscriber who elects to watch or record it, and then transmits the program to the subscriber from that unique copy, the potential audience for each transmission is limited to one subscriber. Moreover, the subscriber has control over how and when his or her copy will be played back. Thus, concluded the court, Aereo’s transmission of a program to an individual subscriber is not a public performance. The court rejected the argument that Aereo’s private transmissions of the same program to many subscribers should be aggregated, finding it irrelevant to the transmit clause analysis that, in the end, the public may be capable of receiving the same underlying work or original performance.
Finally, the Court will decide whether a company with a patented method for delivery of web content is liable for infringement when it performs some steps of its patented process and instructs its customers on how to perform the remaining steps. Once again, we turn to Dan Schweitzer’s summary of the case below.

Limelight Networks, Inc. v. Akamai Tech., Inc., 12-786. In this “divided infringement” case, the Court will decide whether a defendant may be held liable under 35 U.S.C. §271(b) for inducement of infringement when it performs some steps of a patented process and instructs its customers on how to perform the remaining steps, even if no single participant takes all of the steps that would make one liable for direct infringement under §271(a). Respondent Akamai Technologies has a patented method for efficient delivery of web content, which consists of placing some content on a set of multiple alternative servers and modifying the content provider’s web page to instruct web browsers to retrieve the content from the servers. Petitioner Limelight Networks maintains a set of servers as provided for in Akamai’s patented method, but does not itself modify content providers’ web pages to complete the process, instead instructing content providers on how to do so. Akamai sued Limelight for infringement. The jury found for Akamai, but the district court granted Limelight’s motion for judgment as a matter of law. The district court concluded that because Limelight lacked “direction and control” over its customers, their actions could not be attributed to Limelight, meaning that no one entity performed (or vicariously performed) all of the steps of Akamai’s patented process so as to be liable for direct infringement under §271(a). The en banc Federal Circuit reversed, holding that Limelight could be held liable under §271(b) for induced infringement even if no entity could be held liable under §271(a) for direct infringement. 692 F.3d 1301.

Limelight argues in its petition that the Patent Act does not distinguish between direct infringement that violates §271(a) and direct infringement that proves a predicate for claims of inducement under §271(b). The Federal Circuit’s decision, Limelight argues, creates inconsistency between the use of the verb “infringe” in §271(a) and §271(b) and is incompatible with the “fundamental precept” that there can be no indirect infringement absent proof of direct infringement. The United States, in an amicus brief filed at the invitation of the Court, agrees with Limelight, stating that although the Patent Act thus contains a “loophole” for infringers, “the authority and responsibility for filling any
perceived statutory gap belongs to Congress rather than the courts.”

Petitioners argue that Aereo offers precisely the kind of service Congress sought to prohibit when it revised the Act to define “public performance” to include retransmission of over-the-air broadcasts to the public. The plain text of the Act reaches any retransmission “by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.” 17 U.S.C. §101. Petitioners argue that Aereo’s conduct falls squarely within that definition. They insist that Aereo’s elaborate and inefficient system of assigning individual antennas to each subscriber and creating individual digital copies of programs for each subscriber is nothing more than a contrivance designed to take advantage of a loophole Cablevision created in the law. Petitioners argue that the Second Circuit’s extension of Cablevision to Aereo imperils the public interest in protecting the viability of over-the-air broadcast television and authorizes the for-profit exploitation of copyrighted works.

The First Circuit announced a bright-line rule that the search-incident-to-arrest exception does not authorize the warrantless search of data on a cell phone seized from an arrestee’s person under any circumstances. The court reasoned that the Supreme Court’s decisions in Robinson and Edwards did not foreclose treating cell phones as categorically unlike other containers, such as briefcases or wallets, searched incident to an arrest. The court explained that “a modern cell phone is a computer and a computer . . . is not just another purse or address book.” Its “immense” storage capacity allows it to hold a plethora of information “of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records.” The court found that this is “the kind of information one would previously have stored in one’s home and that would have been off-limits to officers performing a search incident to arrest.” The Court also reasoned that a warrantless search of cell phone data cannot be justified as necessary to prevent the destruction of evidence. Rejecting the government’s argument that a warrantless search may be necessary to prevent the remote destruction of data, the court stated that this concern is merely theoretical and thus insufficient to satisfy the Fourth Amendment. Plus, the police can avoid losing cell phone data by turning the phone off, removing its battery, placing it in a “Faraday enclosure,” or blind-copying its contents.

The United States argues in its petition that the First Circuit’s decision cannot be squared with Robinson and Edwards, which establish an across-the-board rule that the police may search any items found on an arrestee’s person so long as the search is not unreasonable. In the United States’ view, item-by-item exceptions would erode and complicate the rule, for no sound reason. The contents of cell phones are not necessarily more personal than information found in a brief case, for example, but are more susceptible to destruction than most other evidence as a result of “remote wiping” technology. The United States also argues that the Robinson/Edwards rule rests as much on an arrestee’s reduced expectation of privacy as it does on the need to protect officers and protect evidence. Whatever limits may exist on searches of highly personal information on a cell phone found on an arrestee’s person, the search of Wurie’s call log did not approach them. Moreover, contends the United States, the limited search in this case is separately justified as a search for evidence relevant to the crime of arrest.
NEW PUBLICATIONS AND WEB-SITES

FOURTH AMENDMENT

Professor Thomas Clancy of the University of Mississippi School of Law released the second edition of his treatise, “The Fourth Amendment – Its History and Interpretation.” This new edition includes hundreds of new cases from the U.S. Supreme Court and lower courts since the first edition was published in 2008. It highlights the increased importance of digital evidence. A discount of 20 percent is available using the discount code FOURTH14 through March 31, 2014 when ordered at http://www.caplaw.com.

CYBER ABUSE AMONG TEENS

“Technology, Teen Dating Violence and Abuse” reports on a study, funded by the National Institute of Justice, examining the prevalence of dating violence among more than 5,000 teens at 10 schools in New York, New Jersey and Pennsylvania. The study found 18 percent of those teens reported cyber abuse, such as “my partner used my social networking account without permission,” or “my partner sent texts/emails to engage in sexual acts I did not want.” The report may be accessed at https://ncjrs.gov/pdffiles1/nij/grants/243296.pdf.

BIG DATA AND PRIVACY

“Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms” by Kate Crawford and Jason Schultz, 55 Boston College Law Review 93 (2014). This article examines several existing privacy regimes and explains why these approaches inadequately address current Big Data challenges. It proposes a new approach to mitigating predictive privacy harms – that of a right to procedural data due pro-

cess. By examining the role of due process in our legal system, the article argues individuals affected by Big Data should have similar rights to those in the legal system with respect to how their personal data is used. The article may be accessed at http://bclawreview.org/review/55_1/03_crawford_schultz/.