The following is a compendium of news reports, case law and legislative actions over the latest bi-monthly period that may be of interest to our AG offices that are dealing with cyber-related issues. Neither the National Association of Attorneys General nor the National Attorneys General Training & Research Institute expresses a view as to the accuracy of news accounts, nor as to the position expounded by the authors of the hyperlinked articles.

NOVEMBER-DECEMBER 2014 ISSUE

Bipartisan Cybersecurity Legislation Finally Enacted
On December 18, 2014, President Obama signed into law S. 1353, the Cybersecurity Enhancement Act of 2014, giving the National Institute of Standards and Technology (NIST) authority to develop voluntary standards for securing the nation’s critical infrastructure with public-private partnerships. NIST is also directed to coordinate a national cybersecurity awareness and education program to 1) disseminate technical standards and best practices usable by individuals, businesses, educational institutions and state and local governments; 2) increase public awareness and understanding of cybersecurity; 3) support education programs; and 4) evaluate workforce needs. Finally, NIST is required to ensure the coordination of federal agencies engaged in developing international technical standards for information system security.

In addition to the requirements for NIST, the bipartisan legislation also directs federal government agencies to develop, and update every four years, a federal cybersecurity research and development strategic plan. The U.S. Departments of Commerce and Homeland Security and the National Science Foundation are also charged with supporting competitions to recruit information technology security personnel and stimulate cybersecurity innovations.

Attorneys General Fighting Cybercrime
Fifty-one Attorneys General, the Federal Trade Commission (FTC) and the Federal Communications Commission reached settlements with T-Mobile USA Inc., resolving allegations T-Mobile placed unauthorized charges for third party services on consumers' mobile phone bills, a practice known as "cramming." Under the settlement, T-Mobile must provide each victim filing a claim under its Premium SMS Refund Program with an opportunity for a full refund. T-Mobile must pay at least $90 million, with at least $67.5 million paid to consumers, $18 million to the Attorneys General and $4.5 million to the FTC. The settlement also requires T-Mobile to stay out of the Premium Short Message Services (PSMS) business and must obtain consumers' express consent before billing third party charges, must provide an opportunity for full refund if consumers are billed for unauthorized third party charges, must inform new customers about third party charges and must clearly distinguish such charges on all customer bills. The signatory Attorneys General represent the 50 states and the District of Columbia.

Forty-six Attorneys General entered into a $3.8 million settlement with satellite radio company Sirius XM Radio Inc., resolving claims the company engaged in misleading advertising and billing practices. Sirius XM was alleged to have failed to honor contract cancellations or made it difficult to cancel contracts, automatically renewed contracts without obtaining consent or providing notification, charged consumers unauthorized fees, failed to provide timely refunds and increased rates after enticing consumers with low introductory rates. The settlement requires Sirius XM to clearly disclose all terms and conditions at the point of sale, to refrain from misrepresenting plans in advertising and to provide advance notice about automatic renewals. Further, Sirius XM will revise its cancellation procedures to make cancellation easier. The Executive Committee for the settlement was led by Ohio and was comprised of Arizona, Connecticut, Tennessee, Vermont and Washington, D.C. Jurisdictions joining the settlement were: Alabama, Alaska, Arkansas, Colorado, Delaware, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, North Dakota, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Texas, Utah, Virginia, Washington, West Virginia and Wisconsin.

Six Attorneys General entered into a settlement with PointRoll, Inc., a digital advertising and technical services company owned by Gannett Corp., resolving allegations the company violated consumers' privacy by unlawfully
 circumventing privacy settings in Apple Inc.’s Safari browser. Those settings would have otherwise blocked cookies from third parties or advertisers. Under the settlement terms, PointRoll is prohibited from engaging in practices to override cookie blocking settings in order to gather consumers’ information. The company must also implement a privacy program within six months to include employee training on the importance and maintenance of privacy. Finally, the company must ensure its servers are configured to instruct Safari browsers to expire any cookie placed by PointRoll using its circumvention technique. New Jersey led the Executive Committee investigating PointRoll, with the other signatory states being Connecticut, Florida, Illinois, Maryland and New York.

Five Attorneys General hosted a forum on transnational cybercrime with attorneys general and prosecutors from El Salvador; Guanajuato, Mexico; and Veracruz; as well as representatives of the U.S. Department of Justice, the U.S. Department of Homeland Security and the FBI. The group discussed multi-jurisdictional investigations of complex computer crimes, forensic and technical investigations of cyber offenses and credit card fraud. The participating Attorneys General were those representing Florida, Idaho, Indiana, Montana and Utah.

Alabama Attorney General Luther Strange announced a favorable decision by the Alabama Supreme Court involving electronic bingo. That court held the trial judge correctly ordered illegal slot machines and gambling devices seized by law enforcement destroyed and the money and records forfeited to the State. The case is Houston County Economic Development Authority v. State of Alabama, No. 1130388.

Attorney General Tom Horne announced the conviction of Jonathan Sanborn and his business, IQ Vending LLC, on charges of felony gambling, conspiracy and running an illegal enterprise. Sanborn placed “redemption” machines in retail stores across the State which, although appearing to be video games, were actually illegal gambling devices offering expensive prizes. A whistleblower reported the machines were set so hundreds of players had to lose prior to a win, and this report was later confirmed during a forensic analysis. An investigation ensued, and agents executed search warrants and seized more than 20 devices found to violate state gambling laws. Sanborn and IQ Vending were ordered to pay a fine proportional to the revenue received, as well as repay the State’s investigation costs. Sanborn was sentenced to two years of felony probation.
Arkansas Attorney General Dustin McDaniel’s Cyber Crimes Unit agents arrested Kenneth Lafkin on 30 counts of possession of child pornography, a Class C felony. The agents executed a search warrant at Lafkin’s residence and seized a desktop computer, two laptops and other electronic devices, all of which will be analyzed at the Unit’s Forensic Lab. The investigation was initiated by Special Agent Chad Meli, and the Mississippi County Sheriff’s Office and Keiser Police Department participated in the investigation and arrest.

Delaware Attorney General Beau Biden announced the arrest of Michael Motto pursuant to an undercover investigation by the Delaware Child Predator Task Force. Motto was charged with one count of attempted solicitation of a child, one count of attempted sexual exploitation of a child and 25 counts of dealing in child pornography. The online investigation involved monitoring chatrooms and communications between Motto and an undercover investigator, and a subsequent search warrant executed post-arrest found images of child pornography.

Florida Attorney General Pam Bondi’s Office and the Federal Trade Commission filed a complaint against Inbound Call Experts, LLC, d/b/a Advanced Tech Support; Super PC Support, LLC; and related entities operating multi-million dollar schemes to sell tech support services nationwide. Defendants allegedly offered to perform a free diagnostic check which falsely found infections on consumers’ computers and could only be resolved manually by a technician. Consumers paid hundreds of dollars for unnecessary repairs and long-term maintenance programs. The complaints seek a permanent injunction to prevent future deceptive trade violations, restitution and attorneys’ fees.

Hawaii Attorney General Russell Suzuki announced the Hawaii Criminal Justice Data Center (HCJDC), a division of his Office, was awarded the Web Marketing Association’s Best Information Services Mobile Application of 2014 for its “Hawaii Sex Offender Search” mobile app. HCJDC partnered with the Hawaii Information Consortium, LLC to create the app, which allows users to locate the residence and business addresses of sex and other covered offenders, as well as view offenders residing or working in relation to the user’s location. It also provides users with the offender’s photo and convictions.

Illinois Attorney General Lisa Madigan’s investigators and the Vandalia Police Department arrested Ryan Koontz after executing a search warrant at his
home. Koontz is charged with two counts of distribution of child pornography, a Class X felony punishable by six to 30 years in prison; and eight counts of possession of child pornography, a Class 2 felony punishable by three to seven years in prison.

**Kentucky Attorney General Jack Conway** announced the conviction of Edgar Purdom on four counts of distribution of child pornography and one count of possession of child pornography. The verdict culminates an investigation by Attorney General Conway's Cybercrimes Unit.

**Louisiana Attorney General Buddy Caldwell's** Cyber Crime Unit joined the Vernon Parish Sheriff's Office and Homeland Security Investigations to arrest Charles Stauffer on five counts of possession of child pornography. If convicted, he faces up to 20 years in prison on each count.

**Maryland Attorney General Douglas Gansler's** Consumer Protection Division entered into a settlement agreement with Verizon over allegations the company misrepresented the actual cost consumers were charged for FIOS television, Internet and phone services. Under the settlement, Verizon agreed to pay an estimated $1.375 million in restitution to State consumers who were allegedly either improperly charged termination fees or paid equipment fees not adequately disclosed in Verizon's advertising. Verizon will directly provide such restitution to eligible current customers, and the Division will notify those who are not current customers. Verizon will also pay the Division a civil penalty of $250,000 and $75,000 in costs. Verizon also agreed to change its price advertising to accurately inform consumers the actual cost to use products and must now provide clearer written disclosures of the terms of their orders and give customers broader cancellation rights if their bills do not accurately reflect their orders. Verizon will also honor all price guarantees, allow customers who do not receive the promotional price to cancel without penalty and not offer promotions it cannot deliver.

**Massachusetts Attorney General Martha Coakley** announced Boston Children's Hospital (BCH) agreed to take steps to prevent future security violations following allegations related to a data breach of patient information. The consent judgment alleges BCH failed to protect the personal information of more than 2,000 patients. According to the complaint, an unencrypted BCH laptop was stolen from a BCH physician speaking at a conference in Buenos Aires. Under the terms of the consent judgment, BCH will pay $40,000, including a $10,000 civil
penalty and a payment of $10,000 to a fund administered by Attorney General Coakley's Office for educational programs on the protection of personal information. BCH will also ensure data security law compliance by taking steps to properly track and physically secure portable devices and by training its workforce on the proper handling of personal information. BCH will also review and audit security measures and take necessary corrective action. The BCH case was handled by Assistant Attorney General Shannon Choy-Seymour of the Health Care Division.

**Mississippi Attorney General Jim Hood** announced the arrest of Roderick Arrington of North Carolina on 10 counts of cyberstalking. Arrington allegedly created fake Yahoo email accounts from which he allegedly sent repeated threatening emails. Arrington was arrested at his workplace by the Rockingham and Hamlet Police Departments pursuant to an investigation by Attorney General Hood's Cyber Crime Unit. If convicted, he faces up to 20 years in prison.

**Acting New Jersey Attorney General John Hoffman** announced Abraham Baruchov pleaded guilty to purchasing and receiving $275,000 worth of stolen coffee makers and other appliances and reselling them on such websites as eBay and Amazon. Baruchov purchased the goods online from a major retailer with stolen credit card information. The retailer's investigators traced the stolen goods to Baruchov and referred the case to Attorney General Hoffman's Division of Criminal Justice. Under the plea agreement, Baruchov must pay $275,000 in restitution to the retailer, and the State will recommend a sentence of three to five years in prison. The investigation was conducted by the Division's Financial & Computer Crimes Bureau. Deputy Attorneys General Janet Bosi and Naju Lathia prosecuted the case, and the lead detective was Detective Abraham Aquino of the Bureau.

**New York Attorney General Eric Schneiderman's Office** filed suit and won a temporary restraining order prohibiting KMG Direct, Inc.; High Life USA, LLC; and owner Eli Kreiger from selling synthetic drugs and street drug alternatives. Based on information from the Colorado Attorney General's Office, Attorney General Schneiderman's senior investigators found the companies selling designer drugs and drug paraphernalia in online storefronts and head shops. The suit seeks an accounting of all commodities sold or offered for sale by the companies and a permanent injunction barring the companies from selling misbranded designer drugs. The investigation was conducted by investigators David Burke, Dennis Churns and Chad Shelmidine; Supervising Investigators Richard Doyle and Chris
Holland and Deputy Chiefs of Investigations Antoine Karam and Jonathan Wood. The case is being jointly prosecuted by Assistant Attorney General Judith Malkin and Assistant Attorneys General in Charge Vincent Bradley and Deanna Nelson.

**Ohio Attorney General Mike DeWine**'s Bureau of Criminal Investigation (BCI) and Charitable Law Section investigators served search warrants on six businesses suspected of operating as illegal casinos. The warrants were served at five Talk n’ Win locations and one Surf’s Up site, and electronic gaming machines were removed from each one. Electronic gaming devices with cash payouts meet the definition of slot machines under State law and cash prize payouts are only permissible at regulated casinos and racinos. The Defiance County Multi-Area Narcotics Task Force; the Findlay, Fremont, Oregon and Toledo Police Departments; the Hancock County Sheriff’s Office, METRICH Enforcement Unit, Ohio Casino Control Commission and the Ohio Bureau of Workers Compensation assisted in serving the warrants.

**Pennsylvania Attorney General Kathleen Kane** announced 110 charges against Jeremy Godin who allegedly recorded nude children inside his home and distributed the child pornography via his cellphone. Attorney General Kane’s Child Predator Section agents identified an IP address on a peer-to-peer network making alleged child pornography files available for download. Agents traced the address to Godin, who is charged with four counts of production of child pornography, one count of distribution of child pornography, 100 counts of possession of child pornography, four counts of invasion of privacy and one count of criminal use of a communication facility.

**Rhode Island Attorney General Peter Kilmartin** announced Joseph Simone, a former wrestling coach, pled nolo contender to child pornography, indecent solicitation of a minor, extortion and impersonating police officers. Impersonating a teenage girl, he sought out high school boys on social media sites and enticed them to send explicit images and videos of themselves. If the boys sought to end the online relationship, he would threaten to post their explicit videos on Facebook. A parent of one of the victims notified the State Police, who investigated the matter. Under the plea agreement, Simone was sentenced to 10 years, with one year to serve at the ACI, two years on home confinement and the remainder suspended on probation. He was ordered to undergo sex offender counseling, is subject to sex offender registration and his Internet and computer access was
severely restricted for the duration of his sentence. Assistant Attorney General Ronald Gendron, Chief of the White Collar Crime Unit, prosecuted the case.

Texas Attorney General Greg Abbott entered into an agreement resolving the State’s enforcement action against operators of an online scheme falsely claiming to offer free credit scores, but actually billing consumers a $29.95 monthly fee for a credit monitoring program they never ordered. One Technologies, LP d/b/a ScoreSense, One Technologies, Inc. and MyCreditHealth; One Technologies Management, LLC; and One Technologies Capital, LLP are required to make clear disclosures to customers about the monthly fee and negative option trial, must cease misrepresenting credit scores are free and have to monitor their advertising affiliates to ensure they comply with the agreement. The companies will also pay $400,000 to the State, with $250,000 to be disbursed to the General Revenue or Supreme Court Judicial Fund and the rest for reimbursement of legal fees.

Vermont Attorney General William Sorrell announced the arraignment of Neil Dragoon on five felony counts of Promoting Child Pornography. According to court documents, Dragoon obtained and distributed child pornography using peer-to-peer file-sharing programs. The charges stem from an investigation by Attorney General Sorrell’s Office, the State Police, the Burlington Police Department, Homeland Security Investigation and the State’s Internet Crimes Against Children Task Force.

Wisconsin Attorney General J.B. Van Hollen announced Michael Scholler was charged with 14 counts of possession of child pornography pursuant to an investigation by Attorney General Van Hollen’s Office. The investigation began after receipt of a National Center for Missing and Exploited Children CyberTipline report of a Facebook post containing child pornography. Search warrants for Facebook and Gmail were executed, leading to the arrest of Scholler, who was a registered sex offender and on parole for second degree sexual assault. A cellphone containing images of child pornography was also located at Scholler’s home. The Waushara Sheriff’s Office and the Wild Rose Police Department, members of the Wisconsin ICAC Task Force, assisted with the investigation.

Cyber News Briefs

Data Breach Study: More U.S. Companies Have Response Plans
The Experian Data Breach Resolution Group released the findings of its second annual study on data breach preparedness. The study, conducted by the Ponemon Institute, surveyed 567 U.S. executives, finding 73 percent of companies now have data breach response plans in place, compared to 61 percent of companies polled in 2013. However, only 30 percent of executives believed their companies were “effective” or “very effective” in developing and executing a data breach plan. Further, 43 percent of executives said their companies had experienced a data breach in the last 12 months, compared to 33 percent in 2013. The study also found 48 percent of executives had increased spending on cybersecurity technology over the last 12 months, and the number of organizations purchasing cyber insurance policies more than doubled, with 26 percent of companies buying a policy compared with just 10 percent in 2013. The study may be accessed at http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf.

Pew Survey: Americans Concerned About Privacy
A survey on perceptions of privacy and security by the Pew Research Internet Project found 91 percent of American adults feel consumers have lost control of how personal information is collected and used by companies. Further, 64 percent think the government should do more to regulate advertisers. Across the board, the survey found a universal lack of confidence in the security of everyday communication channels, with 81 percent feeling not at all secure sharing information on social media sites, and 57 percent feeling insecure about sending private information via email. The survey was conducted by the GfK Group using KnowledgePanel among a sample of 607 adults. The survey report may be accessed at http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/.

NIST Updates Cybersecurity Framework
The National Institute of Standards and Technology (NIST) issued an update to its “Framework for Improving Critical Infrastructure Cybersecurity” to incorporate industry input and describe plans for future use of the framework. The update recognizes the call by stakeholders for more global policy, enforcement alignment and guidance. Some of next year’s initiatives include: developing material aligning the framework with business processes; partnering with other organizations to raise awareness; and hosting workshops, webinars and other meetings to connect stakeholders with the tool.

Survey: Security is Top Law Firm IT Concern
Security has supplanted email management as the number one technology concern for small and mid-sized law firms, according to the 2014 Technology Survey conducted by the International Legal technology Association (ILTA). The results were based on responses from IT professionals from 454 law firms, of which 33 percent were firms with less than 50 attorneys. The survey found 73 percent of firms responding reported conducting security audits, and 81 percent use Internet filtering. The survey also found 46 percent of firms have a mobile device management policy, compared with only 34 percent in 2012. Yet, despite the increased attention to security, the survey found IT budgets remained flat, with 45 percent of respondents reporting their 2014 IT operating budgets were the same as those of 2013. The survey may be accessed at http://www ilma.org/MainmenuCategory/Publications/WhitePapersandSurveys/2014-Technology-Survey.htm.

NYC’s Pay Phones to be Converted to Wi-Fi
New York City’s plan to convert aging pay phones to Wi-Fi hot spots received unanimous approval from the city’s Franchise and Concession Review Committee, clearing the way for the installation of thousands of Wi-Fi sites across New York City over the next decade. The city has chosen CityBridge, a consortium of companies including Qualcomm and Titan, to carry out the project, which will provide free Internet access, free domestic calling and a charging station for mobile devices at an estimated cost of more than $200 million to build the network. The plan is expected to be paid for by advertising revenue from digital displays on the new kiosks.

In the Courts

Duty to Warn: Communications Decency Act
Jane Doe No. 14 v. Internet Brands, Inc., 767 F.3d 894 (9th Cir. September 17, 2014). The Ninth Circuit Court of Appeals found the Communications Decency Act (CDA) did not bar the claim. Jane Doe, an aspiring model, posted information about herself on modelmayhem.com, a networking website for people in the modeling industry. She alleged two rapists used the website to lure her to a fake audition and raped her. She also alleged Internet Brands, the owner of the website, knew about the rapists but did not warn her or other users of the site. She filed suit against the company, alleging liability for negligence under California Civ. Code § 43.92, which imposes a duty to warn a potential victim of third party harm when a person has a “special relationship to either the person whose conduct needs to be
controlled or ... to the foreseeable victim of that conduct." The U.S. District Court for the Central District of California dismissed the suit as barred by the CDA, and Doe appealed. The appeals court reasoned Doe did not seek to hold Internet Brands liable as a publisher or speaker of content someone posted on the site. The court further noted the duty to warn imposed by California law would not require Internet brands to remove any user content or otherwise affect how it published such content. The court held the CDA did not bar the failure to warn claim because it had nothing to do with Internet Brands' efforts, or lack thereof, to edit or remove user-generated content. The judgment was reversed, and the case was remanded.

**Probable Cause: IP Address**

*State v. Bernard*, 762 S.E. 2d 514 (N.C. App. September 2, 2014). The North Carolina Court of Appeals found there was probable cause to support the warrant. A N.C. Agricultural and Technical State University (NC A&T SU) detective was contacted by Linda McAbee, the Vice Chancellor of Human Resources, who complained someone had accessed her University email account without permission. Further, she stated that same person had sent a bogus email to University administrators urging them to rehire or compensate Patrice Bernard, a former employee who was terminated and was involved in a pending suit against the University. University IT staff found the IP address for the sender of the unauthorized email, and the detective then obtained a search warrant from Road Runner for that IP address, finding it was assigned to Bernard. The detective then applied for a search warrant for Bernard's home, vehicle and person. Bernard was arrested and charged with accessing a government computer without authorization, felony accessing computers and identity theft. She moved to suppress evidence obtained from the search warrants as violative of her Fourth Amendment rights.

**Fourth Amendment: Real Time Cell Phone Location Tracking**

*Tracey v. State*, 2014 Fla. LEXIS 3072 (October 16, 2014). The Supreme Court of Florida found the use of defendant's cell site location information was a Fourth Amendment search. Law enforcement learned from an informant that Shawn Tracey obtained cocaine in Broward County for distribution in the state. Based only on this information, officers obtained an order authorizing the installation of a pen register and trap and trace device on Tracey's cell phone, enabling officers to track Tracey's cell phone calls and his trip to a house in Broward County and arrest him. Officers had obtained and used the real time cell site location information from Tracey's cell phone, even though the order provided only for recording
“inbound and outbound dialed digits” to help identify co-conspirators. The application did not provide facts establishing probable cause to track the location of Tracey’s cell phone or ask for access to real time cell site location information. Tracey moved to suppress the evidence, contending probable cause was required to obtain real time location information and officers had exceeded the scope of the order. The trial court denied the motion, finding a warrant was not required to use Tracey’s real time cell site location data to track him on public streets. On appeal, the Florida Supreme Court ruled the motion to suppress should have been granted because, regardless of Tracey’s location on public roads, the use of his cell site location information in order to track him in real time was a Fourth Amendment search requiring probable cause. The decision was quashed and the case remanded. Ed. note: Consiglia Terenzio, Bureau Chief, and Melynda Melear, Assistant Attorney General, of the Florida Attorney General’s Office, represented the State.

**Fourth Amendment: Seizure by Private Citizens**

*State v. Manning*, 2014 Iowa App. LEXIS 1007 (October 15, 2014). The Iowa Court of Appeals found police did not exceed the scope of the searches by private citizens. A friend of Brandon Manning searched his toolbox while Manning was in prison, found and plugged in a flash drive and saw what he believed were photographs of child pornography. He showed them to Manning’s girlfriend, who gave the drive to police. Police interviewed Manning, who denied ownership of the drive, but the State charged Manning with sexual exploitation of a minor, an aggravated misdemeanor. Manning filed a motion to suppress the evidence on the drive, alleging it was obtained by an illegal search in violation of his Fourth Amendment rights. The district court denied the motion, reasoning the initial search was done by private citizens, so the subsequent search by law enforcement was not unconstitutional. The first trial ended in a mistrial, but at the second trial a jury found Manning guilty, and he was sentenced to serve a prison term of up to two years. He appealed, arguing again the evidence found on the drive resulted from an illegal search. The appeals court found under the Fourth Amendment the officers’ viewing and search of the contents of the flash drive did not exceed the scope of the initial private search by private citizens, and the evidence was sufficient to sustain Manning’s conviction. The judgment was affirmed. Ed. note: Mary Triick, Assistant Attorney General in the Iowa Attorney General’s Office, represented the State.
Libel: Continued Availability of Fake Facebook Account

Boston v. Ahearn, 2014 Ga. App. LEXIS 664 (October 10, 2014). The Georgia Court of Appeals ruled a reasonable jury could have found the posting teen's parents caused some of the victim's injuries. Dustin Ahearn, 13 years old, posed as Alex Boston, a fellow student, to create a false Facebook page for her using a computer supplied by his parents and the family Internet account. He then added information, including racial viewpoints and a homosexual orientation, to the false account profile and issued invitations to become Facebook “friends” to other classmates. Alex suspected Dustin, and her parents spoke to the principal, resulting in Dustin's confession. The principal suspended Dustin for two days and sent an explanatory note home to his parents, who disciplined him. However, the unauthorized profile and page remained accessible to users for 11 months, and the Ahearns made no attempt to determine the content or to learn to whom Dustin had distributed the offensive information. The Bostons sued Dustin and his parents, alleging Dustin defamed Alex and caused intentional infliction of emotional distress. The Ahearns moved for summary judgment, which the trial court granted. The Bostons appealed, contending there were questions of material fact as to whether the Ahearns breached a duty to supervise Dustin's use of the computer and a duty to remove defamatory content on their property. The appeals court found the Ahearns had no reason to anticipate Dustin would engage in the offensive conduct until after he had done so. However, the court ruled a reasonable jury could find the Ahearns proximately caused some part of Alex's injuries by allowing the false and offensive statements to remain on display and available to readers for an additional 11 months after they learned of Dustin's actions. The judgment was affirmed in part and reversed in part.

Fourth Amendment: Exclusionary Rule

State v. Henderson, 289 Neb. 271 (October 17, 2014). The Nebraska Supreme Court found the good faith exception to the exclusionary rule applied. Tillman Henderson was involved in a shootout and was taken into custody. Police searched him and removed his personal property, including a cell phone. A detective obtained a warrant to search Henderson's cell phone and downloaded its contents. Prior to trial, Henderson filed a motion to suppress evidence obtained from the search, arguing the affidavit did not establish probable cause. Before the court ruled on the motion, however, detectives obtained a second warrant to search the phone, with the second supporting affidavit also including a statement about affiant's training and experience providing him knowledge about suspects' use of cell phones to communicate about shootings. The court issued the second warrant,
and the contents of the cell phone were again searched. The court ruled on the first suppression motion, agreeing with Henderson it lacked probable cause, but concluding it was a valid warrantless search incident to arrest. The court also found the affidavit of the second warrant application established probable cause. A jury found Henderson guilty of first degree murder, attempted first degree murder, two counts of use of a deadly weapon to commit a felony and possession of a deadly weapon by a prohibited person. Henderson appealed, arguing the trial court erred in denying his motion to suppress and admitting evidence from his cell phone, among other claims. The Nebraska high court found the good faith exception to the exclusionary rule applied because the affidavits provided probable cause. The judgment was affirmed.

Ed. Note: Assistant Attorney General Nathan Liss of the Nebraska Attorney General’s Office represented the State.

**Thumb Drive Evidence: Chain of Custody**

*In the Interest of A.O.*, 2014 UT App. 242 (October 17, 2014). The Utah Court of Appeals ruled the juvenile court did not abuse its discretion in admitting the thumb drive evidence. Law enforcement learned a father was trading alcohol and tobacco for sexual explicit images of minors. They obtained a warrant to search the father’s house for cell phones, computers, thumb drives and other electronic equipment providing storage for images and a second warrant to examine the contents of the devices for evidence of sexual exploitation of minors. Investigators found a thumb drive with sexual explicit images of the daughter and of the wife, as well as a computer with more than 100 images of child pornography. At the ensuing child welfare proceeding, the father moved to suppress all evidence obtained from the thumb drive, arguing the chain of custody of the drive was inadequate. The motion was denied, and the court determined the father had neglected the children and had sexually exploited the daughter. The court placed the children in the custody of the Division of Child and Family Services. The father appealed, arguing the evidence from the thumb drive lacked the proper foundation and chain of custody. The court found it was reasonable for the juvenile court to conclude the thumb drive evidence came from the father’s bedroom, had not been altered or changed and was admissible. The judgment was affirmed.

Ed. Note: John Peterson, Assistant Attorney General in the Utah Attorney General’s Office, represented the State.

**Confrontation Clause: Admission of Text Messages**
U.S. v. Mathis, 767 F. 3d 1264 (11th Cir. September 24, 2014). The Eleventh Circuit Court of Appeals ruled the admission of a victim's text messages did not violate the Confrontation Clause. Arnold Mathis, a registered sex offender, was arrested after he allegedly attempted to convince a minor to send him sexually explicit photographs via text message, and had actually convinced a different minor to do so. Prior to trial, he moved to suppress evidence obtained from his cell phone, arguing the affidavit in support of the warrant was not obtained in good faith. The motion was denied, and a jury convicted him of several sexual exploitation offenses. He appealed, renewing his suppression motion and arguing the admission of the victim's text messages violated the Confrontation Clause. The appeals court found the motion to suppress was properly denied because the affidavit in support of the search warrant established a connection between the cell phone and the sexual abuse of a minor, and there was no indication of the affiant's bad faith. The court further found the admission of the victim's text messages did not violate the Confrontation Clause as the messages were not testimonial. The conviction and sentence were affirmed.