The Cybercrime Newsletter is a publication of the National Attorneys General Training and Research Institute (NAGTRI). It is written and edited by Hedda Litwin, NAAG Cyberspace Law Chief Counsel (hlitwin@naag.org; 202-326-6022).

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

In the interest of making this newsletter as useful a tool as possible for you, we ask that you keep us informed of your efforts. Additionally, we would like to feature articles written by you. Please contact us with information, proposed articles and comments about this newsletter. Thank you.

SUPREME COURT TO HEAR CHILD PORN RESTITUTION CASE

The U.S. Supreme Court has granted certiorari in a case involving criminal restitution for victims of child pornography. The issue to be reviewed by the Court is narrow: “What, if any, causal relationship or nexus between the defendant’s conduct and the victim’s harm or damages must the government or the victim establish in order to recover restitution under U.S.C. § 2259,” the Mandatory Restitution for Sexual Exploitation of Children Act of 1994. The case is notable not only for its potential impact, but also because it represents the first time a crime victim will have appeared before the Supreme Court in a criminal case.

The underlying case concerned a request for restitution by a young adult whose uncle sexually abused her as a child, filmed the abuse and distributed the films to others online. In U.S. v. Paroline, 672 F. Supp. 2d 781 (E.D. Tex. 2009), the victim challenged a decision by the U.S. District Court for the Eastern District of Texas denying her request for restitution under the Crime Victims’ Rights Act (CVRA), 18 U.S.C.S. § 3771. The Fifth Circuit Court of Appeals rejected the victim’s appeal because the CVRA only provides mandamus relief, and conditions were not met to grant the writ. It then ruled 18 U.S.C. § 2250 mandates defendant to pay restitution to the victim, and the victim was not required to show proximate cause in order to trigger a defendant’s restitution, thus vacating the district court judgment. The
defendant then filed a Petition for Writ of Certiorari seeking review.

Since other circuits have held 18 U.S.C. § 2259(b) (3)(F) requires claimants to show a “proximate result” to any claim, the stage is set for the Supreme Court to resolve the circuit split.

ATTORNEYS GENERAL FIGHTING CYBER CRIME

MULTI-STATE
The National Association of Attorneys General (NAAG) called on Congress to amend the Communications Decency Act in order to give state and local prosecutors more tools to combat prostitution and child sex trafficking. In a letter to key members of Congress, a bipartisan coalition of 49 Attorneys General advocated for amendments to the Act which would provide criminal jurisdiction to state and local authorities. Signing the letter were the Attorneys General of Missouri, South Dakota, Washington, Alabama, Alaska, Arizona, Arkansas, California, Colorado, Delaware, Florida, Georgia, Guam, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virgin Islands, West Virginia and Wyoming.

Twenty-three Attorneys General wrote to Google’s Chief Executive Officer, Larry Page, calling on the company to offer greater transparency and more meaningful privacy controls. The letter states that the Attorneys General will continue to closely monitor Google’s activities related to consumer privacy. Signing the letter were the Attorneys General of Arizona, Arkansas, California, Connecticut, Delaware, Hawaii, Illinois, Indiana, Iowa, Kentucky, Maine, Maryland, Massachusetts, Mississippi, New Hampshire, New Mexico, North Carolina, Rhode Island, South Dakota, Tennessee, Utah, Vermont and Washington.

Nebraska Attorney General Jon Bruning and Oklahoma Attorney General Scott Pruitt wrote a letter to Google, outlining their concerns with Google’s revenue from potentially dangerous videos on its subsidiary YouTube. The revenue sharing practice, called monetizing, involves videos posted on YouTube, with Google and the video producers splitting the revenue from advertising appearing when the videos are displayed. Specific examples cited in the letter include videos providing how-to guides for creating forged drivers’ licenses and passports, videos promoting the sale of counterfeit merchandise and illegal foreign “pharmacies” selling prescription drugs without a prescription. The letter seeks information about such postings as well as Google’s actions to remove the videos.

ALABAMA
Attorney General Luther Strange’s Special Agents partnered with Walker County District Attorney Bill Adair’s investigators to shut down an illegal gambling operation involving about 12 “electronic bingo” machines located in a private building. The machines are estimated to have an average value of $2,000 each, and will be held as evidence and be subject to forfeiture procedures.

ALASKA
Attorney General Michael Geraghty announced the conviction of Michael Mendenhall on four counts of distribution of indecent material to minors. Mendenhall had contacted an undercover Anchorage Police Department detective posing as a 14-year-old female and exposed himself via web cam on multiple occasions. Due to a prior conviction for
attempted homicide, Mendenhall faces two to four years on each count.

ARKANSAS
Attorney General Dustin McDaniel’s Cyber Crimes Unit arrested Johnny Carte on two counts of sexual indecency with a child, a Class D felony. The Unit had arrested Carte one month ago on 30 counts of distributing, possessing or viewing child pornography after agents executed a search warrant at his home. The electronic evidence seized from Carte’s residence will be analyzed by the Unit’s Forensic Lab, and the complete investigative file will be turned over to the Fourth Judicial District Prosecuting Attorney.

CALIFORNIA
Attorney General Kamala Harris released the first report detailing the 131 data breaches reported to her office in 2012 and involving the personal information of 2.5 million Californians. The report analyzes those breaches and makes recommendations about how data security could be improved. The report is available on Attorney General Harris’ web site.

DELAWARE
Attorney General Beau Biden announced an undercover investigation by the Delaware Child Predator Task Force led to the arrest of Kirk Simmons after he traveled to a motel to meet an individual he thought was a 13-year-old girl. Simmons had communicated with a Task Force detective posing as the girl’s father. The arrest was made by the State Police Special Operation Response Team. Simmons is charged with one count of Attempted Rape 3rd Degree. Search warrants were also executed at Simmons’ residence and on the vehicle he was driving, and detectives seized multiple computers and digital storage devices and media for forensic examination.

DISTRICT OF COLUMBIA
Attorney General Irvin Nathan announced a settlement with Classmates.com, whereby the online social networking web site agreed to improve its disclosures to District residents in order to resolve allegations of misleading practices. According to the District’s allegations, Classmates’ email solicitations misrepresented the facts by telling consumers people they knew were trying to contact them through the Classmates web site, thus improperly inducing them to purchase Classmates memberships. The District also alleged Classmates failed to notify consumers clearly and conspicuously about the automatic renewal of their memberships unless they terminated the subscription. The settlement also resolves the District’s allegation Classmates failed to give clear and conspicuous notice when Classmates allowed other companies to market their membership plans through the Classmates’ web site. Classmates.com, which is owned by Memory Lane, Inc. of Washington, also agreed to pay the District $300,000 for attorneys’ fees and costs. Bennett Rushkoff, Chief of the Public Interest Division’s Public Advocacy Section, and Assistant Attorney General Gary Tan handled the case.

GEORGIA
Attorney General Sam Olens filed suit against Martin A. Webb; Western Sky Financial, LLC; and CashCall, Inc., alleging that the companies made illegal payday loans in Georgia through web sites they operate. Georgia law prohibits making payday loans, including making payday loans to state residents through the Internet. Although the companies are not licensed in Georgia, they have been making high interest loans at rates up to 340 percent to state consumers. Both Attorney General Olens’ Office and the Governor’s Office of Consumer Protection have received numerous complaints. Although Attorney General Olens’ Office made numerous attempts to resolve the issue prior to suit, defendants failed to respond to correspondence. In addition to asking
the court to prohibit defendants from making payday loans in Georgia, Attorney General Olens is asking the court to declare any pending loans null and void and enjoin defendants from further collection of payments. The suit also seeks civil penalties and attorneys’ fees.

HAWAII
Attorney General David Louie announced a final judgment in favor of the State and against nine Online Travel Companies (OTCs) selling Hawaii hotel rooms over the Internet. The Tax Appeal Court granted the State’s motion for partial summary judgment, deciding the OTCs owe an additional $25 million for statutory interest on tax penalties. The taxes, penalties and interest for the period 2000 through 2011 total approximately $246 million. If the judgment is sustained after any further appeal, it would result in additional annual general excise tax collections of approximately $30 million. The Court ruled in favor of the OTCs on the State’s claim the OTCs owe the State’s Transient Accommodation Tax (“TAT”) during the same tax years, and the State intends to appeal.

IDAHO
Attorney General Lawrence Wasden’s Office, pursuant to a plea agreement and acting as Special Bingham County Prosecuting Attorney, filed an amended indictment charging Louis Krami, Chief Executive Office of Bingham Memorial Hospital, with stalking in the second degree. Indictments had charged Krami and former hospital information technology employees Jack York, Chris Behunin and Tyler Lassen with violations of the Idaho wiretap statute. According to the indictments, defendants intercepted and recorded phone calls made by and to former hospital doctor Robert Rosin and his staff. Krami was sentenced to 30 days in jail, which was suspended, one year on probation and ordered to perform 100 hours of community service and pay a $1,000 fine. Authorities were unable to serve a summons on York, and a warrant was issued for his arrest. Attorney General Wasden’s Office dismissed the cases against Behunin and Lassen because the investigation revealed they were acting solely as directed by their superiors and had cooperated fully with Attorney General Wasden’s investigation.

ILLINOIS
Attorney General Lisa Madigan’s investigators, with assistance from the Knox County Sheriff’s Office and State’s Attorney’s Office, arrested Kevin Martin, who is charged with four Class X counts of distribution of child pornography, punishable by six to 30 years’ incarceration; four additional Class 1 counts of distribution of child pornography, punishable by four to 15 years; three Class 2 counts of possession of child pornography, punishable by three to seven years; and one Class 3 count of possession of child pornography, with a possibility of two to five years. The arrest was made after a search of Martin’s residence revealed evidence of alleged child pornography. The arrest is part of Attorney General Madigan’s Operation Glass House, a statewide initiative against online child pornography.

KENTUCKY
Attorney General Jack Conway and his staff established a booth at the Kentucky State Fair to raise awareness about cyber security and prescription drug abuse. Located in the Kidz Biz section of the Fair, the booth had information and free give-away items related to both initiatives.

LOUISIANA
Attorney General Buddy Caldwell’s High Tech Crime Unit, with the assistance of the Ascension Parish and St. Charles Parish Sheriff’s Offices and the U.S. Department of Homeland Security Investigations, arrested Thomas Newman, Jr. on nine child pornography counts. If convicted, Newman faces up to 20 years in prison on each count.
Ohio
Attorney General Mike DeWine's investigators, joined by investigators from the Union County Sheriff’s Office and the Marysville Police Department, served search warrants on the Marysville Internet Café, Middletown Sweepstakes Café, Kenton Internet Café, Belle Phone Internet Café and the Sidney Internet Café. The following agencies also participated in this multijurisdictional investigation: Union County Prosecutor’s Office; Bellefontaine, Kenton, Middletown and Sidney Police Departments; and the Butler County, Franklin County, Hardin County, Logan County and Shelby County Sheriff’s Offices.

Pennsylvania
Attorney General Kathleen Kane’s Child Predator Section arrested Tyler Kennedy on five counts of possession of child pornography, five counts of distribution of distribution of child pornography and one count of illegal use of a communications facility.

South Dakota
Attorney General Marty Jackley joined Rapid City Police Chief Steve Allender and Pennington County Sheriff Kevin Thom to announce the Division of Criminal Investigation and the Rapid City Internet Crimes Against Children (ICAC) Task Force arrested James Larive Jr. and Curtis Austin as part of their investigation into sex trafficking at the Sturgis Rally. The FBI also cooperated in the investigation.

Texas
Attorney General Greg Abbott announced the sentencing of Stephen Sudduth, a former elementary school teacher, to 60 years in prison after he pleaded guilty to three second-degree felony charges of child pornography promotion. The sentencing stems from an investigation by Attorney General Abbott’s Cyber Crimes Unit, which arrested Sudduth after discovering more than 27,000 illicit images and 1,000 videos on Sudduth’s computers and external media devices. The case originated from a referral from the National Center for Missing and Exploited Children. Assistant Attorney General Brenda Cantu prosecuted the case.

Virginia
Attorney General Ken Cuccinelli filed suit against Jupiter Funding Group, LLC, an Internet payday lender, alleging it is making illegal payday loans to state consumers without a valid state license. Without the required state payday loan license, lenders can charge no more than 12 percent in annual interest, and Jupiter’s payday loans range from 438 percent annually for a 25-day loan to 1,369 percent annually for an eight-day loan. Violation of payday loan laws also violates the Virginia Consumer Protection Act (VCPA). The suit asks the court to stop Jupiter Funding from violating payday loan laws and also seeks consumer reimbursement of certain interest paid and civil penalties of $2,500 for each violation of the VCPA. Assistant Attorney General Mark Kubiak and Senior Assistant Attorney General Dave Irvin are representing the Commonwealth.

Wisconsin
Attorney General J.B. Van Hollen’s Division of Criminal Investigation (DCI) special agents, with assistance from the Prairie du Chien Police Department, executed a search warrant at the home of Cody Tamling and seized computers and cell phones. During an interview with a DCI agent, Tamling admitted to searching for and downloading child pornography, and a review of a hard drive from Tamling’s computer uncovered several images consistent with child pornography. Tamling has been charged with six counts of possession of child pornography, a felony.
CYBER NEWS BRIEFS

GAO ISSUES REPORT ON ROGUE INTERNET PHARMACIES

On July 8, the Government Accountability Office (GAO) issued a report on Internet pharmacies, finding many are complex, global operations, and federal and state law enforcement face significant challenges in investigating and prosecuting those involved. The report, required under the Food and Drug Administration Safety and Innovation Act, identifies 1) how rogue sites violate federal and state laws; 2) challenges federal agencies face in investigating and prosecuting operators; 3) efforts to combat rogue Internet pharmacies; and 4) efforts to educate consumers about the risks of purchasing prescription drugs online. The report can be accessed at http://www.gao.gov/products/GAO-13-560.

DELAWARE HIGH COURT CREATES TECH COMMISSION

The Delaware Supreme Court announced the creation of a technology commission to provide state lawyers with guidance and education on technology and maintaining client confidentiality. The commission is in response to an amendment to the Delaware rules of professional conduct requiring lawyers to maintain competence in technology and stay informed on legal issues related to technology. Supreme Court justice Henry duPont Ridgely will serve as liaison to the 15-member commission, which includes attorneys from both the public and private sector and judges representing different courts. The commission will be tasked with developing guidelines and best practices for using technology in the practice of law and for providing continuing legal education programs relating to technology.

FTC DRAFTS 5-YEAR PLAN

The Federal Trade Commission (FTC) released its draft strategic plan for the next five years, with its main strategic goal continuing to be consumer protection. As to measuring success in the plan, the FTC said it will look to total consumer savings compared to the amount of FTC resources allocated. The plan also called for more collaboration with domestic and international partners, including international consumer protection enforcement models or approaches. Another plan goal is consumer education and research. The draft plan may be accessed at http://www.ftc.gov/opp/gpra/strategic/dspfy14y18.pdf.

TECH COMPANIES SUPPORT ECPA AMENDMENT

On July 12, several of the largest technology and Internet companies, including Microsoft, Oracle, Intel, Adobe, Facebook, Twitter, Google and Yahoo, sent a letter to the U.S. Senate urging passage of a proposed amendment to the 1986 Electronic Communications Privacy Act (ECPA). Under current law, government agencies wanting to seize emails from third-party servers need a warrant for emails less than 180 days old, but only a subpoena or court order for older emails. The proposed amendment by Senators Patrick Leahy (D-VT) and Mike Lee (R-UT) would require government agencies to obtain a warrant before accessing any emails or electronic communications stored on third-party servers, regardless of when received. The letter also opposed a proposal from the Securities and Exchange Commission (SEC) granting the agency an exemption from the amendment. The amendment passed the Senate Judiciary Committee in April, but a vote before the full Senate has not been scheduled. The House Appropriations Committee unanimously passed a similar amendment giving emails the same protection as regular mail.
NY STATE GRANT TO EXPAND INTERROGATION VIDEOTAPING

New York Governor Andrew Cuomo’s administration is making $1 million in grants available for videotaping of interrogations through its Division of Criminal Justice. Currently, 345 law enforcement agencies in 58 of the State’s 62 counties are videotaping interrogations, but many of the smaller police departments and sheriff’s offices in rural counties do not have the equipment. Although the State has already provided more than $3 million to support video recording, these additional grants will enable the smaller counties to record interrogations in at least the major cases. Legislation requiring recording of custodial interrogations has stalled, with some legislators expressing concerns statements might be suppressed if a valid confession was not recorded because of an equipment malfunction or other glitch.

BUSINESS LEADERS URGE ACTION AGAINST “PATENT TROLLS”

Fifty diverse organizations, including the American Bankers Association, the Motion Picture Association of America, the National Association of Broadcasters, the National Retail Federation and the National Association of Realtors, sent a letter to the chairs and minority leaders of both the Senate and House, urging them to pass reform legislation to curb the activity of “patent trolls,” companies existing primarily to buy up patents and assert them. The letter notes the number of defendants sued by patent trolls has quadrupled since 2005, and in 2012 patent trolls sued more than 7,000 defendants and sent thousands of threat letters. According to the letter, this activity cost the U.S. economy $80 billion in 2011, and productive companies made $29 billion in direct payouts to the trolls.

STUDY: COST OF U.S. CYBERCRIME TO REACH $100 BILLION

The cost of cybercrime and cyberespionage to the U.S. is estimated to reach $100 billion per year, according to a joint study by the nonprofit Center for Strategic and International Studies (CSIS) and computer security firm McAfee. Although many previous studies have tackled this issue, the CSIS-McAfee study is the first to address the potential effect on American jobs, citing the loss of as many as 508,000 positions each year. To derive the estimate, researchers asked 20 leading economists about the best modeling techniques to avoid many of the weaknesses of the study approach. The study may be accessed at http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

NLRB: RESTRICTIVE SOCIAL MEDIA POLICIES NOT “LIKED”

The National Labor Relations Board (NLRB) has advised employers against social media policies restricting an employee’s right to speak critically of the employer online, unless the policies were set in collective bargaining. The advice was given in a memo written by the NLRB’s Office of General Counsel concerning the Giant Food company and its three unions. According to that memo, the employer’s policy contained at least three guidelines prohibiting releasing confidential company information, using the company logo or other visual elements or discrediting the company’s products. Another guideline told employees to speak up if someone was violating the guidelines or “misusing” a company website. The NLRB found some of this language too vague and overreaching because an employee could read it to prohibit sharing information on wages or work conditions. The memo concludes portions of the employer’s social media policy violate the National Labor Relations Act because they could reasonably be construed to chill protected employee activity. The
memo may be accessed at http://www.nlrb.gov/case/05-CA-064793.

OAKLAND APPROVES HIGH TECH SURVEILLANCE
On July 31, the Oakland, California City Council voted unanimously to accept a $2.2 million federal grant from the U.S. Department of Homeland Security to help build a 24 hour/day surveillance center to enable law enforcement to monitor the city using a network of video cameras, license plate readers and gunshot detection microphones. The Domain Awareness Center (DAC) was originally proposed in 2008 for the limited purpose of monitoring the Port of Oakland to protect it against terrorist attacks, but has since been expanded to encompass the entire city and will eventually cost an estimated $10.9 million in federal funds. The DAC plan will integrate the city's police and fire dispatch system into a new surveillance network to help them respond more quickly to emergencies. Officials will have access to facial recognition and crime-mapping software, private alarm detection systems and Twitter feeds to better coordinate their responses. Based on the DAC's technical plan, the center will install 35 cameras at target locations and more than 100 police sensor sites, as well as approximately 700 video cameras inside Oakland schools. At the Port, DAC will install 77 perimeter detection cameras, 34 thermal intrusion detection cameras and 21 pan-tilt-zoom cameras.

COMMERCE REPORT: UNAUTHORIZED STREAMING = FELONY
The Department of Commerce’s Internet Privacy Task Force released a report on digital copyright policy endorsing the part of the controversial Stop Online Privacy Act (SOPA) making the streaming of copyrighted works a felony. Currently streaming a copyrighted work over the Internet is considered a violation of the public performance right and only punishable as a misdemeanor, rather than the felony charges accompanying the reproduction and distribution of copyrighted material. The report recommends adopting the same range of penalties for criminal streaming of copyrighted works to the public as now exists for criminal reproduction and distribution, emphasizing the importance of streaming as a significant means for consumers to enjoy content online. The report may be accessed at http://www.uspto.gov/news/publications/copyrightgreenpaper.pdf.

ABA ADOPTS CYBERSECURITY RESOLUTION
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.abanow.org/2013/06/2013am118/.

NY STATE BAR TO LAUNCH ONLINE COMMUNITIES
The New York State Bar Association is set to launch online communities for lawyers to interact with one another and exchange ideas, documents, advice and resources. Powered by Higher Logic, the communities are currently in beta testing mode and are slated to go live on September 1. The association currently relies on 200 listservs for communications among its members, which will remain in place for those
STUDY: RISE IN LITIGATION DUE TO SOFTWARE PATENTS
A study by the U.S. Government Accountability Office (GAO) found software patents are the main reason for the rise in litigation over inventions, especially against companies using the technology. The study, required under a 2011 law overhauling the U.S. patent system, found revisions and court rulings have made it easier to invalidate questionable patents and have limited the collection damages for a minor feature. The report recommended the U.S. Patent and Trademark Office work on improving the review process. The GAO found 46 percent of lawsuits filed from 2007 to 2011 involved software-related patents, and 39 percent of those were against companies outside technology fields, including retailers and drug manufacturers who were sued over features on their websites. Companies whose main business is to extract royalty revenue, known as patent monetization entities or PMEs, filed in about 19 percent of all lawsuits from 2007 to 2011, while operating companies brought 68 percent, according to the study. The study also found the number of defendants sued by patent monetization entities more than tripled, from 834 in 2007 to 3,401 in 2011. The report may be accessed at http://www.gao.gov/products/GAO-13-465.

PEW STUDY: TEENS AVOIDING APPS DUE TO PRIVACY CONCERNS
A new Pew Research Center study found 51 percent of teens aged 12 to 17 years who download apps to their cell phones or tablet computers have avoided certain apps due to privacy concerns. Further, 26 percent of those have uninstalled an app after they found it was collecting personal information they did not want to share. The study found girls appeared to be savvier about turning off tracking features than boys, with 59 percent of girls switching off a location tracking feature, compared with 37 percent of boys. However, among cell phone and tablet owners, boys were the more active downloaders, with 79 percent of boys downloading apps, compared with 62 percent of girls. Household income also played a role in mobile device usage, with teens in wealthier households more likely to download apps. The study found 79 percent of teens living in households earning $50,000 or more downloaded apps, compared with 60 percent of those living in households earning less than $50,000. The report can be accessed at http://www.pewinternet.org/Reports/2013/teens-and-mobile-apps-privacy.aspx.

IN THE COURTS

WIRETAP AUTHORIZATION: EVIDENCE FROM FEDERAL INVESTIGATION
State v. Harrell, 2013 Ga. App. LEXIS 511 (June 19, 2013). The Georgia Court of Appeals, Fourth Division, found the lower court erred in granting defendant’s motion to suppress. Frank Green, a local investigator who was also deputized as a DEA agent, participated in a federal drug investigation and prepared an application for a federal wiretap on a suspected drug dealer. The application was approved by a federal judge, and Green was allowed to monitor the wiretap. He determined that Bryan Harrell had contacted the drug dealer by phone about 50 times to order cocaine. Police officers then stopped
Harrell as he left an arranged meeting with the dealer, found drugs in his vehicle and arrested him. He was charged with illegally using a communications facility and possession of marijuana and cocaine. Harrell moved to suppress the evidence, challenging the legality of the wiretap, which the trial court granted. Specifically, the trial court ruled the wiretap application was deficient because it was not obtained from a Georgia superior court judge, did not show whether it was sealed or unsealed and the required notice listed the wrong issuing judge. The State appealed, and the appellate court reversed, finding the statute merely provided authority to Georgia superior court judges to issue warrant wiretaps and was not a requirement. Further, the court found no prohibition against evidence obtained during a federal investigation in compliance with the federal warrant process. The court also found the application and order were filed under seal, and were not invalidated because the judge’s name was incorrect. The judgment was reversed.

**WARRANTLESS SEARCH: AUTHORITY TO CONSENT**

*State v. Sobczak*, 2013 Wisc. LEXIS 264 (June 20, 2013). The Wisconsin Supreme Court found no Fourth Amendment violation in the warrantless entry and search of defendant’s home. Kenneth Sobczak’s girlfriend, who was staying in his home over the weekend, was alone while Sobczak was at work and used his laptop with his permission. She found what appeared to be child pornography, called police and consented to an officer’s entry into the home and inspection of the files found on the computer. Sobczak was charged with possession of child pornography, and he moved to suppress evidence from the warrantless entry and search of his computer as a violation of his Fourth Amendment rights. The trial court denied the motion, and on appeal, the appeals court confirmed. Sobczak sought further review. The state Supreme Court found no Fourth Amendment violation, as the girlfriend had a sufficient relationship to the premises to establish actual authority to consent to entry. The court cited significant factors, including her three-month relationship with Sobczak and his encouragement for her to spend an evening alone in the home with no restrictions on her use of the house. For the same reasons, the court found she had authority to consent to the search of the laptop, especially since she had permission to use it. The decision was affirmed.

*Ed. Note: Assistant Attorney General Warren Weinstein represented the State.*

**FOURTH AMENDMENT: PARTICULARITY**

*U.S. v. Galpin*, 2013 U.S. App. LEXIS 12965 (2nd Cir. June 25, 2013). The Second Circuit Court of Appeals found the search warrant to be overbroad. James Galpin was charged with several counts of production and possession of child pornography and committing a felony offense involving a minor while being required to register as a sex offender. He moved to suppress all evidence seized in the execution of a search warrant, including images of child pornography found on his computer, digital cameras and digital devices. That warrant authorized officers to search for evidence of violations of “NYS Penal Law and/or Federal Statutes.” The U.S. District Court for the Northern District of New York, while finding the warrant to be overbroad and lacking probable cause to search for child pornography, found it was severable, and further found the computer images would have been in plain view during execution of a properly limited search. It denied Galpin’s suppression motion, and he entered a conditional guilty plea, then appealed. The appeals court agreed the warrant violated the Fourth Amendment’s particularity requirement, but found the record deficient as to whether the warrant was severable and whether the child pornography images were seized in plain view. The court observed where a warrant lacked specificity, redaction required a court to separate the warrant into its constituent clauses, to examine each individual clause to determine whether it was sufficiently particularized and
supported by probable cause and to determine whether the valid parts were distinguishable from the non-valid parts. The court affirmed the district court's determinations regarding lack of probable cause to search for child pornography and a facially overbroad warrant, but vacated the judgment in all other respects and remanded it for further proceedings.

CELL PHONE RECORDS: BUSINESS RECORDS EXCEPTION

The People v. Zavala, 216 Cal. App. 4th 242 (May 13, 2013). The California Court of Appeals, Fourth District, found a printed compilation of cell data for use at trial fell under the business records exception of the hearsay rule. Angel Zavala was found guilty of robbery and burglary, based in part on cell phone records from his and his accomplice’s phones, testimony about those records and a detective’s testimony about call log information seen on Zavala’s cell phone. Zavala appealed, arguing the compilation of cell phone data did not fall within the business records exception. The appeals court disagreed, finding the records were properly admitted because the custodians of the data testified about the automatic generation of the data by the carriers’ computer systems at or near the time each call was made. They also testified about the accuracy of the records and how the trial documents were prepared. The court found the data was not rendered inadmissible because the documents were produced by human query, as the underlying data itself was not produced by human input but rather was recorded by the system each time a user made a call. Further, the court ruled the computer printout was not rendered untrustworthy because it was in the form of a spreadsheet and thus could be manipulated, as there was no evidence of such manipulation. The court also found no error in admitting the detective’s testimony about the call log information for the limited purpose of explaining investigative steps. The court affirmed the judgment.

Ed. Note, Chief Assistant Attorney General Julie Garland and Deputy Attorneys General William Wood and Gary Brozio represented the People.

EXPECTATION OF PRIVACY: STOLEN CELL PHONE

The People v. Barnes, 2013 Cal. App. LEXIS 459 (June 11, 2013). The California Court of Appeal, First Appellate Division, found defendant had no legitimate expectation of privacy in the cell phone he had stolen. Police used the GPS to locate a cell phone Lorenzo Barnes had stolen from its owner. Barnes was arrested and charged with two counts of second degree robbery while personally armed with a firearm and one count of being a past convicted felon in possession of a firearm. He moved to suppress all evidence as a violation of his Fourth Amendment rights, which was denied. He then pled guilty and appealed the denial of his motion. The appeals court concluded the use of the GPS to track the location of the stolen cell phone, and thus assisting in locating Barnes, did not violate the Fourth Amendment. The court found Barnes had no legitimate expectation of privacy in the cell phone he had stolen. The owner of the cell phone, who was the only person with a legitimate expectation of privacy, had consented to the police use of GPS to apprehend the person who had stolen it. As to Barnes’ argument the GPs merely established the location of the stolen phone, and not the location of the thief, the court found police officers could infer a reasonable possibility of locating the thief if they located the phone. Correlating Barnes’ movements with both the GPS location and the victim’s description of the thief gave officers ample reasonable suspicion for a detention. The conviction was affirmed.

Ed. note: Assistant Attorney General Gerald Engler and Deputy Attorneys General Seth Schalit and Leif Dautch represented the People.
EXPECTATION OF PRIVACY: CELL PHONE LOCATION

State v. Earls, 2013 N.J. LEXIS 735 (July 18, 2013). The New Jersey Supreme Court ruled an individual had a privacy interest in the location of his or her cell phone. Police obtained a warrant to arrest Thomas Earls. In an effort to locate him and his girlfriend, who was potentially his hostage, they obtained his cell phone location information from a service provider without getting a court order or warrant. The location information helped them track Earls to a motel room, where they found stolen property. He moved to suppress the evidence found in the motel room, which the trial court denied, holding a warrant was normally required to obtain such cell phone information, but the emergency aid exception to the warrant requirement applied since there was an objectively reasonable basis to believe the girlfriend was in danger. Earls then pled guilty to burglary and theft, both in the third-degree, and appealed the trial court's denial. The intermediate appellate court affirmed, but on different grounds, finding there was no reasonable expectation of privacy in the location of one's cell phone. Earls sought further review. The state high court disagreed, finding the state constitution protected an individual's privacy interest in the location of his or her cell phone. The court ruled police had to obtain a warrant based on a showing of probable cause, or qualify for an exception to the warrant requirement, to obtain tracking information through the use of a cell phone. The judgment was reversed and the case remanded for further proceedings to determine whether the emergency aid doctrine or another exception to the warrant requirement applied.

Ed. Note: Brian Uzdavinis, Deputy Attorney General in the New Jersey Attorney General's Office, argued the case for the State.

GPS PLACEMENT: TRACKING OUTSIDE OF BUSINESS HOURS

In the Matter of Michael Cunningham v. New York State Department of Labor, 2013 NY Slip Op 4838 (June 27, 2013). The New York Court of Appeals found the search was excessively intrusive and therefore unreasonable. The New York State Department of Labor (DOL), suspecting that employee Michael Cunningham was submitting false time reports, referred the matter to the Inspector General, who had a GPS device attached to Cunningham's car. The GPS recorded Cunningham's movements for one month and substantiated DOL's suspicions. Cunningham was terminated after a hearing. He appealed, arguing the GPS evidence should have been suppressed. The Commissioner of Labor affirmed the decision, and Cunningham sought further review. The appeals court found the attachment of the GPS to Cunningham's car was a search, but since it fell under the “workplace” exception to the warrant requirement, it was valid under the Fourth Amendment. However, the court also ruled the search was excessively intrusive and therefore unreasonable, as the GPS tracked Cunningham on evenings, weekends and vacation. The court found where an employer conducts a GPS search without making a reasonable effort to avoid tracking an employee outside of business hours, the search as a whole must be considered unreasonable and the GPS evidence suppressed. The judgment was reversed and the case remanded for further proceedings.

GPS PLACEMENT: PROBABLE CAUSE

Hamlett v. State, 2013 Ga. App. LEXIS 685 (July 18, 2013). The Georgia Court of Appeals ruled the affidavit in support of the application for an order authorizing the GPS device presented insufficient facts to support a finding of probable cause. Paul Hamlett and David Getachew-Smith were found guilty by a jury of burglary and possession of tools for the commission of a crime in a joint trial. They ap-
pealed, contending the trial court erred in denying their motion to suppress because there was not sufficient probable cause to support the order authorizing the State to install the GPS device on Hamlett’s truck, and the traffic stop resulted solely from the illegal installation and was not supported by a reasonably articulable suspicion of criminal activity. The appellate court agreed, finding attaching the GPS device to the truck and then continuously monitoring it constituted an invasion of privacy under the Fourth Amendment and had to be authorized by a valid search warrant supported by probable cause. The court noted the detective had admitted at the time he executed the affidavit there was no evidence Hamlett had been involved in a burglary. In addition, there was already an outstanding arrest warrant for Hamlett, which gave his home address. The court found since the stop was illegal, any evidence seized as a result should have been suppressed. The convictions were reversed.

CONFRONTATION CLAUSE: FORENSIC EXAMINER TESTIMONY

U.S. v. Soto, 2013 U.S. App. LEXIS 12894 (1st Cir. June 24, 2013). The First Circuit Court of Appeals found the non-testifying examiner’s report was not introduced through the testifying examiner. Steven Soto was convicted of mail, wire and bank fraud and aggravated identity theft in the U.S. District Court for the District of Massachusetts. He appealed, arguing the district court violated his Sixth Amendment confrontation right by admitting a forensic examiner’s testimony about another examiner’s prior examination of a laptop. The appeals court found the examiner testified about his conclusions from his own independent examination and did not introduce the non-testifying examiner’s report. That report only bolstered the testifying examiner’s testimony, and a curative instruction could have been given or the first examiner could have been produced. The court further found the statements in the report at issue linking Soto to documents were cumulative of the in-court testimony of the independent examiner. The convictions were affirmed.

POSSESSION OF CHILD PORNOGRAPHY: FORFEITURE OF COMPUTER

U.S. v. Penny, 2013 U.S. App. LEXIS 11076 (10th Cir. June 3, 2013). The Tenth Circuit Court of Appeals ruled the defendant was not entitled to recover his computer and hard drive. Charles Penny’s roommate turned over Penny’s laptop computer and associated equipment to law enforcement. Authorities obtained a search warrant and discovered more than 600 images and videos of child pornography on the computer. Penny subsequently pleaded guilty to possession of child pornography, and filed a motion in the U.S. District Court for the District of Wyoming under Fed. R. Crim. P. 41(g) for return of his seized property. The district court granted the motion as to certain property, but denied it as to the laptop and hard drive, and Penny appealed. The appeals court found the computer and hard drive were subject to forfeiture under 18 U.S.C.S. § 2253. The court ruled Penny was not entitled to recover the computer and hard drive under Rule 41(g) because he admitted he used the property to commit the offense and therefore was not an innocent owner. The district court’s order was affirmed.

______________________________________________

LEGISLATIVE UPDATE

SOCIAL MEDIA PRIVACY EFFECTIVE. On July 28, Washington State’s new Chapter 330 banning employers from asking employees to reveal their user names and passwords for their social media accounts became effective. The new law also proscribes employers from forcing employees to log in to their accounts in view of employers, requiring employees to add employers as friends or asking employees to change their personal settings to enhance visibility for third parties. Em-
Employers are also prohibited from punishing employees for refusing to disclose their personal login information. The limited exception to the law’s restrictions allows employers to retrieve content from an employee’s social media account in order to conduct an investigation into an employee’s conduct or if the employee is accused of unauthorized transfers of proprietary information. Even in those circumstances, employers can only ask, not require, employees to turn over their login information voluntarily. The law does not apply to social media sites and platforms used primarily for work purposes.

INTERNET PRIVACY— “DO NOT TRACK”
PASSED BOTH HOUSES. On August 26, the California Assembly passed AB 370, a bill requiring an Internet website to disclose how it responds to “do not track” signals or mechanisms giving consumers a choice regarding the collection of their personal information. It would also require disclosure of whether other parties may collect a consumers’ personal information when a consumer uses the website. The bill passed the California Senate on August 22 and has been sent to the Governor for signature.

“UNLOCKING” CELL PHONES
PASSED COMMITTEE. On July 31, the U.S. House Judiciary Committee approved HR 1123, a bill sponsored by Representative Bob Goodlatte (R-VA), that would allow consumers to circumvent technologies controlling access (“unlock”) their cell phones without permission from their wireless carrier for the purpose of connecting to different wireless telecommunication networks. The bill would restore an exemption to the Digital Millennium Copyright Act previously rejected by the Library of Congress.

NEW RESOURCES

TECHBeat
The “TECHBeat Summer 2013” publication features an article on the use of Twitter to improve law enforcement/community relations as well as an article on the use of a mobile application to track probation officers. It can be accessed at http://www.justnet.org/interactivetechbeat/summer_2013/techbeatsummer2013.pdf.

Consequences of Conviction
“Beyond the Sentence – Understanding Collateral Consequences” describes the National Inventory of the Collateral Consequences of Conviction, an interactive database of sanctions and restrictions, allowing the legal community to quickly locate the significant details of relevant collateral consequences. It can be accessed at http://www.nij.gov/nij/journals/272/collateral-consequences.htm.