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 human trafficking 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.

SEPTEMBER-OCTOBER 2014 ISSUE

OCTOBER IS NATIONAL CYBERSECURITY AWARENESS MONTH

National Cybersecurity Awareness Month has been observed every October since its inception in 2004 to encourage cyber vigilance and protection by all computer users. However, its sponsors, the U.S. Department of Homeland Security and the National Cyber Security Alliance remind us that cybersecurity is a year-round effort. In recognition of that effort, the NAGTRI Cybercrime eNewsletter begins a series of "Cyber Tips" in each issue.

This issue’s Cyber Tip: Only install mobile applications from trusted sources. Trust may be difficult to establish from the limited information available on a download site, so it is important to read the third party reviews and look at ratings before you download. If an application is requesting more permissions than seems necessary, don’t install it, or if you have already done so, uninstall it.

ATTORNEYS GENERAL FIGHTING CYBERCRIME

Fifty-one Attorneys General, the Federal Trade Commission (FTC) and the Federal Communications Commission reached a $105 million settlement with AT&T Mobility LLC, resolving allegations AT&T engaged in “mobile cramming.” AT&T allegedly placed charges for third party services for premium text message subscriptions on cell phone bills without customer knowledge or consent. The settlement requires AT&T to provide $80 million for refunds to affected customers, with the fund to be administered by the FTC. AT&T also agreed to cease billing customers for premium text message subscriptions and to take steps to ensure customers are only billed for authorized charges.
Forty-four Attorneys General sent a letter to the leadership of the U.S. Senate Judiciary Committee and a House Judiciary Subcommittee calling on them to bring the Amy and Vicky Child Pornography Victim Restitution Improvement Act of 2014 (S. 2301/H.R. 4981) to a vote. The legislation would allow full restitution to victims of child pornography to pay for needed resources.

Nine Attorneys General reached an $850,000 settlement with TD Bank, N.A., resolving an investigation into a 2012 data breach affecting thousands of consumers. The agreement requires TD Bank to notify customers of any future breaches of security or other acquisitions of personal information in a timely manner and to maintain reasonable security policies to protect personal information. It also ensures no backup tapes will be transported unless encrypted and all security protocols are in place. TD Bank will also review its security policies on a bi-annual basis and make changes as required, as well as institute employee training. The Attorneys General joining the agreement represent Connecticut, Florida, Maine, Maryland, New Jersey, New York, North Carolina, Pennsylvania and Vermont.

Arkansas Attorney General Dustin McDaniel’s Cyber Crimes Unit agents arrested Zachary Nehus on 30 counts of possession of child pornography, a Class C felony. Agents had executed a search warrant at Nehus’s residence and seized a desktop computer, several iPads and cell phones and other electronic evidence, to be analyzed at the Unit’s Forensic Lab.

California Attorney General Kamala Harris reached a $28.4 settlement with rent-to-own furniture business Aaron’s, Inc., resolving allegations the company permitted its franchised stores to install spyware on laptop computers rented to customers. A spyware program called “Detective Mode,” installed without customers’ consent or knowledge, allowed the franchises to remotely monitor keystrokes, capture screenshots, track physical locations and even activate webcams. The settlement requires Aaron’s to refund $25 million to state customers and pay $3.4 million in civil penalties and fees.

Delaware Attorney General Beau Biden announced Andrew Alvarez, who had been arrested by the Delaware Child Predator Task Force, was sentenced to 10 years in prison after pleading guilty to two counts of Dealing in Child Pornography. The Task Force investigation revealed he used an online peer-to-peer network to download
and share images of child pornography. The case was prosecuted by Deputy Attorney General Abigail Layton, co-director of the Task Force.

**Illinois Attorney General Lisa Madigan’s** investigators and the Winnebago Sheriff’s Office arrested Christopher Fitzgerald on eight counts of possession of child pornography, a Class 2 felony punishable by three to seven years in prison, and two counts of reproduction of child pornography, a Class X felony punishable by six to 30 years in prison.

**Iowa Attorney General Tom Miller** announced the Council on Licensure, Enforcement and Regulation (CLEAR) awarded its James L. Guffey National Certified Investigator and Inspector Training Development Award to Senior Investigator Michael Ferjak. The award recognizes an individual who has made an outstanding contribution to the enhancement of CLEAR’s programs. Ferjak is assigned to the Iowa Crimes Against Children Task Force.

**Kentucky Attorney General Jack Conway’s** Cybercrimes Unit arrested Sean Graham on one count of possession of child pornography, a class D felony carrying a penalty of one to five years in prison. The Unit executed a search warrant at Graham’s residence and seized computers believing to contain child pornography.

**Louisiana Attorney General Buddy Caldwell** announced the arrest of former Sorrento mayor Wilson Longanecker, Jr. on 40 counts of possession of child pornography and one count of obstruction of justice pursuant to a joint law enforcement investigation. The investigation involved Attorney General Caldwell’s Cyber Crime Unit, the Ascension Parish Sheriff’s Office, Homeland Security Investigations and Louisiana State Police. If convicted as charged, Longanecker faces up to 20 years in prison on each count.

**Massachusetts Attorney General Martha Coakley** announced State Police assigned to her Office arrested Mark Hedgecock, a Level 3 sex offender, on charges of Possession of Child Pornography. The investigation into Hedgecock began after receiving information from the National Center for Missing and Exploited Children about an email account allegedly obtaining child pornography and later linked to Hedgecock. State Police executed a search warrant for Hedgecock’s email account, finding images of child pornography. Hedgecock has two previous convictions relating to assault of a child. The case is being
prosecuted by Assistant Attorney General Tom Ralph, Chief of Attorney General Coakley’s Cybercrimes Division.

**Mississippi Attorney General Jim Hood’s** Cyber Crime Unit investigators arrested Willard Knight for possession of child pornography. The arrest was made through Attorney General Hood’s Internet Crimes Against Children Task Force. If convicted as charged, Knight faces up to 40 years in prison.

**Acting New Jersey Attorney General John Hoffman’s** Division of Criminal Justice Specialized Crime Bureau obtained a grand jury indictment charging three men who operate a private auto inspection business with fraudulently using data simulators to generate false results on motor vehicle emissions inspections. Christopher Alcantara, owner of Five Stars Auto Inspection; Mariano Alcantara; and Lewis Alcantara-Sosa are accused of accepting payment for using simulators instead of data link connectors to enable faulty vehicles to pass inspections. Gary Davis, a customer, was also indicted for allegedly knowingly paying for passing results for limousines he drove. The men are charged with conspiracy, computer theft, tampering with public records and two counts of violation of the Air Pollution Control Act. Deputy Attorneys General Debra Conrad and Michael King of the Division presented the case to the grand jury. The lead Division investigators are Detective Sean Egan and State Investigator Ruben Contreras.

**New York Attorney General Eric Schneiderman** issued “Airbub in the City,” a report finding widespread illegality in New York City listings on the Airbub website. Among the report’s findings were: 1) a small group of hosts generated 37 percent of the listing revenue; 2) several units appeared to serve as illegal hostels, with multiple, unrelated guests sharing the same unit; and 3) short-term units are displacing the City’s long-term housing options. The report is based on data obtained by Attorney General Schneiderman’s Office via subpoena.

**Ohio Attorney General Mike DeWine** reached a settlement with Darren Sizemore, who is accused of sending unsolicited and deceptive text messages to consumers nationwide. According to Attorney General DeWine’s lawsuit, the messages instructed recipients to visit certain websites to claim free gifts, and Sizemore received compensation from third parties for driving traffic to the sites. To receive the gifts, consumers were asked to provide personal information or to sign up for trial offers requiring upfront payments or enrollment in membership programs. Those requirements to claim gifts were not disclosed in the initial text
messages. Under the settlement, Sizemore agreed to stop sending deceptive and unsolicited text messages, pay $2,400 in consumer damages and pay a $25,000 civil penalty, of which $17,000 will be suspended upon full compliance with the agreement.

Oklahoma Attorney General Scott Pruitt’s agents and other members of the Internet Crimes Against Children Task Force arrested Shane DeRyckere after an investigation revealed DeRyckere posed as a teenage girl to solicit underage users to submit obscene pictures of minors. The investigation resulted from a tip from the National Center for Missing and Exploited Children. DeRyckere was charged with two counts of possession of child pornography, one count of distribution of child pornography, two counts of downloading obscene materials and one count of transmitting information by computer for the purposes of instigating sexual conduct with a minor.

Pennsylvania Attorney General Kathleen Kane’s Child Predator Section agents arrested David Ellenberger, a registered sex offender, who allegedly traveled to meet a “father” he believed would allow his five-year-old daughter to participate in sexual acts. The “father” was actually an undercover agent. Ellenberger is charged with one count each of unlawful contact with a minor, criminal attempt of rape of a child, criminal attempt of involuntary deviate sexual intercourse with a child, indecent assault and criminal use of a communications facility. If convicted as charged, he faces a minimum of 25 to 50 years in prison. Ellenberger will be prosecuted by Deputy Attorney General Anthony Marmo of the Section.

Vermont Attorney General William Sorrell announced Justin Bywater, who pleaded guilty to three counts of felony Possession of Child Pornography, was sentenced to three to 12 years imprisonment, all suspended, and placed on probation for 12 years. While on probation, Bywater will be required to complete sex offender treatment; register as a sex offender; and obtain permission before visiting places where children congregate, have unsupervised contact with his son, have any contact with other children or have access to the Internet or any device with recording capabilities. The conviction resulted from an investigation by Attorney General Sorrell’s Office and the Internet Crimes Against Children Task Force.

Virginia Attorney General Mark Herring, U.S. Attorney for the Eastern District of Virginia Dana Boente and Adam Lee, Special Agent in Charge of the FBI’s
Richmond Field Office, announced Cameron Bivins-Breeden was sentenced to 288 months in prison, followed by a life term of supervised release, for using Facebook to entice and attempt to entice 38 minors to produce and send him sexually explicit photographs of themselves. In multiple instances, he used the threat of sending the images to the victims’ family and friends to exhort additional pictures. Bivens-Breeden pled guilty to one count each of production of child pornography and enticement of a minor. Assistant Attorney General and Special Assistant U.S. Attorney Samuel Fishel and Assistant U.S. Attorney Eric Siebert prosecuted the case.

Washington Attorney General Bob Ferguson filed suit against Internet Order LLC and its CEO, Daniel Roitman, d/b/a Stroll, for violations of the federal Restore Online Shoppers Confidence Act. The company, an online marketer of foreign language audio courses via the website pimsleurapproach.com, offers an introductory set of CDs for $9.95, but purchasers were unknowingly and automatically enrolled in a “negative option” purchase plan obligating them to receive up to four additional courses at a cost of $256 each. In order to avoid charges, customers were required to obtain special authorization from the company to ship the CDs back at their own expense within 30 days or be automatically charged. Customers were also charged a $64 “restocking” fee and subjected to high pressure sales tactics. The case is being handled by Senior Counsel Paula Selis.

Wisconsin Attorney General J.B. Van Hollen announced Benjamin Lahti pleaded no contest to child enticement, a Class D felony with a maximum penalty of up to 25 years imprisonment and fines of up to $100,000. The plea resulted from an Internet Crimes Against Children Task Force investigation involving Attorney General Van Hollen’s Division of Criminal Investigation agents and investigators from Brown and Door counties. Lahti had posted an online ad for a sexual encounter, and an undercover officer, posing as a 15-year-old girl, responded. Assistant Attorney General Karie Cattanach is representing the State.

CYBER NEWS BRIEFS

Encryption Used in Only 4% of Breaches
Encryption was used in only 10 of the 237 disclosed data breaches occurring worldwide during the second quarter of 2014, according to data protection firm SafeNet’s Breach Level Index report. According to the report, only two incidents
during that period were classified as “secure breaches,” meaning strong encryption, authentication solutions or key management rendered the breached data unusable to hackers. The full report may be accessed at http://breachlevelindex.com/pdf/Breach-Level-Index-Report-Q22014.pdf.

NY Extends Comment Period for Proposed Virtual Currency Regs
The New York State Department of Financial Services, the first state agency to propose regulations specifically governing the crypto-currency industry, extended by an additional 45 days the comment period for the draft regulations to October 21, 2014. The draft regulations include rules on consumer protection, the prevention of money laundering and cybersecurity. A “BitLicense” would be required for Bitcoin exchanges and for companies securing, storing or maintaining custody or control of virtual currencies on behalf of their customers.

ABA Delegates Pass Cybersecurity Resolution
The American Bar Association (ABA) House of Delegates approved Resolution 109 on cybersecurity, making clear there was no intent to impose new ethical obligations on lawyers and emphasizing the suggested course of action may have different parameters for small law firms. The Resolution states: “RESOLVED. That the American Bar Association encourages all private and public sector organizations to develop, implement and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected.”

FBI Facial Recognition Program Fully Operational
The FBI’s facial recognition system, three years in development, is now fully operational. Called the Next Generation Identification (NGI) system, it includes a controversial feature called the Interstate Photo System (IPS). IPS will serve as “an image-searching capability of photographs associated with criminal identities” and mixes traditional mug shot photos with non-criminal faces extracted from employment records and background check databases. The system is expected to collect as many as 52 million faces.

IN THE COURTS

CELL PHONE FACILITATION OF CRIME: CONSENT
U.S. v. Arrellano, 2014 U.S. App. LEXIS 12654 (7th Cir. July 2, 2014). The Seventh Circuit Court of Appeals ruled the admission of the cell phone was harmless error in light of other evidence. Faustino Arrellano was arrested pursuant to a federal task force investigation of drug traffickers and was charged with one count of conspiring to possess heroin and cocaine with intent to distribute and two counts of using a cell phone to facilitate that conspiracy. At trial, the government introduced Arrellano's cell phone, as well as wiretapped conversations with Arrellano's alleged co-conspirators. He moved to suppress the cell phone, as well as statements made to law enforcement and a voice identification obtained at his arrest. The U.S. District Court for the Northern District of Illinois suppressed the voice identification and statements, finding he was in custody without Miranda warnings, but not the cell phone, finding Arrellano's roommate and alleged co-conspirator had apparent authority to, and voluntarily did, consent to the search of the apartment where authorities found the cell phone. A jury found Arrellano guilty on all counts, and he moved for an acquittal or a new trial, which was denied. He was sentenced to 120 months in prison and five years of supervised release. He appealed, arguing the district court should have suppressed his cell phone, and the evidence was insufficient for conviction. The appeals court found overwhelming evidentiary support to conclude a reasonable jury could have found Arrellano guilty on all counts. As to the cell phone, the court found the roommate's consent to search was involuntary and made under duress, but concluded its admission was harmless error in light of the other evidence. The conviction was affirmed.

STALENESS OF WARRANT: TWO MONTH DELAY
State v. Fuller, 2014 UT 29 (July 11, 2014). The Supreme Court of Utah ruled the information in the warrant was not stale. A police officer conducting an online child pornography investigation using LimeWire, the peer-to-peer file-sharing program, learned the IP address associated with files containing child pornography was assigned to Robert Fuller, who shared a home with his younger brother, Bradley, and a cousin. Officers obtained a warrant to search the entire premises and seize computer hardware and software, documentation and other electronic devices. Robert Fuller told officers he did not use LimeWire, but his brother did. Bradley Fuller ("Fuller") admitted to using LimeWire and to downloading child pornography. Using ImageScan software, officers then searched and seized Fuller's computer, finding child pornography images and videos. The U.S. Attorney's Office declined to prosecute, but the State filed a criminal information, charging Fuller with 10 counts of sexual exploitation of a minor, all second-degree felonies. Fuller moved to suppress the evidence seized and
statements he had made during the search, arguing the warrant lacked particularity because it only identified the IP address rather than the user or computer. The trial court denied the motion, concluding the warrant was sufficiently particular and based on probable cause. Fuller then filed an interlocutory appeal, which was also denied. He pled guilty to five counts of voyeurism, reserving the right to appeal the order denying his motion to suppress. He was sentenced to concurrent prison terms of one to 15 years on all counts. On appeal, Fuller again raised his particularity argument but also argued the warrant lacked probable cause because the information in the supporting affidavit was stale due to a two-month gap between the initial search and the warrant application. As to particularity, the State high court found having more specific identifiers than the IP address would have merely narrowed the scope, but not prevented the finding, of probable cause. The court also rejected Fuller's staleness claim, finding staleness is not determined only by the passage of time but by the facts of the case. The court noted child pornography crimes are generally carried out in secrecy for a long period of time, so the time limitations for other more fleeting crimes are inapplicable. Since a mere two months had passed between the search and the warrant application, the court found the information providing probable cause was still fresh. The order was affirmed.

*Ed. Note:* Assistant Attorney General Jeffrey Gray of the Utah Attorney General's Office represented the State.

**FOURTH AMENDMENT: PRIVACY OF SUBSCRIBER INFORMATION**

*State v. Fielding,* 2014 Ohio App. LEXIS 3030 (July 15, 2014). The Ohio Court of Appeals, 10th Appellate District, ruled defendant had no reasonable expectation of privacy in his subscriber information. A police officer conducting an undercover Internet investigation of child pornography identified an IP address containing file names related to child pornography and downloaded a video file from the computer associated with that IP address, finding it contained child pornography. The officer prepared a subpoena to AT&T for the associated subscriber information, which identified Matthew Fielding as the subscriber. A search warrant was executed at Fielding's residence, and officers seized a laptop and hard drive; subsequent analysis revealed both devices contained files of child pornography. A grand jury returned indictments against Fielding of eight counts of pandering sexually oriented matter involving a minor, all second-degree felonies; and eight counts of pandering sexually oriented matter involving a minor, all fourth degree felonies. Fielding filed a pre-trial motion to suppress all evidence, arguing law enforcement illegally obtained his subscriber information from AT&T in violation of
his Fourth Amendment rights, which the trial court denied. Fielding then waived his right to a jury trial and was found guilty of three counts of the fourth-degree felony and one count of the second-degree felony. He was sentenced to a seven-day jail term, a five-year term of community control and ordered to register as a Tier II sex offender. He appealed, again raising his Fourth Amendment argument as well as arguing the evidence was insufficient to convict. The appeals court found Fielding’s rights under the Fourth Amendment were not implicated, as he had no reasonable expectation of privacy in his subscriber information. Further, the court ruled the weight and sufficiency of the evidence supported Fielding’s convictions because there were multiple files on both the laptop and hard drive containing child pornography, which Fielding was determined to have knowingly possessed and published. The judgments were affirmed.

**WARRANTLESS SEARCH: EXIGENT CIRCUMSTANCES**

McCowan v. State, 10 N.E. 3d 522 (Ind. App. April 23, 2014). The Indiana Court of Appeals ruled in light of the emergency situation, the warrantless search of defendant’s cell phone records did not violate his constitutional rights. Dustin McCowan had a heated argument at his house with Amanda Bach, his ex-girlfriend. His next-door neighbor heard three shots and a man’s voice saying “Amanda, get up” twice. McCowan took Bach’s vehicle and left it in the parking lot of a general store, as evidence later showed. The store owner contacted police, finding the vehicle’s side door open, a tire slashed and the hazard lights flashing. After learning Bach, who was now missing, had been with McCowan, police contacted McCowan, but he denied any knowledge of Bach’s whereabouts. Police filed an exigent circumstances request to obtain cell phone records from Verizon for both McCowan and Bach; they asked for the time, date and phone numbers for all calls and text messages made and received the evening before until the present, as well as information about the cell towers through which activity was transmitted and latitude and longitude coordinates for Verizon’s estimated location of the phone at the time of each call or message. The records included the content of the text messages. Bach’s body was later found approximately 300 yards from McCowan’s home; she had been shot in the neck at close range. A shirt found nearby was found to contain McCowan’s DNA. McCowan was arrested for murder. At trial, McCowan moved to suppress his phone records, arguing exigent circumstances did not exist to justify the invasion of his privacy and were used to build a case against him, rather than locate Bach. The trial court, noting the lateness of the motion, denied it. A jury found McCowan guilty, and he was sentenced to 60 years of incarceration. He appealed, and the appeals court ruled he had waived the
challenges in his motion to suppress because he failed to properly object at trial. Nevertheless, the court ruled police officers had not violated McCowan’s constitutional rights and affirmed the judgment. 

*Ed. Note: Angela Sanchez, Deputy Attorney General in the Indiana Attorney General’s Office, represented the State.*

_and see…_

**State v. Subdiaz-Osorio, 2014 WI 87 (July 24, 2014).** The Supreme Court of Wisconsin found the search did not violate defendant’s Fourth Amendment rights. Nicolas Subdiaz-Osorio, an illegal alien from Mexico, fatally stabbed his brother and fled. Police suspected he was carrying the murder weapon and was heading to Mexico, and acting through the Wisconsin Department of Justice, requested his cell phone provider to track his cell phone location, leading to Subdiaz-Osorio’s arrest. Subdiaz-Osorio moved to suppress all evidence obtained after his arrest, arguing the tracking of his cell location information violated his Fourth Amendment rights. The trial court denied the motion, and Subdiaz-Osorio pled guilty to a lesser charge of first-degree reckless homicide, then appealed. The court of appeals affirmed, and state supreme court review was sought. The supreme court found the tracking of Subdiaz-Osorio’s cell phone location fell within the exigent circumstances exception to the warrant requirement because there was a threat to safety and the risk of destruction of evidence, given no murder weapon had been recovered at the murder scene and there was a likelihood Subdiaz-Osorio would flee to Mexico, where he had family. Therefore, the court found the search did not violate his Fourth Amendment rights, and the judgment was affirmed. *Ed. Note: Assistant Attorney General Daniel O’Brien represented the State.*

**WARRANTLESS SEARCH: INDEPENDENT SOURCE DOCTRINE**

*State v. Russo, 2014 Ida. LEXIS 194 (July 31, 2014).* The information obtained from the warrantless search of the cell phone was admissible under the independent search doctrine. A victim reported a rape and told police the offender took pictures during the rape with his cell phone. Michael Russo, a convicted sex offender, came under suspicion for committing the rape. A detective obtained a warrant authorizing a search of Russo’s residence. Prior to executing the warrant, officers saw Russo leave his apartment; they detained him and removed his cell phone from his pocket. A detective looked through what was stored on the phone and saw a video of a rape, then turned the phone off. Officers searched the apartment pursuant to the warrant and found two cell
phones. The detective sought and obtained an amended search warrant authorizing
the search of the three phones. Russo was indicted, and moved to suppress the
video found on his cell phone on Fourth Amendment grounds, which was denied. A
jury found Russo guilty of Rape, Kidnapping in the First Degree and Burglary and he
was sentenced for each crime to life without the possibility of parole, life with the
first 40 years fixed and a fixed 10 years, all to run concurrently. He appealed,
challenging the denial of his motion to suppress, and the state court of appeals
affirmed the conviction. He then filed a petition for review, which was granted.
The state Supreme Court found the information obtained during the warrantless
search of the cell phone was admissible under the independent source doctrine.
Disregarding the information produced by the unlawful search of the cell phone,
there was still sufficient information from the victim's statements to provide
probable cause for the issuance of an amended search warrant to search the data
contained on that phone. The judgment was affirmed.

Ed. Note: Deputy Attorney General Kenneth Jorgensen represented the State.

ADMISSIBILITY: FACEBOOK MESSAGES
of Appeals found the admission of the Facebook messages was harmless in light of
other evidence against defendant. Crystal Clay learned Marquita Thomas was in a
relationship with DiMarkus Williams, Clay's former boyfriend. She went to Thomas'
apartment and the women fought, leading to Clay slashing Thomas with a box
cutter. Thomas received 28 staples for her injuries at the hospital, and pressed
charges the next day. During the investigation, a police officer accessed Clay's
Facebook profile and printed a copy of her comments, later to be introduced into
evidence at trial. A jury found Clay guilty of aggravated assault, and she was
sentenced to three years in prison, with two years of post-release supervision, and
ordered to pay $150 in restitution. Clay filed a post-trial motion, which was
denied, and then appealed, arguing the State failed to lay a proper foundation for
admitting Facebook postings into evidence. Although the officer had testified to
how he accessed the site, the court noted there was no testimony or other proof
the photo or the profile belonged to Clay. The court found the State failed to
prove the Facebook comments were Clay's. However, the court also noted three
witnesses to the fight had testified that Clay stabbed Thomas. The court affirmed
the judgment, finding although the Facebook messages should not have been
admitted because they were not authenticated, their admission was harmless
because of the other evidence of Clay's guilt.

Ed. Note: Special Assistant Attorney General Barbara Byrd represented the State.
FOURTH AMENDMENT: CELL SITE INFORMATION

State v. Tate, 2014 WI 89 (July 24, 2014). The Wisconsin Supreme Court ruled the search was executed pursuant to an order compliant with the Fourth Amendment. Police responding to a homicide outside of a market found one victim fatally shot. They obtained a description of the shooter from witnesses, and the market’s surveillance camera footage showed a person with the same description purchasing a prepaid cell phone in the market, leaving and shooting the victim. The clerk selling the phone said the suspect identified himself as “Bobby” and said he had just gotten out of prison. The store gave police the telephone number assigned to the phone and its serial number, and police used two databases to confirm US Cellular as the service provider. The ADA obtained an order approving 1) the installation and use of a trap and trace device and a pen register device; and 2) the release of subscriber information, including cell tower activity and location and GPS information identifying the physical location of the phone. Upon receiving cell site information from US Cellular, police used a stingray to locate the phone within an apartment building. They found Bobby Tate asleep in his mother’s apartment with the cell phone and arrested him for first-degree intentional homicide. Tate moved to suppress the evidence seized pursuant to the order to track his cell phone, arguing police needed a search warrant to track his phone, and the order they had was insufficient. The trial court denied the motion, concluding the order was sufficient, so Tate pled no contest and then appealed the suppression decision. The court of appeals affirmed, concluding the court had a substantial basis for finding probable cause to issue the order. Tate sought review of the decision, and the state Supreme Court found the trial judge had a sufficient factual basis for finding probable cause, and the use of the serial number of the phone satisfied the particularity requirement; therefore the order met the requirements of the Fourth Amendment, and law enforcement officers performed a legal search when they tracked Tate’s cell phone. The decision was affirmed.

And see...

Ford v. State, 2014 Tex. App. LEXIS 9159 (August 20, 2014). The Texas Court of Appeals, Fourth District, found defendant had no reasonable expectations of privacy in the cell site data. Jon Ford was charged with the murder of his ex-girlfriend at her house. Although he claimed he was nowhere near her house, the State introduced evidence which included historical cell phone data reflecting activity on Ford’s phone in the vicinity of her house at the time of the murder.
Ford moved to suppress the cell site data as a violation of his Fourth Amendment rights, which was denied. A jury found Ford guilty, and on their recommendation, the court sentenced him to 40 years in prison. On appeal, he raised 18 points of error, including the contention the trial court failed to suppress the historical cell phone records obtained from AT&T. The appeals court noted the cell site data acquired by the State was simply the business records memorializing Ford’s voluntary subscriber transaction with AT&T for the service he wanted, so the fact that the data revealed the general location of his cell phone was immaterial to the legal analysis. The court ruled the State did not violate Ford’s Fourth Amendment rights because he did not have a reasonable expectation of privacy in the information he voluntarily conveyed to a third party. After disposing of the other issues raised, the court affirmed the judgment.

SEARCH OF CELL PHONE RECORDS: PAROLEE STATUS
State v. Cotham, 2014 Tenn. Crim. App. LEXIS 763 (July 31, 2014). The Tennessee Court of Criminal Appeals ruled a search warrant was not needed because of defendant’s status as a parolee. Corey Cotham was convicted by a jury of first degree premeditated murder in the shooting death of Victoria Bozza and especially aggravated robbery and was sentenced to life and 25 years, to be served consecutively. Much of the evidence presented at trial resulted from a series of cell phone calls between Cotham and Timothy Bozza, the victim’s estranged husband, who was also indicted and tried separately. The cell phone call records were obtained by law enforcement pursuant to an exigent circumstances request to the cell phone provider, rather than a search warrant, and provided a partial basis for a search warrant to obtain Cotham’s photographs, physical samples, fingerprints and DNA. On appeal, and among many other arguments, Cotham maintained the trial court erred in denying his pretrial motion to suppress evidence obtained from the search warrant, arguing the cell site location information relied upon by the search warrant as probable cause was obtained without a search warrant and violated Cotham’s constitutional rights. The appeals court, noting Cotham was a convicted felon on parole, agreed with the trial court that a search warrant for the cell site records was not needed because of Cotham’s parolee status. The judgment was affirmed.

Ed. Note: Assistant Attorney General Clark Thornton of the Tennessee Attorney General’s Office represented the State.

TESTIMONIAL EVIDENCE IN JURY ROOM: “UNCLEAN” LAPTOP
Napier v. Commonwealth, 2014 Ky. App. LEXIS 140 (August 15, 2014). The Kentucky Court of Appeals ruled the use of an unclean computer during jury deliberations was error. Tracy Napier was indicted by a grand jury and charged with one count of attempted murder. His first trial ended in a hung jury. Napier was retried, and during jury deliberations, the jury asked to replay the CD of a witness' interview with a detective. The trial court stated it could not spare its computer to show the CD, so the prosecutor volunteered her laptop, and it was taken into the jury room. Defense counsel did not object to the laptop being taken into the jury room, nor did counsel request that any replay of testimony be done in open court. Napier was found not guilty of attempted murder, but guilty of first-degree assault, and he was sentenced to 10 years imprisonment. He appealed, arguing among other claims that the trial court erred in permitting the jury to replay the testimony of a witness using the prosecutor's "unclean" computer in the jury deliberation room. "Unclean" was defined in this case as the laptop's hard drive was not swiped of all data, including data related to the instant case. The appeals court concluded the trial court erred 1) when it allowed the jury to review testimonial evidence in the privacy of the jury deliberation room; 2) when it allowed the jury to review testimonial evidence without Napier's presence; and 3) when it allowed the use of an unclean laptop to review evidence during deliberations. The case was reversed and remanded.

SCOPE OF SEARCH: CONSENT

U.S. v. Watkins, 2014 U.S. App. LEXIS 14261 (11th Cir. July 28, 2014). The Eleventh Circuit Court of Appeals concluded the search was valid because the wife's consent was independent of appellant's. During questioning in an unrelated investigation, Charles Watkins admitted to having downloaded and viewed child pornography. A detective asked Watkins for permission to search his computers for information about the unrelated investigation, not for a search for child pornography, and he agreed. Watkins' wife later independently consented to a general search of the computers. Watkins was subsequently charged with receipt of child pornography via the Internet based on the evidence of child pornography obtained during the search. Watkins moved to suppress the evidence from his computers, and the U.S. District Court for the Middle District of Florida denied the motion, reasoning that although the detective's assurances limited the scope of Watkins' consent to evidence about the unrelated investigation, the consent of Watkins' wife authorized a general search and permitted finding the child pornography. Watkins moved for reconsideration of the motion, which was denied. He was found guilty after a bench trial and sentenced to 60 months' imprisonment,
and he appealed. The appellate court agreed, finding the consent of Watkins’ wife was independent of his and was for a full search of the computers. The court noted the record contained no indication that Watkins raised any objection to that consent. The judgment was affirmed.

WARRANTLESS SEARCH: PROBATION CONDITIONS

State v. Purtell, 2014 WI 101 (August 1, 2014). The Supreme Court of Wisconsin ruled the probation agent had reasonable grounds to believe defendant’s computer contained contraband. Jeremiah Purtell was convicted of two felony counts of mistreating animals and was placed on probation with a probation condition of not possessing or using a computer without permission from his probation agent. Purtell did not surrender his computers as required, so the probation agent took him into custody and confiscated a laptop, desktop and related computer equipment. The agent searched one of the computers without a warrant, found child pornography and contacted local law enforcement, who obtained search warrants for all the equipment. The resulting search revealed multiple child pornography files, and Purtell was charged with eight counts of possession of child pornography. He moved to suppress the evidence seized from the computers, arguing it was obtained in violation of his Fourth Amendment rights since the agent lacked both a warrant and reasonable grounds to conduct the search. The trial court denied the motion, concluding there were reasonable grounds to believe the computer contained contraband. A jury found Purtell guilty on four counts. He appealed the conviction and the order denying his motion to suppress, and the court of appeals reversed, concluding the agent did not have reasonable grounds to search without a warrant. The State petitioned for review, and the state high court ruled the trial court properly denied the motion to suppress. The court found the probation agent had reasonable grounds to believe Purtell’s computer, which he knowingly possessed in violation of the conditions of his probation, contained contraband. The judgment was reversed.

Ed. note: Assistant Attorney General Sandra Tarver of the Wisconsin Department of Justice represented the State.

LEGISLATIVE NEWS

Fourth Amendment Protection

Missouri voters approved Constitutional Amendment 9, adding electronic data and communications to the Fourth Amendment protection from unreasonable searches.
and seizures. The amendment passed the State Senate by a vote of 31-1 and the State House by a vote of 114-28.

Online Posting of Mug Shots
California Governor Jerry Brown signed into law S.B. 1027, a bill prohibiting the solicitation or acceptance of a fee to remove or refrain from publishing a booking photograph, public entities being exempted. The legislation provides a private civil action for damages in an amount equal to the greater of $1,000 per violation or the actual damages suffered, in addition to costs and reasonable attorney's fees. It has been chaptered as Chapter 194 of the Civil Code.

Law Enforcement Use of Drones
On September 28, 2014 California Governor Jerry Brown vetoed A.B. 1327, a bill to require a law enforcement agency to obtain a warrant to use an unmanned aircraft, with the following exceptions: 1) in emergency situations with an imminent threat of life or of great bodily harm; 2) to assess the need for first responders in traffic accidents; and 3) to inspect state parks and wilderness for illegal vegetation or fires.

Access to Motor Vehicle Electronic Recording Devices
On October 2, 2014 the New Jersey Assembly Consumer Affairs Committee passed A3579, a bill limiting access to information from motor vehicle electronic data recorders, known as “black boxes,” to the owner of the vehicle. A law enforcement officer would need a warrant to be allowed access to the information. The legislation also prohibits a motor vehicle owner from destroying the information for two years following an accident causing injury or death; violators would face a $5,000 civil penalty. If enacted, the legislation would take effect immediately. The companion Senate bill, S2433, was introduced on September 22, 2014 and referred to the Law and Public Safety Committee.