The U.S. Department of Commerce’s National Institute of Standards and Technology (NIST) released a draft cybersecurity framework to enable both private and public companies to better evaluate cyber risk to critical infrastructure and prepare better defenses against online attacks.

The NIST draft, “Preliminary Cybersecurity Framework,” sets forth specific steps and best practices for organizations to follow, regardless of their size or public/private status, in order to better protect the U.S. infrastructure. The draft originated with an executive order issued by President Obama identifying cyber threats to the critical infrastructure as “one of the most serious national security challenges” and directing NIST to produce the framework document. The document sets out a risk-based approach to fighting cybercrime, outlining five basic functions for security strategies: identify, protect, detect, respond and recover. The framework does not impose legally binding regulations, but instead aims to serve as a model for companies to tailor to their own more specific cybersecurity needs and circumstances.

The NIST draft may be accessed at http://www.nist.gov/itl/cyberframework.cfm.
The 2014 National Cyber Crime Conference (“NCCC”), hosted by Massachusetts Attorney General Martha Coakley’s Office, has been scheduled for April 28-30, 2014. As in the previous two years, police, prosecutors and forensic examiners from local, state and federal law enforcement agencies will take part in three full days of training to help them with the challenges posed by digital evidence and technology. Attendees will learn how to better investigate cybercrime cases, as well as have the opportunity to network with law enforcement personnel from other jurisdictions. The National Association of Attorneys General Research and Training Institute (NAGTRI), the National White Collar Crime Center, SEARCH and Microsoft are partnering with Attorney General Coakley’s Office on this initiative. For more information and to register, you may access http://www.mass.gov/ago/nccc. For questions about the NCCC, please contact Natasha Falke, Program Coordinator, at Natasha.falke@state.ma.us.

Forty-eight Attorneys General announced a settlement with marketing company Affinion and its subsidiaries Trilegiant and Webloyalty, with the companies agreeing to pay more than $30 million to resolve allegations of misleading consumers into signing and paying for discount clubs and memberships. Affinion offers services such as credit monitoring, roadside assistance and discounted travel through agreements with banks and retailers and markets them via direct mail, the Internet, telemarketing and face-to-face point of sale transactions. The company charges a monthly fee for these services until cancelled by the consumer. An investigation into Affinion revealed the company misled consumers by failing to clearly and conspicuously disclose its identity and the ongoing nature of the charges. Several deceptive marketing practices were also found, including Affinion’s use of “live check” solicitations (checks which, when endorsed, effectively enrolled consumers in membership programs) and online data pass offers (offers presented immediately after an online retail purchase from one of Affinion’s partners, enabling the company to enroll and bill consumers without independently acquiring their account information).

The agreement prohibits these marketing practices and requires Affinion to provide clear information to consumers about memberships. Affinion will also establish a $19.3 million restitution fund for eligible consumers who received unauthorized charges in these participating jurisdictions: Alabama, Alaska, Arizona, Arkansas, California, Colorado, Delaware, Guam, Hawaii, Idaho, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Dakota, Tennessee, Utah, Vermont, Virgin Islands, Washington and Wyoming.

**ALABAMA**

**Attorney General Luther Strange** joined Brooke Oberwetter of Facebook’s Public Policy Office to present the “Safety and Privacy on Facebook” program to an assembly of students and parents at a high school in Montgomery. The interactive program focuses on the tools and features available on Facebook to learn more about digital citizenship and online safety.

**ARKANSAS**

**Attorney General Dustin McDaniel** filed a lawsuit against several entities accused of offering online payday loans with interest rates as high as 342 percent, in violation of state law. The defendants are Western Sky Financial; Martin Webb, aka Butch Webb and owned by Western Sky; J. Paul Reddam; and Cashcall, Inc. and its subsidiary WS Funding, both based in California and owned by Reddam. Western Sky, based in South Dakota, erroneously identified itself as a tribal entity protected by sovereign immunity because it is not owned or operated by a tribe. State consumers have been offered loans in amounts ranging from $850 to $10,000, with corresponding annual percentage rates of between 89 and 342 percent. Attorney General McDaniel is asking the court to prohibit the defendants from offering these illegal loans in the State, as well as to order restitution, civil penalties and attorneys’ fees and costs.

**CALIFORNIA**

**Attorney General Kamala Harris** filed suit against Corinthian Colleges, Inc. (CCI) and its subsidiaries operating Everest, Heald and WyoTech colleges for false and predatory advertising, intentional misrepresentation to students, securities fraud and unlawful use of military seals in advertisements. The complaint alleges CCI intentionally targeted low-income consumers through aggressive Internet, telemarketing and television marketing campaigns and knowingly misrepresented job placement rates to investors and accrediting agencies. The complaint further alleges CCI runs millions of online and mobile ads promoting medical technician programs it does not offer, and also includes U.S. military seals on web sites without authorization in violation of state law.

**CONNECTICUT**

**Attorney General George Jepson** joined Governor Dannel Malloy, Lt. Governor Nancy Wyman, Department of Transportation (ConnDOT) Commissioner James Redeker, Department of Motor Vehicles (DMV) Commissioner Melody Currey and executives from AT&T and Travelers Insurance to kick off a statewide campaign to raise awareness about the dangers of distracted driving, particularly focusing on teens using cell phones and other electronics while at the wheel. State law prohibits a motor vehicle operator from using a hand-held phone or mobile electronic device while the vehicle is in motion.

**DELAWARE**

**Attorney General Beau Biden** announced the sentencing of Thomas Fort, Jr. to nine years in prison after he pled guilty to two counts of Dealing in Child Pornography. Fort was arrested following an online undercover investigation by the Child Predator Task Force after an undercover detective obtained a video of child pornography online. A search warrant was executed at Fort’s residence, and several computers and digital storage devices containing multi-
ple videos of child pornography were seized. The continuing investigation following Fort’s arrest revealed evidence he met teens in online chat rooms and solicited unlawful images from them.

**FLORIDA**

Attorney General Pam Bondi unveiled a statewide initiative to raise awareness about human trafficking and help parents protect their children from online sex traffickers. The initiative, “From Instant Message to Instant Nightmare” debuted on billboards, bus shelters and mail displays throughout the State. Parents are directed to Attorney General Bondi’s website to download a parental tip sheet about online safety and a pledge for children to sign and print.

**ILLINOIS**

Attorney General Lisa Madigan announced the sentencing of Jesus Alanis to 20 years in prison, after he pled guilty to possession and manufacturing of child pornography, a Class X felony, and criminal sexual assault, a Class 1 felony. Alanis was arrested after a minor reported repeated sexual assaults which Alanis also videotaped. The case was referred to Attorney General Madigan’s Office by the Cook County State's Attorney's Office. Unit Supervisor Martin VanKampen of the Criminal Prosecutions/Trial Assistance Bureau handled the case.

**KENTUCKY**

Attorney General Jack Conway announced that Thomas Sellers, a former school teacher, has entered a guilty plea to seven counts of possession of child pornography, Class D felonies. The charges stem from an undercover operation by the Ohio Attorney General’s Office, which identified a computer with images of child sexual exploitation. A subpoena revealed Sellers to be the Internet subscriber. The findings were referred to Attorney General Conway’s Cybercrimes Unit, and Unit investigators executed a search warrant at Sellers’ home. A forensic examination of his computer found 455 images and 325 videos depicting the sexual exploitation of children. The Commonwealth has recommended Sellers serve 10 years.

**LOUISIANA**

Attorney General Buddy Caldwell’s High Technology Crime Unit arrested Christopher Ramos-Hernandez, charging him with 10 counts of possession of child pornography. The arrest was part of a joint investigation involving the Unit, the Iberia Parish Sheriff’s Office, the Louisiana State Police and Homeland Security Investigations. If convicted, Ramos-Hernandez faces up to 20 years in prison on each count.

**MARYLAND**

Attorney General Douglas Gansler’s Consumer Protection Division reached a settlement with Stanislav Komsky, the operator of Joomsef.net, a website publishing publicly available information on traffic citations issued against state consumers. The webpages exaggerated the traffic offenses by representing consumers as having been “booked” or arrested, and by displaying a blank space on each webpage reserved for a photograph of the consumer captioned “Mugshot Unavailable,” wrongly suggesting a mugshot had been taken. In order to have the information taken down, consumers had to pay Komsky from $39.99 to $89.99, depending on how rapidly they wanted it removed. Joomsef.net also required a fee of $9.99 to fully view the information about the “charged” offenses. The Division alleged Komsky engaged in unfair or deceptive trade practices. Under the settlement, Komsky has taken down the website, agreed to refund the payments he collected from consumers and will pay a $7,500 civil penalty to the Division.

**MASSACHUSETTS**

Attorney General Martha Coakley announced Stephen Megliola, manager of Cafeno’s Internet Café,
has entered a guilty plea to charges of organizing and promoting gambling services and operating an illegal lottery. Stephen Sheldon, the owner and other manager of the café and the corporation had previously pleaded guilty. Megliola was sentenced to two years of probation. The case was handled by Assistant Attorneys General Thomas Ralph and Timothy Wyse of Attorney General Coakley’s Cyber Crime Division and Assistant Attorney General Lee Heitinger. Attorney General Coakley’s Computer Forensic Laboratory, Senior Financial Investigator Mark Pulli, Department of Revenue investigator Thomas Nowicki and State Police assigned to Attorney General Coakley’s Office assisted in the investigation.

NEBRASKA

Attorney General Jon Bruning announced the sentencing of Eric Baker to five to seven years imprisonment for two counts of possession of child pornography; four to six years for one count of unlawful intrusion; and one year for one count of possession/distribution of obscene material. The sentences for possession of child pornography and possession/distribution of obscene material will run concurrently following completion of his sentence for unlawful intrusion. Baker used a hidden camera smartphone application to photograph an undressed minor female and other female victims and uploaded the photos on his computer hard drive.

NEW JERSEY

Acting Attorney General John Hoffman announced that John “Jay” Mulligan has entered a guilty plea to second-degree distribution of child pornography and fourth-degree possession of child pornography. Mulligan was among 27 defendants arrested last year under “Operation Watchdog,” a multi-agency investigation targeting offenders who distributed known images and videos of child pornography, which was led by the State Police and the Division of Criminal Justice. Under the plea agreement, the State will recommend Mulligan be sentenced to three years in state prison and 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. The Digital Technology Investigation Unit of the State Police coordinated the investigation, which also involved the Division and 19 other law enforcement agencies.

NEW MEXICO

Attorney General Gary King hosted a Safe School Summit with presentations and breakout sessions on such topics as bullying and current trends in child exploitation. The Summit was attended by school superintendents, teachers, health professionals, law enforcement personnel, government officials, school board members and other stakeholders. The keynote speaker was Dr. Joel Haber, a nationally known psychologist and author specializing in health psychology and bullying prevention.

NEW YORK

Attorney General Eric Schneiderman’s Office entered into Assurances of Discontinuance with 19 companies that agreed to cease writing fake consumer reviews and to pay more than $350,000 in penalties. “Operation Clean Turf,” a year-long investigation into the reputation management industry and the practice of astroturfing, found companies had posted thousands of fake consumer reviews on websites such as Yelp, Google Local and CitySearch in violation of state laws against false advertising and deceptive business practices. Some companies had even paid overseas freelance writers up to $10 per review. The companies signing the Assurances are A&E Wig Fashions, Inc. d/b/a A&E and NYS Surgical Center; A.H. Dental P.C. d/b/a Platinum Dental; Body Laser Spa Inc.; The Block Group, LLC d/b/a Laser Cosmetica and LC MedSpa, LLC; Bread and Butter NY, LLC d/b/a La Pomme Nightclub and Events Space; Envisions MT Corp.; iSEOiSEO; Medi-
OHIO
Attorney General Mike DeWine joined Cuyahoga County Prosecutor Timothy McGinty to announce a plea agreement in which VS2 Worldwide Communications, a New Jersey-based company providing computers and software to Internet sweepstakes cafes, will cease operations in the State after pleading guilty to felony charges related to operating a gambling enterprise and money laundering. In addition to VS2, four other defendants pleaded guilty: P & E Technologies Inc., Philip Cornick, Richard Upchurch and Michael Koty. Under the terms of the agreement, the defendants agreed to a civil forfeiture totaling $615,000 and to cease doing business. Their convictions also make them ineligible for jobs in the gaming industry in the State. The Ohio Department of Public Safety, Parma Heights Police Department, Cuyahoga County Sheriff’s Office, U.S. Secret Service and U.S. Postal Service assisted in the case.

OREGON
Attorney General Ellen Rosenblum’s Office entered into a settlement with Florida-based Best Brand Values and several related companies in which the companies agreed to refund more than $252,000 in improperly charged “membership fees.” The companies sold heavily discounted books, movies and other goods online, but when customers clicked on the “free shipping” icon, they were automatically enrolled in a shopping club and electronically billed a $10-$20/month fee. The companies do business through the following websites: Nuvalife.com, BestBrandvalues.com, DiscountBookSale.com, DiscountMovieSale.com, DiscountPosterSale.com, TopMusicZone.com, HotBookSale.com, HotMovieSale.com and SmartGameShopper.com. Attorney General Rosenblum’s investigators traced the websites to Robert Oesterlund and his manager Frederick Middleton in Florida. In addition to refunding customers, Best Brand Values agreed to pay $300,000 to the Department of Justice Protection and Education Account and to more clearly warn consumers about membership fees and make it easier to cancel the fees.

Pennsylvania
Attorney General Kathleen Kane’s Child Predator Section agents arrested Jesse Cross on seven counts of possession of child pornography, four counts of distribution of child pornography and one count of criminal use of a communications facility. The agents, who were conducting an online investigation into the sharing of child pornography, found numerous images of adolescents engaged in graphic sexual activity being shared from Cross’s computer. The State Police assisted with the arrest. The case will be prosecuted by Deputy Attorney General Anthony Marmo of the Section.

Rhode Island
Attorney General Peter Kilmartin joined the State Police and State Department of Transportation to kick off a statewide high school tour at a local high school to bring attention to the dangers of texting and driving. The assembly included a driving simulator showing how much texting affects a driver’s ability to maintain control of a vehicle, as well as an AT&T documentary featuring families impacted by texting and driving accidents. Students and faculty were then asked to sign a pledge not to text and drive, and more than 500 students took the pledge.

South Dakota
Attorney General Marty Jackley announced that a jury convicted Nathan Adams on one count of pos-
session of child pornography, a class 4 felony. The charges stemmed from a search warrant executed at his residence. The maximum penalty is 10 years in the state penitentiary and/or a $20,000 fine. The case was investigated by the Division of Criminal Investigation and prosecuted by Attorney General Jackley’s Office.

TEXAS

Attorney General Greg Abbott objected in federal bankruptcy court to the sale of online dating service True.com’s 43 million-member database. The database and web site are owned by True Beginnings, which filed for Chapter 11 bankruptcy protection and sought permission from the court to sell its assets, including the database and all information provided by True.com’s users, to a Canadian-based online dating service. Attorney General Abbott has argued the bankruptcy trustee must first give True.com’s members an opportunity to object to the sale of their personal information, as they were told their information would not be transferred at the time they joined the site.

VERMONT

Attorney General William Sorrell announced charges were filed against Michael Karlberg for one felony count of Promoting a Recording of Sexual Conduct by a Child and four felony counts of Possession of Child Pornography. The charges stem from a shared investigation between Attorney General Sorrell’s Office and the Vermont Internet Crimes Against Children Task Force and originated with a complaint received from the Austin, Texas Police Department. According to court documents, Karlberg recorded video chats with a juvenile in which the juvenile engaged in sexual conduct.

VIRGINIA

Attorney General Ken Cuccinelli joined Neil MacBride, U.S. Attorney for the Eastern District of Virginia, to announce that Lawrence Sayers entered a guilty plea to production of child pornography for pictures and videos he took of himself engaging in sexually explicit conduct with a minor. The Chesterfield Police Department had executed a search warrant at Sayers’ residence, recovering two cellular phones. A subsequent forensic examination revealed approximately 40 images and five videos of the conduct with the minor. Sayers faces a mandatory minimum sentence of 15 years’ imprisonment up to a maximum of 30 years. The case was investigated by the Police Department and the FBI. Assistant Attorney General and Special Assistant U.S. Attorney Thomas Johnstone is prosecuting the case on behalf of the United States.

WISCONSIN

Attorney General J.B. Van Hollen joined Dr. Julie Sprague, Horace Mann Middle School Principal, to host the State’s first “Good to Know” school road show, designed by Google to educate kids about how to stay safe online. The “digital citizenship” program was tailored specifically for the school’s age group.

CYBER NEWS BRIEFS

STUDY: ANDROID PRIME TARGET FOR MALWARE ATTACKS

Android, the most widely used mobile operating system, is by far the primary target for malware attacks, according to a study by the U.S. Department of Homeland Security and the FBI. The study found Android was a target in 79 percent of malware threats to mobile operating systems in 2012, with text messages representing one-half of the malicious applications. Android was found to be a prime target because many users are still using older versions of the software. The study can be accessed at http://publicintelligence.net/dhs-fbi-android-threats/.
FACEBOOK: GOVERNMENTS SOUGHT INFO ON 38,000 USERS

Governments sought information on more than 38,000 of Facebook’s more than one billion users, according to the “Global Government Requests Report,” the company’s first report on the scale of data inquiries it receives. U.S. law enforcement authorities were the most active, seeking information on between 20,000 and 21,000 users during the first half of 2013, representing a slight rise from their requests during the last six months of 2012. Facebook acknowledged it has partially complied with about 80 percent of those requests, noting it requires governments to meet a “very high legal bar” to receive user data. Authorities in other countries with large Facebook user bases, including India, the United Kingdom and Germany, also requested information on thousands of users. Facebook said it would begin to publish information on data requests on a regular basis.

And see...

Yahoo published its first transparency report outlining global government data requests received during the first half of 2013. Notably, Tumblr statistics were not included, with Yahoo saying it will issue a separate report for its recent addition. The report shows 12,444 requests from U.S. law enforcement, impacting 40,322 user accounts. Yahoo said it provided “non-content” user data, including email addresses, names, locations, IP addresses, login details and billing information, for 6,798 of the requests. User-created content, including emails, Flickr uploads and data from Yahoo Answers, was released for 4,604 of the requests. Yahoo also turned down 241 requests, and was unable to come up with any relevant data in 801 requests. Germany had the second highest number of requests with 4,295 data requests. Yahoo said it will publish transparency reports every six months.

STUDY: DEMAND UP FOR DIGITAL CONTENT AT LIBRARIES

Libraries are experiencing a sharp increase in demand for electronic material, and are spending more of their available funding on ebooks, online databases and other electronic products, according to a study released on September 4 by Information Today Inc. The study, sponsored by ProQuest, was based on 796 responding library managers and librarians and was conducted by the Library Resource Guide and Unisphere Research, the market research arm of Information Today. While responding libraries still spend the largest chunk (37 percent) of their budget on printed books, that percentage decreased from the previous two years (39 percent in 2011 and 2012). The same libraries reported spending 29 percent on online databases (up from 25 percent in 2012 and 19 percent in 2011) and six percent on ebooks (up from three percent in 2011 and 2012). Sixty percent of the libraries said they plan on increasing digital access and availability of online publications in 2014. The study may be accessed at http://libraryresource.onlineinc.com/Downloads/ResearchReports/.

PEW STUDY: ANONYMITY ONLINE IMPOSSIBLE

Almost 60 percent of polled Internet users do not believe it is possible to remain completely anonymous on the Internet, according to a Pew Research Center study. In fact, more than 85 percent of those surveyed have taken steps to remove or mask their digital footprints, such as by clearing cookies, encrypting email, not using their real names online and hiding their IP addresses. Of those surveyed, 59 percent said everyone should have the ability to search the Internet anonymously, a view most strongly held by young adults, who were also the most likely Internet users to try to remain anonymous online. Those with a college or graduate school education were also more concerned about online privacy than those with less education. Priva-
cy concerns are on the rise, with one-half of those polled saying they were worried about their online privacy, up from 33 percent in 2009. However, only five percent said they are trying to hide their activities from the government, and only four percent said the same of law enforcement. Most Internet users said they are just trying to protect themselves from criminals, marketers and people from their past. The report may be accessed at http://www.pewinternet.org/Reports/2013/Anonymity-online.aspx.

NIST TO REOPEN ENCRYPTION VETTING PROCESS

The National Institute of Standards and Technology (N.I.S.T.), the federal agency responsible for recommending cybersecurity standards, announced it would reopen the public vetting process for an encryption standard. The announcement followed reports published by the New York Times, the Guardian and ProPublica about the National Security Agency’s (N.S.A.’s) success in foiling much of the encryption protecting vast amounts of information on the Internet. For encryption to be secure, the system must generate secret prime numbers randomly. That random number generation process is based on mathematical algorithms, making it practically impossible to predict the scrambling protocols necessary to unscramble an encrypted message. Because of cryptographers’ concerns, N.I.S.T. will reopen the public content period for three publications – Special Publication 800-90A and drafts of Special Publications 800-90B and 800-90C – all of which use the random number generator in question.

REPORT: ONLINE PIRACY UP BY 159.3 PERCENT

Online infringement in North America, Europe and Asia-Pacific increased by 159.3 percent between 2010 and 2012, according to a report commissioned by NBC Universal and produced by Net-Names, a U.K. company managing online brands. The report, “Sizing the Piracy Universe,” found 327 million unique Internet users sought to access infringing content in January 2013 alone, an increase of 9.9 percent from November 2011. The study examined a range of intellectual property infringement, including books, music, movies, video games and software. It found piracy is often carried out through one of three methods – a BitTorrent protocol, video streaming or a direct-download cyberlocker, such as Mediafire or Piratebay. The report had some good news as well – data showed the prosecution and shutdown of cyberlocker MegaUpload in January 2012 decreased the use of direct-download services by infringers by 7.7 percent. Page views for the cyberlockers also decreased by 40.6 percent. The report may be accessed at https://s3.amazonaws.com/www2.itif.org/panelists+powerpoints/2013-netnames-piracy.pdf.

STUDY: OPT-OUT IN ONLINE ADVERTISING ESSENTIAL

TRUSTe, an online privacy management company, released its 2013 privacy study of consumer views about online advertising and tracking. The study found 91 percent of respondents said privacy is important, with 64 percent acknowledging they were more concerned about privacy now than in the past. As for online shopping, 53 percent of respondents said they are more willing to “click” on ads with opt-out options, while 33 percent said they have stopped shopping with a brand because of privacy concerns. The study may be accessed at http://www.truste.com/uk-advertising-privacy-index-2013/.

FREE CONSTITUTION APP NOW AVAILABLE

A free app of the Constitution Annotated was released in honor of Constitution Day by the U.S. Senate Committee on Rules and Administration, the Library of Congress and the U.S. Government Printing Office. In its original non-digital form, the Constitution Annotated runs 2,860 pages, weighs 10
pounds and costs $290. The app is available from iTunes for iPhones and iPads and includes case law and analysis. An Android version is under development.

PHILLY BAR WEIGHS IN ON EMAIL OF FORMER PARTNER

The Philadelphia Bar Association Professional Guidance Committee issued an ethics opinion in a dispute over a law firm’s handling of email sent to the account of a former partner. According to Opinion 2013-4 issued on September 13 authorizing the firm to read the incoming mail, the former partner had no right to insist the account simply be closed and set to a bounce-back message to that effect. However, the opinion determined any email related to matters the partner took with him to his new firm must be forwarded by his old firm, and replies to email senders had to provide the ex-partner’s new contact information. Further, the opinion noted “the inquirer is reminded that considerations of substantive law may influence this analysis. Although the Committee does not address those considerations here, relevant points to consider may include the firm’s partnership agreement, any sidebar agreements with [the ex-partner] concerning the latter’s withdrawal and/or the firm’s written or customary employment practices.” The opinion may be accessed at http://www.philadelphiabar.org/WebObjects/PBReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion2013-4.pdf.

STUDY: AVERAGE COST OF CYBERCRIME UP $3 MILLION/YR

The average annualized cost of fighting cybercrime for a large U.S. company has grown to $11.56 million per year, up from $8.9 million in 2012, according to an annual report conducted by the Ponemon Institute, a data privacy and protection think tank. The “2013 Cost of Cybercrime Study: United States” is the fourth edition of the study and was sponsored by HP Enterprise Security. The costs could actually be much higher, because the study does not monetize the value of the information lost in cyberattacks or the resulting damage to a company’s reputation. The number of digital attacks also increased – up 18 percent from the 2012 study. The most costly attacks measured in the study were denial of service, malicious insider and web-based attacks, accounting for more than 55 percent of cybercrime costs per organization annually. The study found many companies are falling prey to sophisticated and targeted attacks, such as “spear-fishing,” in which cybercriminals send personalized emails to employees of a company, often after gathering personal information about the employees from social media pages to better target them. The report may be accessed at http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.

CAN LAWYERS OFFER Groupon-TYPE DEALS? ABA WEIGHS IN

On August 12, the American Bar Association (ABA) House of Delegates passed a resolution calling on federal, state and local governments to enact strong laws combating unauthorized intrusion into lawyers’ computers and networks. The resolution also urged lawyers and law firms to do their part to preserve their clients’ confidentiality by keeping abreast of technological advances and complying with cybersecurity safeguards. It also urged the U.S. government to work with other nations to create “legal mechanisms, norms and policies” punishing and deterring cyberattacks against law firms and lawyers, and encouraged lawyers to keep their clients reasonably informed in the event of a breach. The resolution may be accessed at http://www.americanbar.org/content/dam/aba/directories/policy/2013_hod_annual_meeting_118.docx.

FOUR NEW FOREIGN SCRIPT DOMAINS BUILT
The first four of a total planned 1,400 new generic top-level domains (“GTLDs”) have been added to the root servers holding the master list of Internet addresses. The new domains are the first non-Latin character domains and consist of the Chinese word for game, the Arabic word for Web or network and the Russian words for online and website. The new domains are not yet live, since there is now a “sunrise period” of at least 30 days during which trademark holders can register addresses using their own trademarks. The years-long process is overseen by the International Corporation for Assigned Names and Numbers (ICANN) amid concerns about trademark protection.

IN THE COURTS

CONSENT TO SEARCH: ANSWERING INCOMING CELL CALLS

U.S. v. Lopez-Cruz, 2013 U.S. App. LEXIS 18930 (9th Cir. September 12, 2013). The Ninth Circuit Court of Appeals concluded defendant’s consent to search his cell phone did not extend to answering incoming calls. Andres Lopez-Cruz gave a border patrol agent consent to look in and search his two cell phones, but the agent answered an incoming phone call and passed himself off as Lopez-Cruz. Lopez-Cruz challenged the search and moved to suppress evidence obtained during the search. The U.S. District Court for the Southern District of California granted the motion and then denied the government’s motion for reconsideration. The government appealed, and the appeals court affirmed, finding Lopez-Cruz’ consent to search his cell phone did not extend to answering incoming calls.

READING ONLINE CHAT TRANSCRIPT ALOUD: “DOING THEATER” CLAIM

U.S. v. Tragas, 2013 U.S. App. LEXIS 17628 (6th Cir. August 23, 2013). The Sixth Circuit Court of Appeals found it not improper for the prosecutor and a witness to read properly admitted transcripts of online chat conversations aloud to the jury. Joanna Tragas was charged with conspiracy to commit access device fraud and related bank and wire fraud offenses. At her trial, the U.S. District Court for the Eastern District of Michigan admitted a transcript of the online chats between Tragas and her co-conspirators, but in addition, the prosecutor and a Secret Service agent witness read several of the chats aloud to the jury. After her conviction, Tragas appealed, arguing the prosecution had made a “remarkable departure from traditional American trial practice” by “doing theater” at the trial. The appeals court, while cautioning about the dangers of “performing” transcript evidence for the jury but finding no showing of prejudice, ultimately affirmed “the mere reading aloud of previously admitted documentary evidence.

WARRANTLESS PLACEMENT OF GPS: FEDERAL PRECEDENT

Taylor v. State, 2013 Tex. App. LEXIS 10923 (August 28, 2013). The Texas Court of Appeals, Seventh District, found at the time a GPS unit was placed on defendant’s vehicle, several courts had approved the wireless installation and monitoring of GPS devices. Joseph Taylor pled guilty to possession of marijuana and then appealed, arguing the trial court erred in denying his motion to suppress because the authorization to install and monitor a GPS tracking device on the vehicle he was driving was in contravention of state and federal law. The state appeals court decided that based on the state of the law as it existed when the device was installed, and even assuming a Fourth Amendment violation occurred, the evidence would not have been subject to the exclusionary rule because offic-

But see...

*People v. LeFlore*, 2013 IL App. LEXIS 636 (September 17, 2013). The Illinois Court of Appeals, Second District, found defendant had standing to challenge the placement of the GPS device on his vehicle. Keith LeFlore was found guilty of aggravated robbery, robbery and burglary. He appealed, arguing the trial court erred in denying his motion to suppress evidence obtained from the covert placement of a GPS device on his vehicle. The appeals court found LeFlore had borrowed the vehicle with the owner’s consent, and therefore had standing to challenge the State’s use of the GPS device or any evidence obtained from that use, despite the fact LeFlore was not in possession of the vehicle when the GPS was installed. The court also found LeFlore’s status as an unlicensed driver did not necessarily defeat his expectation of privacy in the owner’s vehicle. The judgment was reversed and the case remanded.

**SEARCH OF ALL COMPUTER EQUIPMENT: OVER-SEIZING CHARGE**

*U.S. v. Schesso*, 2013 U.S. App. LEXIS 19256 (9th Cir. September 18, 2013). The Ninth Circuit Court of Appeals found the warrant to search all of defendant’s computer equipment was not overbroad. The government appealed an order of the U.S. District Court for the Western District of Washington granting defendant Joseph Schesso’s motion to suppress all evidence seized from his residence. The appeals court found the warrant authorizing an electronic search of all of Schesso’s computer equipment and digital storage devices was not overbroad and did not raise the risks inherent in over-seizing. The court further found no violation of the Fourth Amendment, as evidence showing Schesso possessed and distributed a child pornography video on a peer-to-peer file-sharing network provided probable cause to search his entire computer system and digital storage devices for any evidence of possession of or dealing in child pornography. The court acknowledged the government had no way of knowing which or how many illicit files there might be or where they might be stored. Therefore, the court determined there was probable cause to believe Schesso was a child pornography collector, making his entire computer system and all of his digital storage devices suspect. The court reversed the grant of the motion to suppress.

**FIRST AMENDMENT: FACEBOOK “LIKE”**

*Bland v. Roberts*, 2013 U.S. App. LEXIS 19268 (4th Cir. September 18, 2013). The Fourth Circuit Court of Appeals held former employees who used Facebook “likes” to show their support had viable First Amendment free expression claims. Bobby Bland and five other co-workers in the Hampton, Virginia Sheriff’s Department sued Sheriff B.J. Roberts, alleging wrongful termination due to their support of his opponent in Sheriff Roberts’ re-election campaign. Three of the former employees showed their support of his opponent by “liking” the opponent’s Facebook page. Sheriff Roberts filed a motion for summary judgment, arguing there was insufficient evidence for their First Amendment claims and stating the employees were fired due to poor job performance. The U.S. District Court for the Eastern District of Virginia granted the motion, holding “liking” an opponent’s Facebook page was not speaking out, and therefore the employees did not sufficiently engage in expressive speech. On appeal, the Fourth Circuit held the Facebook “like” was speech protected by the First Amendment, and those former employees had raised a material issue of fact as to whether they were terminated for that speech. However, the court found their claims against Sheriff Roberts in his personal capacity were
barred by the doctrine of qualified immunity and the Eleventh Amendment. The court did find their claims for reinstatement to their prior positions could proceed because the Eleventh Amendment does not bar prospective relief. The court remanded the case to proceed to trial on the claims for reinstatement, and affirmed dismissal of all other claims.

**ONE ACT, ONE CRIME: POSSESSION OF DUPLICATE IMAGES**

*People v. Sedelsky*, 2013 IL App. 2d f11042 (September 26, 2013). The Illinois Appellate Court, Second District, found only one conviction of possessing child pornography could be entered. Bryan Sedelsky was convicted of three counts of possession of child pornography. He appealed, arguing that one count should be vacated because it was based on possession of an identical image stored on the same storage medium although under a different file name. The court acknowledged the statute was unclear as to whether the simultaneous possession of a duplicate depiction by computer could constitute a separate offense of possessing child pornography. Therefore, the court adopted a construction favoring Sedelsky, finding only one conviction could be entered for his possession of the same digital image stored in the same medium under the one-act, one-crime rule. The court reversed, vacated conviction on the third count and vacated the corresponding sentence and affirmed the other convictions.

**FOURTH AMENDMENT: SEARCH BY STORE TECHNICIAN**

*U.S. v. Tosti*, 2013 U.S. App. LEXIS 20008 (9th Cir. October 1, 2013). The Ninth Circuit Court of Appeals ruled suppression under the Fourth Amendment was not warranted. Donald Tosti took his computer to CompUSA for service. The technician working on Tosti’s computer encountered images appearing to be child pornography and called police. The responding officers directed the technician to open those images for the officers to scroll through. The officers seized the computer and also obtained and executed a search warrant on Tosti’s residence. Tosti’s estranged wife, who was living in the house, consented to the search and turned over a computer, several hard drives and numerous DVDs, all of which were not password protected and appeared to contain pornography. Tosti was arrested and charged with possession of child pornography. He moved to suppress the evidence from the search of his computer at CompUSA and the search of his home office, both of which were denied by the U.S. District Court for the Northern District of California. He appealed, arguing a violation of his Fourth Amendment rights. The appeals court held the search of his computer at CompUSA to be lawful because the police officers who conducted it did not exceed the scope of the permissible search already conducted by the technician, a private party. The court also found the search of Tosti’s home office to be lawful, because his wife had apparent, if not actual, authority to consent to the search. Tosti’s conviction was affirmed.

He moved to dismiss his indictment for failure to state an offense, arguing his alleged statement did not constitute a threat under 18 U.S.C. § 875©. The U.S. District Court for the Western District of Pennsylvania denied the motion, determining a reasonable jury could find Stock’s statement to be a threat. He appealed, but the appeals court, agreeing that a jury could find the posting to be a threat, affirmed.

**ONLINE POSTINGS: DEFINITION OF “THREAT”**

*U.S. v. Stock*, 2013 U.S. App. LEXIS 17737 (3rd Cir. August 26, 2013). The Third Circuit Court of Appeals ruled the statements in the online posting constituted threats. Adrian Stock was indicted for knowingly and willfully communicating a threat to injure another person. Specifically, Stock had posted a statement perceived as a threat on Craigslist.
LEGISLATIVE UPDATE

POSSESSION OF CHILD PORNOGRAPHY
CALIFORNIA. On October 12, Governor Jerry Brown signed SB 145 into law, increasing the penalties for possession of child pornography. The legislation, chaptered as Chapter 777, increases penalties for offenders who possess more than 600 images of child pornography involving at least 10 images of children 12 years old or younger, those who possess images of children forced to endure sadism or masochism and those who send child pornography images to a child with intent to “groom” the child into engaging in sexual conduct.

TEXTING WHILE DRIVING
FLORIDA. On October 1, Florida became the 41st state to prohibit texting while driving. However, unlike many other states, violation of the Florida law is a secondary offense, meaning an officer will first have to witness another offense, such as swerving or running a stop sign, in order to ticket the texter. The Florida law also permits texting while stopped at a red light or if using a talk-to-text device, such as the iPhone Siri. The penalties are $30 plus court costs for a first offense and $60 for a second offense.

REMOVAL OF MINORS’ ONLINE INFORMATION
CALIFORNIA. On September 23, Governor Jerry Brown signed SB 564 into law, requiring an Internet service provider to permit a minor to request removal of content posted on the provider’s website. The law, codified as Chapter 336, also bans website operators from marketing certain goods, such as guns, ammunition, alcohol, tobacco and dietary products, to Internet users under 18 years of age. The law becomes effective on January 1, 2015.

ONLINE TICKET SALES
CALIFORNIA. On September 23, Governor Jerry Brown signed AB 329 into law, making it a misdemeanor to use software to circumvent the security of ticket-selling websites in order to purchase large numbers of tickets. Penalties are up to six months in jail and special civil fines of up to $2,500.

USE OF HANDHELD CELL PHONES WHILE DRIVING
MARYLAND. On October 1, the use of handheld cell phones while driving is prohibited, except to call or text 911 in the event of an emergency. A first-time offender will be fined $75; a second offense will cost $125; and the fine is $175 for a subsequent offense.

REVENGE PORN
CALIFORNIA. On October 1, Governor Jerry Brown signed SB 255 into law, making it a misdemeanor to take private, explicit photos of individuals and then circulate such photos online without consent with the intent to harass or humiliate, a practice known as revenge porn. A conviction is punishable by up to six months in jail and a $1,000 fine for the first offense.

SOCIAL MEDIA PRIVACY
FLORIDA. On September 25, SB 198, a bill prohibiting an employer from requesting or requiring access to a social media account of a current or prospective employee, was introduced. The bill would also prohibit an employer from taking retaliatory action if an employee fails to provide such access or from refusing to hire a prospective employee who does not provide such access. If enacted, the legislation would become effective on October 1, 2014. The bill was referred to the Commerce and Tourism, Governmental Oversight and Accountability, Judiciary and Rules Committees.
NEW PUBLICATIONS AND WEBSITES

CRIMINAL JUSTICE RESEARCH

The National Institute of Justice (NIJ) released the 11th issue of “Research Report Digest,” an online publication providing brief descriptions of studies in many criminal justice disciplines, such as crime, violence and forensic sciences. It also includes evaluations of technologies used by law enforcement. It can be accessed at http://nij.gov/publications/digest/issue11.htm.

CYBERCRIME INVESTIGATION TOOLS


CRIME SCENE INVESTIGATION GUIDE