Initiatives in the Attorney General Community

Three Attorneys General announced a $1 million multi-state settlement with Internet Order LLC, d/b/a Pinsleurapproach.com, over the use of negative option marketing in the sale of Pinsleur audio language courses over the Internet. The agreement resolves an investigation into the company's failure to clearly disclose that the purchase of a language course advertised as "only $9.95" included the shipment of additional language courses at a cost of $256 per course that, if not returned within 30 days, could cost the consumer more than $1,000. Consumers were also required to pay return shipping, despite the offer being advertised as "risk free" and "100% money back guarantee." The company also sent threatening collection letters to consumers who didn't pay. Among the conditions of the settlement, the company must receive the consumer's express consent before enrollment and, during any free trial period, must reaccept the items with no fee. The company must also pay $1,002,000 in restitution to victims. The States entering the settlement were New York, Pennsylvania and Washington.

Arkansas Attorney General Leslie Rutledge gave opening remarks at a Technology-Facilitated Crimes Against Children training attended by more than 60 law enforcement officers and child advocacy service providers. The training provided an overview of the types of technology used for sexual exploitation and facilitation of crimes against children, with discussion focusing on offenders' use of technology and the impact on victims.

California Attorney General Kamala Harris joined Congresswoman Karen Bass, Los Angeles Police Chief Charlie Beck and University of California Berkeley Professor Steven Raphael to launch OpenJustice, a criminal justice open data initiative. The tool has two components: a Dashboard that spotlights key criminal justice indicators and an Open Data Portal that publishes raw data from the California
Department of Justice’s repository of criminal justice datasets. It will enable researchers to help tackle problems in the criminal justice system.

Florida Attorney General Pam Bondi’s Office of Statewide Prosecution announced that Shawn Thomas was sentenced to 885 years in prison for possession of massive amounts of child pornography. The Department’s investigation revealed that Thomas communicated with an informant regarding his plans to kidnap a child, kill the parents and sexually batter the child while producing child pornography. He was intercepted before he was able to carry out his plans.

Hawaii Attorney General Doug Chin announced that the State has recovered $53.1 million in general excise taxes, penalties and interest from online travel companies, including Travelocity.com, LLP; Expedia, Inc.; Orbitz, LLC; and Priceline.com, LLP. The Hawaii Supreme Court upheld the Tax Appeal Court’s ruling that the companies owed the taxes.

Kentucky Attorney General Jack Conway’s Cybercrimes Unit investigators arrested Donnie Cooper for using a computer to contact a minor for sex. Cooper allegedly sent electronic messages to an undercover officer, posing as a minor, to arrange a meeting to engage in illicit sexual acts. He was arrested when he arrived at the meeting place. The Shelbyville Police Department assisted with the arrest. The charge is a Class D felony punishable by one to five years in prison.

Louisiana Attorney General James “Buddy” Caldwell’s Cyber Crime Unit arrested Erik Stapper on one count of possession of child pornography. During an online undercover operation, Unit investigators downloaded child pornography from Stapper, who faces up to 20 years in prison. The Jefferson Parish and Plaquemines Sheriff’s Offices and Homeland Security Investigations assisted in the investigation.

Massachusetts Attorney General Maura Healey filed an amicus brief with the First Circuit Court of Appeals urging the court to reverse a district court decision dismissing Doe v. Backpage.com, LLC, a case filed by human trafficking victims against Backpage.com. The case was filed by three women who allege they were sold for sex on Backpage.com when they were as young as 15 years old. They allege that they were recruited by sex traffickers, advertised on the website, and repeatedly sold for sex in locations around the State.
Mississippi Attorney General Jim Hood’s Internet Crimes Against Children Task Force was awarded $292,281 in federal funding from the Department of Justice to support the development of strategies to protect children from commercial and sexual exploitation. The task force now has 60 local, state and federal law enforcement affiliate agencies and multi-disciplinary partners.

Acting New Jersey Attorney General John Hoffman announced that Laquanda Tate, a former senior payroll clerk at the State’s Department of Human Services, pleaded guilty to simulating a motor vehicle insurance identification card and theft by deception for using her work computer to generate false insurance cards for herself and others. She also admitted to stealing public assistance benefits by creating false documents to claim childcare expenses. Under a plea agreement, the State will recommend that Tate be sentenced to 364 days in jail and 30 hours of community service as conditions for a term of probation. She must pay full restitution of the public assistance benefits received and will be permanently barred from public employment. Deputy Attorney General Jonathan Gilmore and Deputy Bureau Chief Peter Lee of the Division of Criminal Justice Corruption Bureau presented the case to the grand jury. It was investigated by Detective Thomas Page of the Division of Criminal Justice. Deputy Attorney General Victor Salgado and Police Detectives Alex Rivero and Carlos Ramirez of the Department of Human Services assisted with the investigation.

New Mexico Attorney General Hector Balderes announced that Adam Kerns was found guilty of Child Solicitation by an Electronic Device, a third degree felony. Kerns engaged in graphic sexual communication with an undercover detective, who was posing as a child. When Kerns showed up for an arranged meeting, he confessed to sending sexual text messages to someone he believed to be 13 years old. Kerns faces up to three years in prison and must register as a sex offender for 10 years.

New York Attorney General Eric Schneiderman announced a partnership with Facebook to leverage technology to identify victims of sex trafficking in online advertisements for commercial sex. Attorney General Schneiderman’s Office will work with Facebook to develop algorithms that will identify evidence of trafficking in the online ads, as well as identification of missing children who appear in the ads.

North Carolina Attorney General Roy Cooper announced that online lenders Western Sky Financial, CashCall and related companies are barred under a
preliminary injunction from making or collecting on loans in the State. Attorney General Cooper and the Office of the Commissioner of Banks had filed suit against the companies for violating state laws than ban excessive interest rates on small consumer loans. The companies allegedly charged consumers annual interest rates of 89 to 342 percent on loans of $850 to $10,000.

Pennsylvania Attorney General Kathleen Kane’s Child Predator Section arrested Antonio Denardo on one count each of distribution of child pornography and criminal use of a communications facility and 12 counts of possession of child pornography. The arrest resulted from an online investigation in which agents identified a computer on a network that was sharing files containing suspected child pornography. The IP address linked the images to Denardo’s residence, and execution of a search warrant resulted in the seizure of multiple electronic devices. A preliminary review by the Computer Forensic Unit revealed several files indicative of child pornography. Denardo will be prosecuted by Deputy Attorney General Rebecca Elo of the Section.

South Carolina Attorney General Alan Wilson announced that Jason Long was arrested on charges related to sexual exploitation of minors. The Anderson County Sheriff’s Office, a member of the State’s Internet Crimes Against Children Task Force, made the arrest, with assistance from the Berkeley County Sheriff’s Office, also a Task Force member. Long was allegedly involved in the sharing of child pornography via file-sharing networks. Specifically, Long is charged with one count of Sexual Exploitation of a Minor second degree and three counts of Sexual Exploitation of a Minor third degree, both felonies punishable by up to 10 years in prison on each count.

Texas Attorney General Ken Paxton’s Child Exploitation Unit arrested David Skoog on one count of Possession of Child Pornography. The Unit had executed a search warrant at Skoog’s residence and seized multiple digital storage devices, resulting in the recovery of illegal images. Skoog had previously been arrested on similar charges.

Virginia Attorney General Mark Herring announced that Timothy Bodenheimer pleaded guilty to 10 felony counts involving the solicitation of an undercover investigator posing as a 12-year-old boy and distribution and possession of child pornography. Specifically, Bodenheimer pleaded guilty to one count of use of a communication system to solicit a minor, which carries a maximum penalty of 10 years in prison. He also pleaded guilty to nine additional counts of distribution and possession of child pornography, which carry a maximum penalty of 30 years in prison.
years' imprisonment; one count of distribution of child pornography, with a maximum penalty of 20 years' imprisonment; and eight counts of possession of child pornography, with a maximum penalty of five years' imprisonment. The case was investigated by the Northern Virginia-Washington, DC Internet Crimes Against Children Task Force. Assistant Attorneys General Marc Birnbaum and Stacy Rohrs are prosecuting the case.

Washington Attorney General Bob Ferguson announced that the State Supreme Court ruled that a lawsuit brought by three young women who were sold for sex on Backpage.com can proceed against the company, an approach advocated by Attorney General Ferguson's Office in an amicus brief. The court found the plaintiffs should be allowed to try to prove their claims in court, and remanded the case to the trial court.

Wisconsin Attorney General Brad Schimel's investigators, the FBI and the Milwaukee Police Department charged Todd Dischler and Alexandria Williams with trafficking of a child. Investigators had communicated with an underage female who advertised in the escort section of an online classified ad site and arranged a meeting with her. Her traffickers dropped her off at the scene and were taken into custody. The victim was offered services for trafficking victims.

**Cyber News Briefs**

**GAO Report: FAA Making Progress on Drone Integration**
The Federal Aviation Administration (FAA) is making progress on integrating drones into the national airspace, despite challenges at agency-designated test sites and delays in finalizing regulations to cover commercial operations, according to a new Government Accountability Office (GAO) report. The report noted that the FAA has issued some basic frameworks and is working toward final regulations as it continues to approve more drone licenses on a case-by-case basis pending finalization of the rules. Total annual public certificates of waiver or authorization allowing drone use have increased dramatically from 2010, when 286 were issued, to 609 in 2014 and 403 in 2015 through April. Commercial authorizations were issued for the first time this year. The FAA is working with the MITRE Corp. on the foundation of an implementation plan, due this December. The GAO report may be accessed at [http://www.gao.gov/assets/680/671469.pdf](http://www.gao.gov/assets/680/671469.pdf).

And see...
U of Arkansas Bans Drones on Campus
The University of Arkansas issued a policy banning the use of drones and other remote-controlled aircraft on campus. The policy prohibits the use of "unmanned aircraft systems" on university property or within the university’s air rights without prior written approval. Violations of the policy may result in a criminal trespass warning or an arrest. The policy does permit the use of a drone if approved in advance. To receive approval, the aircraft would have to meet all federal certification requirements, federal and state laws and any FAA requirements. The stated purpose of the policy is public safety.

Report Issued on Future Technologies to Strengthen Criminal Justice
RAND issued a report on proceedings conducted with an expert panel on the criminal justice community's needs in the use of emerging web technologies. Among the top priorities listed were: 1) developing a common criminal history record and cataloguing scheme; 2) developing real-time language translation capabilities; and 3) developing displays to meet officers' dynamic information needs. The panel also called for procurement checklists and cost-benefit tools for systems acquisition, as well as policies and procedures to address the anticipated use of unmanned vehicles. The report may be accessed at http://www.rand.org/content/dam/rand/pubs/research_reports/RR900/RR928/RAND_RR928.pdf.

Pennsylvania Oks Smartphone Photos of Public Records
The Pennsylvania Office of Open Records ruled that government agencies cannot charge fees if people requesting public records want to use smartphones to photograph documents. The ruling will apply to any agency subject to the Right to Know Law for its fee structure, including townships, counties and state agencies.

FCC: E-Faxes Covered by TCPA, Junk Fax Protection Act
E-faxes, documents converted to an email or attachment, are subject to the same consumer protections as regular faxes, according to a declaratory ruling from the Federal Communications Commission (FCC). The ruling found that unsolicited communications that begin as faxes, whether they are converted to an electronic format after being sent or not, are subject to the consumer protection provisions of the Telephone Consumer Protection Act and the Junk Fax Protection Act. The ruling noted the agency’s interpretation of the statute focused on the sender's means of transmission, not the ultimate destination. The declaratory ruling may be
Montana Survey: 84% Have Internet Access
A study commissioned by the Greater Montana Foundation found that 84 percent of residents have Internet access at home, the first time the State has met the national average. The study also found that 48 percent of residents consider community news a top priority on a daily basis, with four in 10 residents accessing news online or on a mobile device. The study revealed that 62 percent of respondents reported having at least one social media account, with Facebook the most popular site, followed by Pinterest. A total of 526 adults participated in the survey. Additional survey results may be accessed at http://greatermontana.org/greater-montana-foundation-media-survey/.

Huge Clamor for .Law Domain
Sales for the new .law domain extension were brisk on July 30, 2015, the first day of sales, although sales were restricted to those who had registered their trademarks with the Internet Corporation for Assigned Names and Numbers (ICANN). Sales were opened to the entire legal community of an estimated two million attorneys on October 12, 2015, with a goal of 10 percent market penetration, or approximately 100,000 sales. The cost for the domain is approximately $200/year, plus a $10 verification fee, resulting in an annual market of more than $200 million.

Fl. Bar: Ads by Text Message OK
The Florida Bar Board of Governors reversed the decision of the Bar's Standing Committee on Advertising and determined that an advertisement sent via text message is not a prohibited solicitation. The text ads, which the Bar considers to be simply another form of written advertising, must comply with the same legal ethics rules as other ads. Opponents of the ruling had argued that test ads are more akin to prohibited phone calls to prospective clients. Florida is now only the second state to approve the use of texts for advertising; Ohio was the first.

DOJ Awards $19 Million in Grants for Body Cameras
The Department of Justice awarded $19.3 million in grants under the Body-Worn Camera Pilot Partnership Program to 73 law enforcement and tribal agencies for body cameras, noting that the requests for these grants far exceeded the funds
available, with 285 law enforcement agencies seeking the funding. The grants will help purchase 21,000 body cameras for agencies in 32 states and the District of Columbia. An additional $3.9 million has been allocated for training, technical assistance and a study to analyze the effectiveness of the program. The largest awards of $1 million each were given to Los Angeles; Washington, D.C.; Miami-Dade County, Florida; Chicago; Detroit; and San Antonio, Texas. Agencies receiving the grants must develop best practices for the use of body cameras and keep statistics on their effectiveness during the two-year grant period. Each agency was required to provide 50 percent in-kind or cash matching funds in order to qualify for the grants.

**Tennessee Bar Oks Cloud Storage for Confidential Records**

The Tennessee Board of Professional Responsibility held in Formal Ethics Opinion 2015-F-159 that lawyers can ethically use cloud storage for client confidential information upon taking reasonable and competent care to ensure their confidentiality and protection from loss, data breach or other risks. The Opinion applies long standing attorney ethical obligations to cloud storage just as they would to any other storage medium. In doing so, Tennessee joins 20 other states in approving the use of cloud storage. The opinion may be accessed at [http://www.tbpr.org/ethic_opinions/2015-f-159](http://www.tbpr.org/ethic_opinions/2015-f-159).

**In the Courts**

**Admission of Cell Phone Call Records: Hearsay Exception**

*Baker v. State*, 2015 Md. App. LEXIS 89 (July 6, 2015). The Maryland Court of Special Appeals found the State failed to show how the records were produced in order to qualify within the non-hearsay category. A.O., a prostitute, worked for a pimp who advertised her number on Backpage.com. She received a call from a Michael Baker and set up an encounter, but A.O. refused to engage in the type of sexual encounter Baker wanted. Baker then displayed what appeared to be a police badge, told her he was a police officer and warned she would be arrested if she didn’t comply. He then physically struck her and forced himself upon her. A.O. put his phone number in her cell phone under the contact name “Do not answer.” A.O. told a trooper about the rape, showing him Baker's number on her phone. The trooper found several calls from that number to A.O.'s phone. The State's Attorney's Office obtained an order for AT&T to produce subscriber information, incoming and outgoing text message phone numbers and cell tower location records for the cell phone number A.O. identified as the rapist. AT&T complied, showing
Michael Baker as the phone’s owner. Baker was arrested and charged with second degree rape, second degree and fourth degree sex offense, second degree assault and impersonating a police officer. At trial, the State attempted to admit the call records through the testimony of the trooper, claiming he was an expert who relied on the records during his investigation. The trial court ruled the trooper could testify about calls made but not location. Baker was convicted on all counts and sentenced to 10 years in prison. He appealed, arguing the trial court erred in admitting the call records obtained from AT&T. The Court of Special Appeals agreed, finding the State did not show how the records were produced in order to qualify within the non-hearsay category. Further, the court found the records were not admissible under the business records exception because a proper foundation was not laid. The judgment was reversed and the case remanded for further proceedings.

*Ed. Note:* Assistant Attorney General Brenda Gruss in the Maryland Attorney General’s Office represented the State.

**Fourth Amendment: Warrantless Search of Cell Phone**

*People v. Colon, 2015 V.I. LEXIS 94 (August 5, 2015).* The Virgin Islands Superior Court ruled the search and seizure of defendant’s cell phone violated the Fourth Amendment. William Hyde was found beaten and unconscious near Magens Bay, and later died from his injuries. Hyde’s daughter subsequently reported his truck missing, and police reviewing a video recording of Magens Bay saw a truck with the same description exiting the beach driven by Khalif Francis. Francis was arrested for unauthorized use of a vehicle and/or tampering with a vehicle and taken to the Juvenile Bureau. Francis’ cell phone, seized from him during the arrest, was not given back to him when he was released into his parents’ custody, and the police later searched for and obtained its contents without a warrant. Pursuant to the investigation, Francis and three other defendants, all minors, were arrested for attacking Hyde and charged with murder, assault and using a dangerous weapon in the commission of a crime. Among other arguments, Francis moved to suppress the information taken from his cell phone on Fourth Amendment grounds. The Superior Court agreed, finding Francis had a significant expectation of privacy in his cell phone contents, and the State had not shown he had given consent to search. The motion to suppress was granted as to the evidence seized from his cell phone.

*Ed. Note:* Assistant Attorney General Daniel Huston, U.S. Virgin Islands Department of Justice, represented the People.

**Probable Cause: Affidavit for CSLT**
Commonwealth v. Augustine, 472 Mass. 448 (August 18, 2015). The Massachusetts Supreme Court ruled that the trial court erred in allowing defendant's motion to suppress. Pursuant to a murder investigation, the Commonwealth obtained an order for and received more than 64 pages of cellular site location information (CSLI) records of Shabazz Augustine's cell phone from his provider. Augustine was subsequently indicted for the murder, and he then filed a motion to suppress the CSLI evidence, arguing the Commonwealth had violated his Fourth Amendment rights. The trial court allowed the motion, and the Supreme Court concluded such a search would be permissible only upon a showing of probable cause, vacating the allowance of the motion and remanding the case for consideration of whether the supporting affidavit by a State trooper demonstrated probable cause. The trial court ruled the probable cause standard had not been met, and again allowed the motion to suppress; the Commonwealth sought interlocutory review of the order. The Supreme Court found probable cause was demonstrated to conclude that, based on Augustine's CSLI, he committed the arson of the victim's vehicle, which in turn provided a basis for concluding that he was involved in committing the victim's murder and depositing the body in the river. The court found the facts in the affidavit suggested Augustine had both the opportunity and the motive to harm the victim and had committed suspicious acts, the timing and content of which suggested his involvement in the crime. The order was reversed and the case remanded.

Fourth Amendment: Plain View Exception
State v. Cardwell, 2015 S.C. App. LEXIS 206 (Sept. 2, 2015). The South Carolina Court of Appeals ruled the lower court properly denied the motion to suppress the video file. Sarah Cardwell took her laptop for repair to a technician, who explained repairing it would entail downloading the data from the hard drive, rebuilding the hard drive and then reloading the extracted data. As the technician was downloading Cardwell's data, a police chief came by with some packages and saw what appeared to be a video of child pornography featuring Cardwell's two minor children. The police chief instructed the technician to make a copy of the video, and took the copy and the laptop to a sheriff's department investigator. The investigator obtained a search warrant for the contents of the laptop prior to sending it to the computer lab for analysis. Cardwell was subsequently indicted on two counts of unlawful conduct toward a child and two counts of first-degree sexual exploitation of a minor. Prior to trial, Cardwell moved to suppress both the video and laptop, arguing the laptop was unlawfully searched and both were unlawfully seized in violation of the Fourth Amendment. The lower court denied the
motion, ruling there was no Fourth Amendment violation because Cardwell relinquished any expectation of privacy in her laptop when she turned it over for repair. Further, the court found the video images fell within the plain view of the police chief. During trial, Cardwell twice unsuccessfully renewed her motion to suppress. She moved for a directed verdict, which was also denied. The jury found Cardwell guilty on all charges. Cardwell then again renewed her motion to suppress and moved for a new trial; both motions were denied. Cardwell was sentenced to two years on each count of unlawful conduct toward a child, to run concurrently, and three years on each count of sexual exploitation of a minor, to run concurrently, and she was required to register as a sex offender. Cardwell appealed on the suppression issue. The appeals court found the lower court properly denied the motion to suppress pursuant to the plain view exception to the warrant requirement. The court also noted the inevitable discovery doctrine further supported the denial of the motion to suppress. The judgment was affirmed.

Ed. Note: Assistant Attorney General William Blitch Jr. of the South Carolina Attorney General’s Office represented the State.

And see...

U.S. v. Oates, 2015 U.S. App. LEXIS (11th Cir. Sept. 16, 2015). The Eleventh Circuit Court of Appeals ruled seizure of the computer did not violate defendant’s Fourth Amendment rights. Agents using P2P software downloaded child pornography from an IP address traced back to Exie Oates, a 60-year-old woman with no criminal history. When they went to her residence, the door was answered by an adult male who identified himself as her son, Christopher Oates. Once inside the residence, agents saw a computer that was actively running P2P software. Oates admitted he had downloaded child pornography and agreed to go to the police station. The agents also seized the computer, later obtaining a search warrant for the hard drive’s contents. Prior to trial, Oates moved to suppress the child pornography files, which he argued were seized illegally. The U.S. District Court for the Middle District of Georgia denied the motion, making a factual finding that agents had probable cause to believe the computer contained illegal contraband and that exigent circumstances existed for them to seize the computer because of concerns evidence would be damaged or removed. A jury found Oates guilty of possession of child pornography, and the district court sentenced him to 120 months’ imprisonment and lifetime supervised release. He appealed on the same issues as his pretrial motion. The appeals court found that once agents entered
the residence, the computer displaying a P2P downloading file was in plain view, and coupled with their prior investigation of downloading at that IP address, the computer's incriminating nature was immediately apparent. The court found that even if agents had not lawfully seized the computer under the plain view doctrine, exigent circumstances existed for them to seize it. The judgment was affirmed.

**CDA: Website Content Development**  
The Washington Supreme Court ruled the plaintiffs were not exempted from proceeding on their state tort law claims. Advertisements featuring J.S. and other minor girls were allegedly posted on Backpage.com, a website owned and maintained by Village Voice Media Holdings. J.S. was allegedly raped multiple times by customers who responded to the ads. J.S. filed suit against Backpage alleging negligence, sexual exploitation of children, vicarious liability, unjust enrichment, invasion of privacy, sexual assault and battery and civil conspiracy under state law. Backpage moved to dismiss because of immunity under the Communications Decency Act, 47 U.S.C. § 230. J.S. argued that Backpage was not immune from suit in part because its advertisement posting rules were designed to help pimps develop ads that could evade unwanted attention from law enforcement while still conveying the illegal message. The trial court denied the motion, and Backpage moved for discretionary review. The Court of Appeals granted review and certified the case to the Supreme Court. The Supreme Court found that while the CDA shields website operators from state law liability for merely hosting content developed by users, it does not protect website operators who develop the content. The court ruled the plaintiffs were not preempted under the CDA from proceeding because they alleged sufficient facts that, if proven true, would show that Backpage helped to produce the illegal content shown on the website. The trial court's denial of the motion to dismiss was affirmed, and the case remanded.

**Fourth Amendment: Cell Phone Location Records**  
*State v. Perry*, 2015 N.C. App. LEXIS 769 (Sept. 15, 2015). The North Carolina Court of Appeals found no error in non-suppression of the records of the location of defendant's cell phone. A police detective made an arrest for possession of marijuana, and the arrestee gave the detective the phone number of his drug supplier. The arrestee also called that number on speakerphone in the presence of the detective and set up a drug buy. The detective then successfully applied for a phone records production order to access records associated with that telephone number, seeking complete account and billing information and complete call detail

pg. 12
records with cell site location information. Accordingly, AT&T provided the records, including the location of the cell tower “pings” whenever a call was made to or from the phone. Based upon those “pings,” the detective located the phone at a hotel room but, before he could prepare the search warrant, his surveillance team saw the occupants had been tipped off and were leaving and stopped them. The occupants had plastic grocery bags which were open enough for the team to see drug paraphernalia, and the team arrested Paul Perry and two other individuals. A grand jury indicted Perry for trafficking by possession of heroin; trafficking heroin by sale; trafficking heroin by transportation; conspiracy to traffic heroin by transportation, possession and sale; and maintaining a dwelling used for keeping or selling controlled substances. Perry moved pretrial to suppress the search of his phone and cell site location records, arguing it was an unreasonable warrantless search in violation of the Fourth Amendment; the motion was denied. A jury found Perry guilty on all charges, and he was sentenced to mandatory minimum sentences of 225 to 282 months imprisonment for the three trafficking convictions, to run concurrently; 14 to 26 months imprisonment for sale of heroin and six to eight months imprisonment for intentionally maintaining a dwelling to sell controlled substances, to run concurrently with the mandatory sentences. Perry appealed on the same grounds as his pretrial motion. The appeals court held it was not error to deny the suppression motion for Perry’s cell phone location records because the records were historical third party records properly disclosed under a court order. The court found retrieval of the information was not a “search” requiring a warrant under the Fourth Amendment as no physical trespass occurred. The court noted Perry voluntarily conveyed the information to his buyer, so he showed no reasonable expectation of privacy. The judgment was affirmed.

**Probable Cause: GPS Surveillance**

*State v. Urdiales*, 2015 Ohio 3632 (Sept. 8, 2015). The Ohio Court of Appeals ruled the warrantless search of defendant’s person was supported by probable cause. Based on an informant’s tip related to the possession and trafficking of cocaine, a sheriff obtained a search warrant authorizing installation and monitoring of a GPS tracking device on a minivan registered to Roberto Urdiales’ mother. The device was placed on the vehicle, which was tracked. Law enforcement then initiated a stop, ordered the driver out of the vehicle and conducted a pat-down for weapons. A K-9 unit arrived and cocaine was found on the driver, Roberto Urdiales. Urdiales was charged with possession of drugs, a felony of the fifth
degree. He pleaded not guilty, then filed a motion to suppress evidence obtained from the stop and search, alleging the search warrant and the stop and search of his vehicle were not based on probable cause. At the hearing on the motion, the sheriff testified that the vehicle’s movements and their timing were consistent with the information provided by the informant. Another sergeant testified about knowing the vehicle was being monitored, and they also knew what time the drug activity was going to occur. The court denied the motion. Urdiales changed his plea to no contest. The trial court found him guilty and sentenced him to 11 months in prison. He appealed on the same grounds as before. The appeals court found the officers had reasonable suspicion to stop the vehicle based on the vehicle’s description, its movements on the GPS tracking monitor and their knowledge of when the drug activity was to occur. The court further found the warrantless search of Urdiales was supported by probable cause because a reliable informant had provided a detailed tip, which was corroborated by the GPS surveillance and observations on the scene. The judgment was affirmed.

And some federal cases of note....

**Statute of Limitations: Unauthorized Access to Social Media Account**

_Sewell v. Bernardin, 2015 U.S. App. LEXIS 13542 (2nd Cir. Aug. 4, 2015)._ The Second Circuit Court of Appeals ruled that plaintiff’s claim arising out of her AOL account was properly dismissed based on the two-year statute of limitations. Chanty Sewell filed suit alleging that Phil Bernardin, her former boyfriend, had gained access to her email and Facebook accounts without permission in violation of the Computer Fraud and Abuse Act (CFAA) and the Stored Communications Act (SCA). On or about August 1, 2011, Sewell could not sign in to AOL as her password had been altered. That same month, malicious statements about her sex life were emailed to family and friends. On February 24, 2012, Sewell was unable to log into her Facebook account, and on March 1, 2012, someone posted a public message from her Facebook account containing the same malicious statements. Sewell alleged that Bernardin obtained her passwords without permission while he was a guest at her home, and Verizon Internet records confirmed that Bernardin’s computer was used to gain access to the server on which Sewell’s accounts were stored. On May 15, 2013, Sewell filed suit against Bernardin’s wife, which was settled on September 27, 2013. On January 2, 2014, Sewell filed this action. Bernardin moved to dismiss as time-barred, and the U.S. District Court for the Eastern District of New York granted the motion, finding that her suit was time-barred under the Acts’ two-year limitations periods. The appeals court found that
Sewell's claim arising out of her AOL account was properly dismissed based on the statute of limitations, which ran from the date she discovered that she could not access the account. However, the court found her Facebook-related claims accrued six months later when she could not access her Facebook account, and those claims were filed within the two-year period. The court further ruled that her discovery that the AOL account had been accessed did not give her reasonable opportunity to discover that another account might be compromised. The judgment was affirmed in part, vacated in part, and remanded.

**Burden of Proof: Deletion of Emails**

*U.S. v. Katakis*, 2015 U.S. App. LEXIS 15340 (9th Cir. Aug. 31, 2015). The Ninth Circuit Court of Appeals found the Government failed to carry its burden to show destruction or concealment of emails. Andrew Katakis became the primary focus of a federal investigation into a scheme to rig bids at foreclosure auctions. When Katakis learned federal investigators had subpoenaed his bank records, he installed DriveScrubber, a program designed to wipe hard drives clean of all information, on his home computer. DriveScrubber overwrites all data in the unallocated, or free, space of a hard drive, permanently erasing any files. Katakis also installed a different version of DriveScrubber on the computers of his co-conspirator, Steve Swanger, to delete all of the emails. The Government seized all four computers, finding 10 incriminating emails in the deleted items folder on one of Swanger's computers that implicated Katakis. The metadata showed that Katakis had received and opened all of them. The Government was unable to find those emails on the other computers, leading it to believe Katakis had destroyed them with DriveScrubber. Based on this discrepancy, the Government charged Katakis with obstruction of justice, alleging he deleted, and caused others to delete, electronic records. At trial, the Government's expert witness testified that Katakis "double-deleted" emails by deleting them once from the mail client and again by emptying the deleted items folder. Katakis' expert testified it would be impossible for DriveScrubber to overwrite double-deleted emails, and was able to recover thousands of them, but not the 10 incriminating emails; in rebuttal, the Government's expert admitted it was impossible for DriveScrubber to delete the incriminating double-deleted emails. However, the jury convicted Katakis, who then filed a motion for judgment of acquittal, alleging the evidence was insufficient to convict him. The U.S. District Court for the Eastern District of California agreed, vacated the conviction and entered a judgment of acquittal. The Government appealed. The appeals court agreed the Government had not carried its burden to show Katakis' actual destruction or concealment of the emails. The
court noted the Government’s first theory was based only on speculation that Katakis’ DriveScrubber program had overwritten the email transmission logs, but there was no evidence that the logs were made available for the program to overwrite. The court ruled no reasonable juror could have found the Government carried its burden to show that double deletion of incriminating emails occurred. The court affirmed the district court’s order of acquittal. 

Ed. Note: The Government did not charge Katakis with attempted obstruction of justice, which might have produced a different result.

**Reasonable Suspicion: Violation of Supervised Release Conditions**

*U.S. v. Hilton*, 2015 U.S. App. LEXIS 16210 (6th Cir. Sept. 9, 2015). The Sixth Circuit Court of Appeals found suppression of the phone and evidence was not warranted. Paul Hilton was convicted of distribution and transportation of child pornography and was sentenced to 60 months’ imprisonment, followed by three years of supervised release. His supervised release was subject to several conditions, including not subscribing to Internet services without permission from his probation officer, not possessing or using a device with Internet capability and not possessing or using a computer without permission. He also had to submit his person and residence to a search by a probation officer based on reasonable suspicion or evidence of a violation of a condition of his supervised release. During his release, his probation officer received a tip that Hilton had a profile on the social network Mocospace, and the tip provided a link to that profile. The officer checked it out, and recognized the profile picture as that of Hilton, who was holding a camera phone in the picture. He also determined it was a recent picture because he recognized the surroundings as the house where Hilton had been living only since his release. The officer believed Hilton had violated his release conditions, including having a camera phone and a social media profile without permission. A probation search team went to Hilton’s residence, where Hilton admitted to possessing child pornography on a Blackberry (which the team found at the home) and admitted to having profiles on both Mocospace and Mbuzzy, another social media site. An FBI agent later obtained a warrant for the contents of the Blackberry, finding many images and movies of child pornography as well as text messages about exchanging such images. A grand jury charged Hilton with 24 counts related to production, transfer, receipt and transportation of child pornography. Hilton filed a motion to suppress the Blackberry for lack of reasonable suspicion during the warrantless search. He also moved to suppress the evidence on the Blackberry and his confession as fruits of his unwarned statements during the initial search of his residence. The U.S. District Court for
the Eastern District of Missouri denied both motions, and Hilton entered a guilty plea for two counts of conspiracy to produce child pornography, reserving his right to appeal the suppression motions. The district court sentenced him to 40 years imprisonment followed by lifetime supervised release, and Hilton appealed. The appeals court found the probation officer had reasonable suspicion of Hilton's violation of his supervised release conditions based on the profile picture of Hilton holding a camera phone. The court further found that suppression was not warranted because none of the evidence was fruit of Hilton's unwarned statements since the officer would have discovered the phone regardless of any unwarned statements, and the lawfully obtained information would have justified issuance of the warrant for the phone contents apart from the unwarned statements. The denial of the motions to suppress was affirmed.

Hedda Litwin is the Editor of the Cybercrime E-Newsletter and may be reached at 202-326-6022. The Cybercrime E-Newsletter is a publication of the National Association of Attorneys General. Any use and/or copies of this newsletter in whole or part must include the customary bibliographic citation. NAAG retains copyright and all other intellectual property rights in the material presented in this publication. NAAG, 2030 M Street, NW, Eighth Floor, Washington, DC 20036 (202) 326-6000 | http://www.naag.org/