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.

Attorneys General Fighting Cybercrime

Texas Attorney General Ken Paxton, supported by 30 Attorneys General, filed an objection to the sale of the personally identifiable information of 117 million RadioShack customers in the associated bankruptcy case. Supporting the objection are Attorneys General from the following jurisdictions: Arizona, Arkansas, Colorado, Connecticut, District of Columbia, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kentucky, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Montana, Nebraska, Nevada, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Virginia, Washington and Wisconsin.

Alabama Attorney General Luther Strange announced that Thomas Hixon pled guilty to Attempted Computer Tampering, a Class C felony, and was sentenced to five years in prison and a $1,000 fine. The conviction arose from a call Hixon made to the Calhoun County Sheriff’s Office in which he claimed to be a Weaver Police Department employee and used spoofing software to manipulate the caller ID in order to obtain access to the National Crime Information Center database. The case, the first under the Alabama Digital Crime Act, was prosecuted by Deputy Attorney General Pete Smyczek and Special Prosecutions Division investigators. The Georgia Bureau of Investigation and Chickamauga Police Department assisted in the case.

Arkansas Attorney General Leslie Rutledge announced that David West pled guilty to five counts of possession of child pornography and was sentenced to 20 years imprisonment. Cyber Crimes Unit agents had arrested West after executing
a search warrant at his residence, conducting a forensic exam on his computer and
finding evidence of child pornography. Upon release, West will be required to
register as a sex offender. The Jacksonville Police Department assisted in the
arrest and investigation.

California Attorney General Kamala Harris announced that Kevin Bollaert,
the operator of a cyber-exploitation website which posted photos of people with
personal identifying information without their consent, was sentenced to 18 years
in prison. Bollaert was found guilty of six counts of extortion and 21 counts of
identity theft pursuant to an investigation by the eCrime Unit.

Connecticut Attorney General George Jepsen created a Privacy and Data
Security Department to focus on investigations and litigation related to consumer
privacy and data security. It will also help to educate the public and business
community about their responsibilities. Assistant Attorney General Matthew
Fitzsimmons, who has served as Chair of the Privacy Task Force, will head the new
department.

Delaware Attorney General Matt Denn’s Child Predator Task Force arrested
Samuel Diamond on 25 counts of distribution of child pornography. The Task
Force, investigated and, assisted by a State trooper, executed a search warrant at
Diamond’s residence and conducted a forensic preview on the computers and
electronic devices, finding more than 25 child pornography images.

Florida Attorney General Pam Bondi’s Office filed four complaints involving
deceptive marketing and sales of computer software and tech support services
against the following call centers: ASAP Tech Help, LLC; E-Racer Tech, LLC;
Protech Support LLC d/b/a/ Rapid Tech Support; Techfix USA, LLC d/b/a PC
Smart Support and First Class Tech Support. The call centers allegedly used such
ruses such as pop-up ads warning of viruses and other malware to lure consumers
to a sales pitch designed to scare them into paying for unnecessary computer
repairs and support services costing between $99 to $600, in violation of the
Florida Deceptive and Unfair Trade Act. The complaints seek a permanent
injunction, consumer restitution and civil penalties.

Hawaii Attorney General Doug Chin announced the Hawaii Supreme Court
ruled that nine online travel companies, including Expedia, Orbitz, Priceline and
Travelocity, owe millions of dollars in back taxes to the State for selling hotel
rooms online. The ruling affirms the state Tax Appeal Court’s judgment upholding
the State’s assessment of penalties and interest against the companies for failing
to file tax returns.

Illinois Attorney General Lisa Madigan announced Timothy Saxton was
charged with two counts of distribution of child pornography, a Class X felony
punishable by six to 30 years in prison, and two counts of possession of child
pornography, a Class 2 felony punishable by three to seven years in prison.
The Attorney General’s investigators, the Macoupin County Sheriff’s Office and
the State Polices had executed a search warrant at Saxton’s residence.

Kentucky Attorney General Jack Conway’s Cybercrimes Unit investigators,
with assistance from Frankfort Police, arrested Sherwin “Rick” Collins on one count
of unlawful use of electronic means to induce a minor to engage in sexual or other
prohibited activities, a Class D felony punishable by up to five years in prison.
Collins exchanged emails and texts with a person he met on Craigslist who he
believed was the mother of an underage girl, but was actually an undercover Unit
agent. Collins had made arrangements to engage the girl in sexual conduct.

Louisiana Attorney General Buddy Caldwell’s Cyber Crime Unit investigators
charged Jamison Henry with nine counts of child pornography pursuant to a joint
investigation by the Unit, Homeland Security Investigations, the FBI, the Ouachita
Parish Sheriff’s Office and the State Police. The Unit executed a search warrant
at Henry’s residence and conducted a forensic examination of evidence seized
after receiving a cyber tip from the National Center for Missing and Exploited
Children that a suspect was uploading child pornography on a social media site.

Massachusetts Attorney General Maura Healey announced that Alba Andino
was indicted on charges of Trafficking of Persons for Sexual Services and Deriving
Support from Prostitution for allegedly using Backpage.com to advertise sexual
services. The investigation began from a referral from the Lowell Police
Department and Middlesex District Attorney’s Office. Andino allegedly lured
women into prostitution, posted ads for their services, set up appointments for
them and arranged transportation to their appointments. Andino was arrested by
Lowell Police Department officers. The indictment was through the Human
Trafficking Unit.
Michigan Attorney General Bill Schuette’s Criminal Division charged Anthony Modrzejewski with 10 counts of possessing child pornography, a felony punishable by up to four years in prison and/or a $10,000 fine; 10 counts of distributing child pornography, a felony punishable by seven years in prison and/or a $50,000 fine; one count of Using a Computer to Commit a Crime, a felony punishable by up to seven years in prison and/or a $5,000 fine; and one count of Videotaping an Unclothed Person, a felony punishable by up to five years in prison and/or a $5,000 fine. Modrzejewski was arrested by the Internet Crimes Against Children Task Force and the St. Clair Shores Police Department.

Mississippi Attorney General Jim Hood announced that John Wiggins of Texas pled guilty to two counts of Fraudulent Use of Identity and was sentenced to the maximum penalty of five years in prison on each count, with sentences to run concurrently. The case was referred to the Consumer Protection Division by the Lafayette County Sheriff’s Office, and an investigation revealed Wiggins was behind a Craigslist scam in the sale of a nonexistent truck using the identity of a deceased resident as the seller. Wiggins was also ordered to pay full restitution of $3,500 to the victims. Special Assistant Attorney General Shaun Yurkuran of the Division prosecuted the case.

Nebraska Attorney General Doug Peterson announced that Billy Schrader, who pled guilty to one count of manufacturing child pornography, was sentenced to the maximum of 30 years in federal prison. The North Platte Police Department and the Lincoln County Sheriff’s Office investigated the case, and Assistant Attorney General Kale Burkick and Assistant U.S. Attorney Steve Russell prosecuted it.

Acting New Jersey Attorney General John Hoffman announced that Christopher Alcantara, Mariano Alcantara and Lewis Alcantara-Sosa, who operated a private auto inspection business, pleaded guilty to fraudulently using data simulators to generate false results for motor vehicle emissions inspections. Deputy Attorneys General Debra Conrad and Michael King of the Division of Criminal Justice presented the case to the grand jury. The lead investigators for the Division were Detective Sean Egan and State Investigator Ruben Contreras.

Ohio Attorney General Mike DeWine’s Crimes Against Children Unit and the Leetonia Police Department arrested Lucas Ippolito on 10 felony charges of disseminating child pornography. The arrest followed execution of a search
warrant at Ippolito’s home, where multiple computers and other digital media were seized.

**Oklahoma Attorney General Scott Pruitt** charged Sam Douglas with distribution of child pornography, aggravated possession of child pornography and violation of the Computer Crimes Act, all felonies. An undercover investigation by State Bureau of Investigation (OSBI) agents uncovered the sharing of child pornography images at an IP address registered to Douglas’ roommate. Agents from OSBI, the Attorney General’s Office and the Oklahoma City Police Department executed a search warrant and seized Douglas’ laptop with hundreds of child pornography images. If convicted, Douglas faces life in prison and fines up to $40,000.

**Pennsylvania Attorney General Kathleen Kane’s** Child Predator Section investigators arrested Patrick Carrick on 10 counts of possession of child pornography and one count of criminal use of a communications facility. The arrest follows a joint investigation by the Section and the U.S. Postal Inspection Service leading to execution of a search warrant and seizure of computers containing movies of child pornography ordered by Carrick.

**Rhode Island Attorney General Peter Kilmartin** announced that the State Senate passed S. 596, a bill filed on behalf of Attorney General Kilmartin designed to protect businesses against predatory and bad faith patent infringement claims by patent trolls. The bill has been referred to the House Judiciary Committee.

**South Carolina Attorney General Alan Wilson** announced that the Florence County Sheriff’s Office, a member of the Internet Crimes Against Children Task Force, arrested Lentheus McAlister on nine counts of distribution of child pornography, a felony punishable by up to 10 years in prison on each count. A search warrant executed at McAlister’s residence found computer equipment containing child pornography which he distributed via file sharing. The Attorney General’s Office will prosecute the case.

**South Carolina Attorney General Marty Jackley** joined Minnehaha County Sheriff Mike Milstead and Sioux Falls Police Chief Doug Barthel to announce that the Division of Criminal Justice and the Internet Crimes Against Children Task Force arrested Jose Oxlaj, Andrew Krogman, Scott Larson, Lance Hunter, Nathaniel Downs and Benjamin Iverson on one count each of solicitation of a minor,
a class 4 felony punishable by up to 10 years in prison and/or a $20,000 fine. Iverson is also charged with two counts of Aggravated Assault on a Police Officer, a class 2 felony punishable by up to 25 years in prison and/or a $50,000 fine. The Sioux Falls and Watertown Police Departments, Department of Homeland Security and the FBI assisted in the case.

**Vermont Attorney General William Sorrell** announced that Christian Cowell was arraigned on three felony counts of Promoting Child Pornography for distributing child pornography using peer-to-peer file sharing programs. The charges stem from an investigation by the Attorney General's Office; State Police; the Burlington, South Burlington and Springfield Police Departments; Homeland Security Investigations; and the Internet Crimes Against Children Task Force. If convicted, Cowell faces a maximum of 30 years in prison.

**Virginia Attorney General Mark Herring** announced that Benjamin Thompson pled guilty to three counts of possession of child pornography and was sentenced to 10 years in prison, with eight years suspended. Assistant Attorney General Tommy Johnstone prosecuted the case with cooperation from the Chesterfield County Commonwealth's Attorney's Office. The case was investigated by the Richmond Police Department as part of the Southern Virginia Internet Crimes Against Children Task Force.

**Washington Attorney General Bob Ferguson** announced that the state House of Representatives passed his Patent Troll Prevention Act, a bill designed to protect small businesses from predatory and bad faith patent infringement claims and demands. The bill would provide the Attorney General with enforcement authority to hold patent trolls accountable.

**Cyber News Briefs**

**Verizon Releases 11th Annual Data Breach Report**

Verizon released its annual Data Breach Investigations Report, this year compiling data from 79,790 security incidents and 2,122 data breaches from 61 countries. As was true last year, the industries most affected were Technology/Information, with 1,496 security incidents and 95 confirmed data breaches; Public, with a large 50,315 security incidents and 303 confirmed data breaches; and Finance, with 642 security incidents and 277 confirmed data breaches. This year's analysis also revealed that nearly 70 percent of the attack victims were targeted as a means to
advances a different attack against another victim. The full report may be

Public Comment Sought on Cybersecurity Issues
The U.S. Commerce Department’s Internet Policy Task Force (IPTF) is seeking
public input on which key cybersecurity issues facing the digital economy could be
addressed by a consensus-based multistakeholder process. Comments may be
submitted to securityRFC2015@ntia.doc.gov and are due by cob on May 18, 2015.
All comments received are part of the public record and will generally be posted
without change.

White House Releases Consumer Privacy Bill of Rights Draft
The Administration released a draft of its proposed Consumer Privacy Bill of
Rights detailing what an individual should be able to expect from a service they
use, including how security is managed. The draft also addresses data deletion and
the revocation of consent on the part of a user, as well as restrictions on the types
of information that can be collected. The draft may be accessed at
http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-

In the Courts

Authentication: Facebook Records
of Appeals ruled the Facebook printouts were properly authenticated. Roger
Glover was convicted by a jury of first degree murder. At trial, the People
presented conversations recorded on Glover’s Facebook account of Glover
threatening the victim. On appeal, Glover contended the court erroneously
admitted printouts of those communications from his Facebook account. The
appeals court disagreed, finding the Facebook records were authenticated by an
unchallenged affidavit of a Facebook records custodian. The court found Glover
was linked to the Facebook account by testimony that the account was registered
to him; there were photos of Glover on the profile of the account; and Glover
provided his phone number when creating the account and it was verified by
Facebook. The judgment was affirmed.

Ed. Note: John Lee, Assistant Attorney General in the Colorado Attorney
General’s Office, represented the People in the appeal.
Warrantless Search: Abandoned Cell Phone

*State v. Samalia*, 344 P. 3d 722 (Wash. App. Mar. 5, 2015). The Washington Court of Appeals found the officer did not require a warrant to search the abandoned cell phone. Adrian Samalia was convicted of possessing a stolen vehicle. He had fled after being followed in the car by a police officer. The officer found a cell phone abandoned in the vehicle, called phone numbers listed in the cell phone’s contacts and eventually identified Samalia in a police database. At trial, Samalia unsuccessfully moved to suppress evidence leading to his identification derived from the cell phone, and he raised the same issue on appeal, contending the cell phone evidence was constitutionally protected and could not be accessed without a warrant. The appeals court disagreed, finding the cell phone was not seized from Samalia, but was found abandoned in the vehicle, and therefore the use of the phone came within the abandonment and exigency exception to pursue a fleeing suspect. Samalia did not have a privacy interest in the abandoned phone, so the officer did not need a warrant to use the phone in that manner. The judgment was affirmed.

Content of Warrant: Authorization to Search

*Moore v. State*, 2015 Miss. App. LEXIS 182 (April 7, 2015). The Court of Appeals of Mississippi ruled the warrant authorized the search of defendant’s cell phone. Pursuant to an investigation into the sexual assault of a minor, an investigator obtained a search warrant for Robert Moore’s cell phone. Included in the search warrant was the minor’s statement that Moore had photographed her with his phone during the assault, as well as the underlying facts. Moore was in custody on an unrelated charge, and the phone was in his property bag at the jail. The investigator turned the phone on, found the photographs and arrested Moore. The investigator subsequently obtained a second warrant expressly authorizing him to search and download any and all electronic data stored on the phone. Eighteen photographs were downloaded and presented to the grand jury, which indicted Moore on one count of sexual battery and one count of exploitation of a child. At trial, Moore moved to suppress the phone and photographs, which was denied, and he was found guilty on both counts. He appealed, challenging among other things the denial of his motion to suppress and arguing that the first warrant only authorized the investigator to retrieve, not search, the phone and thus violated his Fourth Amendment rights. The appeals court disagreed, finding the search warrant was specific enough to authorize both the physical seizure of the phone and the search of its photo library. The judgment was affirmed.
Legislative News

Patent Trolls
WASHINGTON. On April 16, 2015, the state House passed HB 1090, a bill requested by Attorney General Bob Ferguson that would ban making patent infringement claims in bad faith and a violation of the state Consumer Protection Act. The state Senate passed the companion bill, S. 5059, on April 14, 2015. The bill authorizes the Attorney General to bring an enforcement action. It would be effective 90 days from passage. The bill has been sent to the Governor.

RHODE ISLAND. On April 16, 2015, the state Senate passed S. 596, a bill that would ban making patent infringement claims in bad faith. The bill authorizes the Attorney General to bring an enforcement action, with courts authorized to award equitable relief, actual damages, cost and fees and/or exemplary damages. The bill would be effective upon passage and has been referred to the state House.

Drones Over Schools
CALIFORNIA. On April 20, 2015, the state Senate Committee on Public Safety passed SB271, a bill banning the unauthorized use of a drone on school grounds or to capture images of school grounds. Violation would result in a fine of up to $50 for a first offense, and a second violation would result in a fine of up to $200. The bill has been forwarded to the Committee on Appropriations.

Data Breach Notification
U.S. HOUSE. On April 15, 2015, the House Energy and Commerce Committee passed HR 1770, 29-20, the Data Security and Breach Notification Act, a bill which would preempt all state data breach notification laws. The bill would require companies to implement and maintain reasonable security measures to secure personal information. It would not require companies to provide notice of a breach if there was no reasonable risk of identity theft, economic loss or financial harm. The Federal Trade Commission and state Attorneys General would be authorized to enforce the bill.

New Resources
“The Emergence of Cybersecurity Law” is a new report prepared for the Indiana University School of Law by Hanover Research. It is only 30 pages and has three main sections addressing: 1) the importance of cybersecurity and how counsel are responding; 2) an overview of the current state of legislation, regulations and
other sources of law and policy influencing cybersecurity; and 3) lawyers’ roles in cybersecurity. It can be accessed at http://info.law.indiana.edu/faculty-publications/The-Emergence-of-Cybersecurity-Law.pdf.

“Understanding New Threats to Privacy and Cybersecurity” is a podcast under the new University of Pennsylvania Law School series, Case in Point, and examines trends in privacy and cybersecurity. It features Anita Allen, Professor of Law, and Lisa Sotto, partner at Hunton & Williams and chair of the U.S. Department of Homeland Security’s Data Privacy and Integrity Advisory Committee. It can be accessed at http://caseinpoint.org/.

“Electronic Signatures in Court” is a free six-page white paper by Silanis Inc. addressing the reliability of the technology, risks associated with electronic transactions, how relying on electronic signatures fares in settlement negotiations and whether courts admit and enforce electronically signed records. It may be accessed at https://www.silanis.com/resource-center/29-electronic-signatures-in-court/.