ATTORNEYS GENERAL SAY
MOBILE CRAMMING MUST BE STOPPED

On June 24, the National Association of Attorneys General (NAAG) sent comments to the Federal Trade Commission (FTC) urging action to stop mobile cramming, the placement of unauthorized third-party charges on mobile phone bills.

Mobile cramming practices are increasing nationwide, and Attorneys General are continuing to receive consumer complaints about unauthorized charges on their mobile phone bills, usually in amounts from $9.95 to as much as $24.95, and for goods and services they neither requested nor used. Consumers are usually unable to get a full refund for these charges, and are often unable to discontinue future charges.

The NAAG comments focus on four areas of particular concern:

1. Unauthorized charges placed on consumers’ bills for unwanted and unused services;
2. Inadequate disclosure of third party charges on mobile phone bills;
3. Inadequate procedures for consumers to effectively block future charges and obtain refunds, and
4. Lack of state and federal statutory protections governing consumer disputes about fraudulent or unauthorized charges on mobile phone bills.

The comments were signed by 40 Attorneys General of the following states and territories: Alaska,

A copy of the NAAG comments can be accessed at http://www.naag.org/sign-on_archive.php.

ATTORNEYS GENERAL FIGHTING CYBER CRIME

MULTI-STATE

Connecticut Attorney General George Jepson and Maryland Attorney General Douglas Gansler sought information from Living Social Inc., the daily deals website, regarding a recent data breach affecting as many as 50 million accounts. The Attorneys General asked the company to provide a detailed timeline of the incident, including when and how the company discovered the breach, in addition to a breakdown on the number of individuals affected in each state and the types of information compromised. They also requested information about the data storage, password protection and internal security systems the company had in place and whether the company received any complaints or reports of unauthorized charges from users. The Attorneys General also requested an outline of any plan developed to prevent recurrence of a breach, a timeline of that plan’s implementation, copies of any security reports or forensic analyses related to the incident and copies of the company’s privacy policies at the time of the breach.

Eight Attorneys General are participating in the Secure Our Smartphones (S.O.S.) Initiative, launched and co-chaired by New York Attorney General Eric Schneiderman and San Francisco District Attorney George Gascon and aimed at encouraging the cell phone industry to adopt technologies to deter theft by drying up the secondary market in which stolen devices are sold. The Initiative will focus on several areas: 1) analyzing patterns, causes and trends behind the device theft problem; 2) investigating the capability of manufacturers to develop technology to deter theft, including a “kill switch” to permanently disable stolen devices; 3) understanding how the economics of device theft have affected the smartphone industry; 4) working with device manufacturers to make a “kill switch,” or another equally deterrent technology, a standard feature on their products; and 5) investigating any impropriety on the part of manufacturers, raising public awareness about industry practices in this area and using all available tools to press for safety-oriented innovation and responsible corporate citizenship. Participating in this Initiative are Connecticut Attorney General George Jepson, Delaware Attorney General Beau Biden, Hawaii Attorney General David Louie, Illinois Attorney General Lisa Madigan, Massachusetts Attorney General Martha Coakley, Minnesota Attorney General Lori Swanson and Nebraska Attorney General Jon Bruning, as well as police chiefs, state legislators, district attorneys and state and local government officials nationwide.

Thirty-three Attorneys General entered into an agreement with the Penguin Group (USA) Inc., resolving a multistate antitrust investigation involving allegations that Penguin colluded with other major publishers and Apple Inc. to manipulate prices in the e-book marketplace. The agreement must be approved by the U.S. District Court for the Southern District of New York. When finalized, the agreement will give e-book outlets greater freedom to reduce e-book prices. Consumers represented by the Attorneys General of the participating states will receive $75 million in compensation. Participating in the settlement are the Attorneys General of Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut,
Delaware, the District of Columbia, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maryland, Massachusetts, Michigan, Missouri, Nebraska, New Mexico, New York, North Dakota, Ohio, Pennsylvania, Puerto Rico, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, West Virginia and Wisconsin.

**ALABAMA**

Attorney General Luther Strange joined U-Haul and the University of Alabama at Birmingham to present the “Arrive Alive: Stop the Texts. Stop the Wrecks” program to raise awareness of the dangers of texting and driving. The event featured the “Save-a-Life Tour, Distracted Driver Program” showcasing high intensity videos, show presenters engaging attendees and simulators. The partnership will also launch a statewide campaign with posters to be located in U-Haul locations in the state.

**ALASKA**

Attorney General Michael Geraghty announced the sentencing of Mark Coombs to four years in prison after he pled guilty to one consolidated count of possession of child pornography. Coombs had organized almost 1,000 images and videos of child pornography and saved them onto cds and thumb drives. Upon release, Coombs must register as a sex offender and will be on probation for six years. A violation of his probation conditions will result in imprisonment for another four years.

**ARKANSAS**

Attorney General Dustin McDaniel’s Cyber Crimes Unit agents arrested John Ross and Amanda Hartie who are each charged with five child pornography counts, a Class C felony. Special Agent Chris Cone of Attorney General McDaniel’s Office began investigating the defendants after suspecting child pornography was possessed at their residence. Unit agents executed a search warrant at the residence, seizing a laptop and other electronic evidence, to be analyzed at the Unit Forensic Lab. The Hot Springs Police Department assisted with both the investigation and arrest. The completed case file will be turned over to Prosecuting Attorney Steve Oliver.

**CALIFORNIA**

Attorney General Kamala Harris announced criminal charges against three brothers who face up to five years in prison for operating an illegal website on which users could watch bootleg versions of copyrighted television shows and movies. Hop Huang, Tony Huang and Huynh Huang were arraigned for allegedly operating mediamp4.com, a website allowing users to illegally stream more than 1,000 titles on computers and mobile devices. Each has been charged with one count of conspiracy, four counts of receiving stolen property and one count of grand theft. The Motion Picture Association of America began investigating the brothers, who were then operating two other illegal websites, and sent them a cease and desist letter. When the brothers resumed illegal operations under a new domain name, Attorney General Harris’ Office initiated an investigation, executed a search warrant and seized property in connection with the operation and filed charges against the brothers. The brothers earned approximately $150,000 in advertising revenue during their 18 months of operation, allegedly generating traffic to the website through Google search ads. The investigation was conducted by Attorney General Harris’ eCrime Unit, California Highway Patrol and REACT, a law enforcement task force specializing in investigating technology and identity theft crimes. The eCrime Unit conducted the forensic analysis of the computer seized during the search and is prosecuting the case.

**COLORADO**

Attorney General John Suthers announced the statewide grand jury indictment of John Parks and Darryl Honowitz on 28 criminal counts related to the state Organized Crime Control Act and felony charges for computer crime, theft, defrauding a secured
creditor, identity theft and forgery. The indictment was based on an 18-month investigation by Attorney General Suthers’ Office and the Colorado Bureau of Investigation. Parks is accused of accessing the Colorado Secretary of State’s website to find delinquent businesses, then using his own name and the identities of others to submit unauthorized Statements Curing Delinquency and of Change. He then acquired the businesses by paying a fee, often submitting false information to Dun and Bradstreet to increase their credit worthiness. Parks and Honowitz also engaged in a lease-back scheme in which leased computer equipment was represented as high-end, and the computers shipped were of much lesser quality and value than represented. Both men were arrested in Florida and will be extradited to Colorado and prosecuted by Attorney General Suthers’ Office.

CONNECTICUT

Attorney General George Jepson sent a letter to Google’s chief executive officer, asking the company to address concerns related to Glass, its new head-mounted computing and recording device, and its potential impact on the privacy of state residents. Attorney General Jepson requested a meeting with Google to discuss concerns including 1) the time frame in which Glass will be available to state consumers for purchase; 2) the terms of Google’s announced restriction on facial recognition capabilities and the privacy protections to be required before permitting facial recognition applications or capabilities; 3) whether Glass will have eye-tracking capabilities; 4) whether Google will allow consumers to store data on the device and how any stored information will be safeguarded should it be lost or stolen; and 5) the information Glass will collect from users and non-users and whether Google will obtain consent to collect such information. Assistant Attorney General Matthew Fitzsimmons, head of Attorney General Jepson’s Privacy Task Force, is assisting on this issue.

DELAWARE

Attorney General Beau Biden announced the arrest of Kevin Boone, a registered sex offender, on 25 counts of dealing in child pornography. The arrest resulted from a Child Predator Task Force investigation into the online distribution of child pornography. The Task Force, along with detectives from the State Police Sex Offender Apprehension and Registration Unit and a DSP #9 trooper, executed a search warrant at an address of suspected child pornography and seized multiple computers and other digital media devices. In addition, the Middletown Police Department, which provided forensic support and facilities, discovered email Boone had received and sent containing multiple files of child pornography, leading to Boone’s arrest. Boone, currently a student at Delaware Technical and Community College, is a Tier 2 sex offender following a 2010 conviction for possession of child pornography.

ILLINOIS

Attorney General Lisa Madigan’s investigators arrested and charged Jeremy Best with five counts of aggravated child pornography, a Class 2 felony punishable by three to seven years in prison. The arrest is part of Operation Glass House, Attorney General Madigan’s statewide initiative to apprehend offenders who download and trade child pornography. The investigators, with assistance from the Springfield Police Department and Sangamon County State’s Attorney’s Office, conducted a search of Best’s residence, arresting him after evidence of alleged child pornography was located. The State’s Attorney’s Office will prosecute the case.

KENTUCKY

Attorney General Jack Conway’s Cybercrimes Unit arrested Robert Walker on eight counts of distribution, and four counts of possession, of child pornography. The charges resulted from the Unit’s undercover investigation, including the execution of
a search warrant at Walker’s residence, with assistance from the State Police.

**LOUISIANA**

Attorney General Buddy Caldwell’s High Technology Crime Unit, joined by U.S. Homeland Security Investigations, the St. Charles Parish Sheriff’s Office, the Greater Lafourche Commission Harbor Police and U.S. Customs and Border Protection, arrested Bruce Wagenstein of Florida on 100 counts of child pornography. The arrest follows a forensic review of Wagenstein’s computer, revealing multiple images and videos depicting child pornography. Wagenstein faces pending child pornography charges in multiple parishes and, if convicted, could receive up to 20 years in prison on each count.

**MASSACHUSETTS**

Attorney General Martha Coakley announced the sentencing of Steven Sheldon, owner of Cafeno’s Internet café, after he pled guilty to charges of organizing or promoting gambling services, operating an illegal lottery, allowing lottery in a building and the sale and advertising of lottery tickets. His corporation pled guilty to the same charges, as well as to charges of aiding, assisting, procuring, counseling or advising a false tax return. Each defendant was sentenced to two years of probation. The court also ordered the forfeiture of more than $250,000 of defendants’ assets to the Commonwealth, $100,000 of which will be forfeited by the corporation as a fine for falsifying tax returns. Cafeno’s ceased operation in March 2011; the case against Stephen Meglioia, Sheldon’s business partner, is still pending. The case was handled by Assistant Attorneys General Thomas Ralph and Timothy Wyse of Attorney General Coakley’s Cyber Crime Division, and Assistant Attorney General Lee Hettinger, Chief of the Western Massachusetts Regional Office. Attorney General Coakley’s Computer Forensic Laboratory, Senior Financial Investigator Mark Pulli, Department of Revenue investigator Thomas Nowicki and State Police assigned to Attorney General Coakley’s Office assisted in the investigation.

**MICHIGAN**

Attorney General Bill Schuette announced the arrest of Kenneth Hilton on 12 child pornography counts. Specifically, Hilton is charged with two counts of Using a Computer to Commit a Crime, a seven-year felony, and 10 counts of possession of child pornography, a four-year felony. The arrest follows an investigation by Attorney General Schuette’s Criminal Division in which both photos and videos of child pornography were found on Hilton’s home computer. Investigators were able to identify some of the pictures as known child pornography stored in a national data base by the National Center for Missing and Exploited Children. Hilton must wear a GPS tether and cannot have any unsupervised visits with children, use a computer or leave the state.

**MISSISSIPPI**

Attorney General Jim Hood announced the sentencing of John Brown after he pled guilty to one count of possession of child pornography. He was sentenced to 20 years, of which 15 years are suspended and five years to serve, in addition to five years post release supervision. Brown also received a $50,000 fine and must register as a sex offender upon release. The case was prosecuted by Special Assistant Attorney General Brandon Ogburn of Attorney General Hood’s Cyber Crime Division.

**NEBRASKA**

Attorney General Jon Bruning announced the arrest of Joseph Benz, a University of Nebraska-Kearney psychology professor, on three counts each of possession and distribution of child pornography. The Kearney Police Department made the arrest following an investigation by Attorney General Bruning’s cybercrimes unit. A search warrant was executed at Benz’s home, with a search of one computer uncovering more than 20,000 questionable im-
age files. The analysis of at least two other computers is in progress.

**OKLAHOMA**

Attorney General Scott Pruitt's investigators arrested David Kennedy on one count of distribution of child pornography and one count of violating the state Computer Crimes Act. A search warrant was also issued for Kennedy's former residence, and the Oklahoma City Police Department assisted in serving the warrant. Computer items were seized and sent to the OSBI Computer Crimes Unit for examination. The case was initiated by a Guthrie police officer who investigates the distribution of child pornography online. During his investigation, Kennedy distributed multiple child pornography videos to that officer, who referred the case to Attorney General Pruitt's Office, a member of the Oklahoma Internet Crimes Against Children Task Force, for further investigation.

**PENNSYLVANIA**

Attorney General Kathleen Kane announced the sentencing of Joshua Albert, who used his Facebook page to threaten Philadelphia District Attorney Seth Williams and FOP President John McNesby. Albert pled guilty to the charges, receiving a term of imprisonment of seven and one half months to 23 months, followed by 24 months of probation. Albert had offered financial incentives on his Facebook page and on a website to anyone who would kill the two men, as well as other police officers.

**TEXAS**

Attorney General Greg Abbott's Cyber Crimes Unit arrested John Williams, a seventh grade teacher, on five third-degree felony counts of possession of child pornography. Based on a referral from the National Center for Missing and Exploited Children, Unit investigators identified Williams as the suspect who illegally uploaded child pornography images to a social networking website. Unit officers executed a search warrant at Williams' residence and seized computers and digital media. They also conducted a search of Williams' classroom and school-issued computer. Unit investigators conducted an initial forensic examination of the flash drive and discovered several images of child pornography. Officers seized the school-issued computer and flash drive for further examination. Each of the counts against Williams is punishable by two to 10 years in prison and up to a $10,000 fine.

**VIRGINIA**

Attorney General Ken Cuccinelli joined U.S. Attorney for the Eastern District of Virginia Neil McBride to announce the sentencing of Adam Stanley to 17.5 years in prison for production of child pornography. He was additionally ordered to pay $205,21 in restitution to the victim and received a term of 20 years of supervised release following his prison term. He will also be required to register as a sex offender upon release. Stanley used a hidden video camera to produce a child pornography video of a child for whom he babysat. He also distributed child pornography videos and images over a peer-to-peer network on the Internet and saved hundreds of videos and images of child pornography on computers and computer media. The case was investigated by the FBI Innocent Images Task Force. Senior Assistant Attorney General and Special Assistant U.S. Attorney Gene Fishel prosecuted the case on behalf of the U.S.

**WASHINGTON**

Attorney General Bob Ferguson's High Tech Unit secured a $97,000 settlement with ZookaWare, a software company based in Arizona, and its owner for engaging in unfair and deceptive practices. The company's products labeled tracking cookies as "infections," misleading consumers into believing they were dangerous, and labeled harmless errors like empty register keys as needing correction. Consumers then had to purchase the products to fix the
“problems.” ZookaWare also allegedly 1) used pre-checked boxes to automatically add to the consumer’s shopping cart; 2) added disclosures of charges in fine print only to “free trials,” 3) provided only minimal disclosure of automatic renewal of products, 4) made cancellation difficult and 5) posted fake positive reviews on social media, known as “astroturfing.” In addition to agreeing to stop the deceptive practices, the company agreed to pay $40,000 in civil penalties, with an additional $85,000 suspended; $57,000 in costs and attorney’s fees; and restitution to state consumers who purchased products and were charged automatic renewal fees. The company will be subject to civil penalties of $25,000 per violation in the future.

**WISCONSIN**

**Attorney General J.B. Van Hollen** announced that a criminal complaint was filed against Rickey Spence for possession of child pornography, a felony. Special agents from Attorney General Van Hollen’s Division of Criminal Investigation (DCI), with assistance from the Kaukauna Police Department, which is a member of the Wisconsin Internet Crimes Against Children Task Force, had previously executed a search warrant at Spence’s home. A forensic preview by a DCI analyst of a hard drive from a desktop computer seized at the home revealed a video file consistent with child pornography located in the computer’s recycle bin. DCI was also assisted by the Outagamie County Sheriff’s Office and the Town of Freedom Police Department.

**COMING SOON: AUDIO OF DC CIRCUIT ARGUMENTS ONLINE**

On May 14, the judges of the U.S. Court of Appeals for the DC Circuit voted unanimously to provide audio recordings of oral arguments before the court available online free of charge. The recordings will be available on the court’s website, [www.cadc.uscourts.gov](http://www.cadc.uscourts.gov), by three p.m. on the same day of the oral argument beginning on September 9, the first day of the court’s 2013-2014 term. An archive of audio recordings as far back as the 2007-2008 term will also be available.

**NASA LAUNCHES SPINOFF IPAD APP**

The National Aeronautics and Space Administration (NASA) released a new iPad app, Spinoff 2012, showcasing dozens of technologies developed by NASA and transferred to the private sector as commercial products or services. Spinoff 2012 organizes them by industry: information technology, health and medicine, transportation, public safety, consumer goods, energy and industrial productivity. The app is NASA’s iPad incarnation of its annual Spinoff publication which since 1976 has featured more than 1,800 space age innovations that went com-
IP THEFT REPORT OFFERS AGGRESSIVE SOLUTIONS

The Commission on the Theft of American Intellectual Property, a U.S. advisory group, released a report estimating annual losses from such theft at more than $300 billion a year. They suggest that affected companies be given the right to aggressively combat such theft, arguing for “…a more permissive environment for active network defense that allows companies not only to stabilize a situation but to take further steps, including actively retrieving stolen information, altering it within the intruder’s networks or even destroying the information within an authorized network.” The commission is headed by Dennis Blair, former director of National Intelligence, and Jon Huntsman, former ambassador to China and former governor of Utah. The report may be accessed at http://ipcommission.org/report/ip_commission_report_052213.pdf.

GSA SEEKS FEEDBACK ON CYBERSECURITY

The General Services Administration (GSA) issued a request for information from industry on how to incorporate cybersecurity standards into government purchasing requirements. The request asks for input on how the government can protect itself while not imposing new barriers to entry for companies seeking to become contractors, as well as input on the kinds of existing redundant standards. The request also solicits information about commercial standards and their applicability to federal purchases. Respondents are asked about their own processes and how they guard against risk. Further, the request delves into “harmonization,” or how conflicts in regulations, contracts or policies related to cybersecurity can be resolved. The GSA has already received several responses.

OMB ISSUES MOBILE SECURITY GUIDELINES

The White House Office of Management and Budget (OMB) published the first government-wide set of mobile computing security guidelines. They include a baseline of standard security requirements for mobile computing, a mobile computing decision framework for federal agencies and a mobile security reference architecture. The documents are significant not only for establishing ways for agencies and industry to develop safer mobile products for use on government networks, but also for the active roles of the Department of Homeland Security, the Department of Defense and the National Institute for Standards and Technology in developing them. The guidelines can be accessed at https://do.gov/wp-content/uploads/downloads/2013/Mobile-Security-Reference-Architecture.pdf.

FACEBOOK REVISES POLICY ON “CRUEL” CONTENT

Facebook unveiled policy changes on posting of controversial material, including making creators of “cruel and insensitive” content more accountable. The changes come in response to an advertising boycott campaign launched by Women, Action & the Media to prevent graphic images and messages against women from being posted on the social network. Facebook said most of the images have been removed, and the company will review policies for evaluating materials deemed to be forms of hate speech and will update the training given to teams in charge of monitoring content on the site. Facebook also promised to “increase the accountability of the creators of content that does not qualify as actionable hate speech, but is cruel or insensitive by insisting that the authors stand behind the content they create.”
COURT: NYC CABS CAN BE HAILED VIA SMARTPHONE

Taxi riders will be able to hail a cab in New York City using smartphone applications after a New York Supreme Court lifted an order blocking the program. However, according to the court decision, the smartphone program is restricted to pickups within one-half mile in the area south of 59th Street. Elsewhere, the range would extend to one and one-half miles. The program, adopted in December 2012 by the New York City Taxi & Limousine Commission (TLC), would run for 12 months and exempt areas such as airports with provisions for taxi lines. Participation in the program is optional, although all licensed city cab drivers are eligible, subject to Commission approval. The Livery Roundtable, Black Car Assistance Corp. and several car service firms had sued the TLC, claiming the program violates city codes and may let drivers discriminate against minorities. The Supreme Court dismissed the suit and lifted an injunction blocking the program from going forward.

NEW MEASURE TO COMBAT IP THEFT PROPOSED

The Administration proposed to strengthen its approach to combating online piracy and protecting intellectual property, outlined in the “2013 Joint Strategic Plan on Intellectual Property Enforcement.” The plan includes reaching out to private sector entities not previously involved in the initiative, including domain name registries, search engines, cyber-lockers and other digital storage services. It also calls for working with rights holders to adopt best practice guidelines. Further, the Administration hopes to encourage the growth of legitimate alternatives for accessing works, such as facilitating the development of copyright registries and online databases, micro-licensing arrangements and other market-driven mechanisms. The 2013 Plan can be accessed at http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

IN THE COURTS

ONLINE HARASSMENT: ALTERATION OF SOCIAL MEDIA PAGE

The People v. Kucharski, 2013 Ill. App. LEXIS 179 (March 29, 2013). The Illinois Appellate Court, Second District, rejected defendant’s argument that the Harassing or Obscene Communications Act, 720 ILCS 135/1-2 was unconstitutional. Steven Kucharski appealed a lower court judgment convicting him of two counts of violating that statute and one count of unlawful use of encryption. He argued the statute was unconstitutional under the First Amendment, which the appeals court rejected because there was no content-based discrimination. The court found the evidence was sufficient to support Kucharski’s conviction because 1) the victim testified that after she saw the changes on her social media, she called Kucharski who laughed at her and
told her she deserved it; 2) the victim testified she and Kucharski had broken up and were not on good terms; 3) the victim testified that Kucharski helped her create the page and only she and Kucharski knew the password; and 4) the victim’s page had been accessed from a computer at Kucharski’s home address. The court also held the evidence was insufficient to support Kucharski’s conviction of unlawful use of encryption because his changing the password of the account did not alter a file or prevent law enforcement from tracking him down. His convictions for harassment through electronic communications were affirmed but his conviction for unlawful use of encryption was reversed.

QUALIFICATION OF EXPERT: DAUBERT FACTORS

U.S. v. Springstead, 2013 U.S. App. LEXIS 7473 (4th Cir. April 15, 2013). The Fourth Circuit Court of Appeals ruled the district court’s decision to qualify a special agent as a computer forensics expert was not an abuse of discretion. Robert Springstead was convicted in the U.S. District Court for the Eastern District of Virginia of distribution, possession and three counts of receipt of child pornography and receipt and possession of obscene visual representations of the sexual abuse of children. He appealed, arguing that the district court abused its discretion in qualifying the special agent as an expert in computer and Internet forensics. The appeals court disagreed, noting the district court heard considerable evidence about the agent’s education, experience, expertise and personal involvement in the case and found the agent had the requisite knowledge, training and experience in operating the Forensic Tool Kit he used in his computer forensic investigation. To the extent Springstead alleged the district court inadequately considered factors such as testing, peer review, error rates and acceptability in the relevant scientific community, the appeals court found the test of reliability was “flexible,” and Daubert’s list of specific factors neither necessarily nor exclusively applied to all experts or in every case. The court affirmed the district court’s judgment.

FOURTH AMENDMENT: CELL PHONE SEARCH INCIDENT TO ARREST

Smallwood v. State, 2013 Fla. LEXIS 887 (May 2, 2013). The Florida Supreme Court ruled the search of the cell phone when there was no reasonable belief it contained evidence violated the Fourth Amendment. The Florida First District Court of Appeal affirmed Cedric Smallwood’s conviction and sentence for robbery and possession of a firearm by a convicted felon following the denial of his motion to suppress. The court certified a question as to whether the U.S. Supreme Court’s decision in U.S. v. Robinson, 414 U.S. 218 (1973), allowed an officer to search through photographs on a cell phone that had been on an arrestee’s person if there was no reasonable belief the cell phone contained evidence of a crime. First, the state Supreme Court held the conformity clause in Fla. Const. art. I, § 12 did not require state courts to apply Robinson to the search of a cell phone incident to arrest. The court noted that when the cell phone was removed from Smallwood’s person, it could not be used as a weapon or to destroy any evidence that might have existed, so neither the officer protection nor the evidence preservation justification for the search incident exception applied. The court found the officer had to obtain a warrant before searching the contents and data in the phone, so the search violated the Fourth Amendment. The court answered the question in the negative and quashed the appellate court’s decision. The case was remanded for further proceedings consistent with the opinion.

And see also...

U.S. v. Wurie, 2013 U.S. App. LEXIS 9937 (1st Cir. May 17, 2013). The First Circuit Court of Appeals ruled suppression of the evidence obtained from a warrantless search of defendant’s cell phone
was warranted. Brima Wurie was taken to the police station after his arrest on one count each of possessing with intent to distribute, distributing cocaine base and being a felon in possession of a firearm and ammunition. Two cell phones were taken from him. Officers noticed that one of the phones was repeatedly receiving calls, and they were able to see the caller ID screen. The officers accessed the phone’s call log and found the phone number associated with the caller ID they saw. At trial, Wurie moved to suppress the evidence obtained from the search of the cell phone as a violation of his Fourth Amendment rights, which was denied by the U.S. District Court for the District of Massachusetts. A jury found Wurie guilty on all three counts, and he was sentenced to 262 months in prison. He appealed the denial of his motion to suppress. The appellate court determined suppression of the evidence was warranted because the search incident to arrest exception did not authorize the warrantless search of data on the cell phone. Further, there was no showing by the government that such a search was necessary to protect the arresting officers or preserve destructible evidence. The appellate court reversed the denial of Wurie’s motion, vacated the conviction and remanded the case to the district court.

**FOURTH AMENDMENT: PROBABLE CAUSE**

*State v. Shields*, 2013 Conn. LEXIS 159 (May 28, 2013). The Supreme Court of Connecticut found there was a reasonable basis for the court to find the defendant used his computer to obtain child pornography. Robert Shields was charged with possession of child pornography in the first degree and importing child pornography. At trial, he filed two motions to suppress photographic and video recorded images depicting child pornography discovered by police on his home computer pursuant to a warrant; both motions were denied. Shields entered a conditional plea of nolo contendere to the possession charge, and the State entered a nolle prosequi as to the importation charge. He was found guilty of the possession charge and appealed, arguing that the trial court violated his rights under the Fourth Amendment by denying his motion to suppress. The Appellate Court held the search warrant was supported by probable cause and affirmed the trial court judgment. He appealed, but the state Supreme Court found there was a reasonable basis for the issuing court to believe Shields used his computer to obtain child pornography. The court noted the search warrant affidavit, which delineated an instant message sent by Shields to a known collector of child pornography expressing his interest in and requesting copies of such images. Further, the court noted the affiant’s experience with the Internet crimes against children task force, providing a substantial basis for the issuing court to credit his observations about the retrieval of deleted pornographic images from Shields’ computer. The judgment was affirmed.

And see...

*Checo v. State*, 2013 Tex. App. LEXIS 7029 (June 11, 2013). The Texas Court of Appeals, Fourteenth District, found the officer’s affidavits provided probable cause for the search. Al Checo was convicted of attempted sexual assault of a child, aggravated kidnapping and 27 counts of possession of child pornography. He appealed the possession conviction, arguing the officer’s affidavits did not provide probable cause under the Fourth Amendment. The court of appeals disagreed, noting that the officer found the child to be credible. He recounted how she told him Checo lured her into his truck, took her to his townhouse, showed her pornography on a computer and pulled down his pants. The officer also clearly delineated in his affidavit, based on his experience, training and discussions with other experienced investigators, links between Checo’s alleged actions and the likelihood he possessed child pornography. The affidavit also established Checo
as having an interest in and ready access to pornography, as established by the fact he showed pornography to the child. The judgment was affirmed.

Also see...

*Commonwealth v. Rousseau*, 2013 Mass. LEXIS 353 (June 5, 2013). The Supreme Court of Massachusetts found the affidavit in support of the warrant application was sufficient to establish probable cause. During the investigation of some fires, police applied for a warrant to place a GPS device on Michael Dreslinski’s pickup truck as an instrument of that criminality. Information obtained from the GPS revealed that the truck was at or near the scene at about the same time as fires set at four different locations. Dreslinski and John Rousseau, the passenger in the truck, were indicted on charges of arson, breaking and entering, malicious destruction of property and malicious injury to a railroad. They moved to suppress evidence obtained from the GPS, which was denied, and both were subsequently convicted. They appealed, claiming a violation of their Fourth Amendment and state constitutional rights in the attachment of the GPS device to the truck. The Supreme Court found Dreslinski had standing as the owner and operator of the truck and Rousseau, as a passenger in the truck, also had standing based on his expectation of privacy. The court further found the GPS monitoring of the truck constituted a search. However, the court also ruled the affidavit submitted in support of the warrant application was sufficient to support a finding of probable cause that Rousseau participated with Dreslinski in setting the fires. The convictions were affirmed.

**FOURTH AMENDMENT: FOREIGN WIRE-TAP ORDER**

*U.S. v. Lee*, 2013 U.S. App. LEXIS 11496 (1st Cir. June 7, 2013). The First Circuit Court of Appeals found the collaboration between a U.S. law enforcement agency and its foreign counterpart did not give rise to an agency relationship sufficient to implicate the Fourth Amendment. Stephen Lee, a U.S. citizen, was charged in the U.S. District Court for the Eastern District of New York of conspiring to distribute 1,000 kilograms or more of marijuana knowing it would be unlawfully imported into the U.S. He moved to suppress evidence obtained from wiretap orders executed against him abroad by a Jamaican law enforcement agency which had a close and ongoing collaboration with its U.S. counterpart. He also moved to compel the wiretap application materials and documentation. Upon conviction, he appealed the denial of both motions. First, the appellate court held ongoing, formalized collaboration between a U.S. law enforcement agency and its foreign counterpart does not, by itself, give rise to an agency relationship between the two agencies sufficient to implicate the Fourth Amendment abroad. In the instant case, the Jamaican investigation of Lee was an independent undertaking taken before the DEA began their investigation. Jamaican law enforcement officials did not solicit the views of the DEA agents, nor were DEA agents involved in the actual interception. Therefore, the court concluded the trial court correctly denied the motion to suppress. Further, the appellate court concluded the Fourth Amendment exclusionary rule does not impose a duty on U.S. law enforcement to review the legality, under foreign law, of wiretap surveillance applications considered by foreign courts. Therefore, Lee was not entitled to discovery of the wiretap materials underlying the surveillance. The decision was affirmed.

**FOURTH AMENDMENT: SCOPE OF WARRANT**

*Jeffers v. Commonwealth*, 2013 Va. App. LEXIS 184 (June 18, 2013). The Virginia Court of Appeals held the search of defendant’s barn was valid under the Fourth Amendment. Patrick Jeffers was charged with 18 counts of possession, and one count of reproducing, child pornography. He moved to sup-
press the evidence obtained pursuant to a search warrant, which was denied. He was convicted and then appealed the denial of his suppression motion. The search warrant authorized officers to search a residence described as a single wide trailer and “all persons, vehicles or outbuildings located within the curtilage.” Jeffers argued the officers misinterpreted the scope of the warrant to include the barn. He claimed the officers could not search the barn when they discovered he was living there because it was no longer within the scope of the warrant. The appeals court disagreed, finding the trial court did not err in denying the motion to suppress evidence obtained pursuant to the warrant because the search was valid under the Fourth Amendment. They noted police had traced child pornography to that address but did not know in which buildings the child pornography transactions were occurring. The warrant did not state the barn could be searched only if no one resided in it; it identified the trailer as the owner’s residence and then specifically identified the barn with no mention of whether anyone lived there. The court therefore concluded the officers properly searched the barn as the warrant directed, affirming the trial court judgment.

EMAIL AS ESTATE PROPERTY: FORUM SELECTION CLAUSE

Ajemian v. Yahoo! Inc.. 2013 Mass. App. LEXIS 73 (May 7, 2013). The Appeals Court of Massachusetts ruled that Yahoo! failed to show enforcement of its forum selection provisions against plaintiffs was reasonable. After John Ajemian’s death, Yahoo! refused to allow Marianne and Robert Ajemian, co-administrators of his estate, to access his Yahoo! email account. They sued Yahoo! seeking a declaration that email messages the decedent sent and received using a Yahoo! account were property of the estate. The probate court dismissed the suit based on res judicata and on a forum selection clause in Yahoo!’s terms of service (TOS) agreement requiring suit to be brought in California. On appeal, the appeals court ruled res judicata did not bar the action because the estate’s entitlement to the contents of the emails was never at issue; the Ajemians had only sought production of email header information in the first action. The court further found Yahoo! had failed to meet its burden of establishing by undisputed facts that the TOS’ forum selection and limitations provisions were reasonably communicated and accepted by the decedent, and enforcement of those provisions against the Ajemians, who were not parties to the TOS, was reasonable. The court noted the decedent was living in Massachusetts at the time of his death, and there was no relationship between the estate or the email account to California that would make in rem jurisdiction over the emails reasonable in California. The judgment dismissing the complaint was reversed, and the case remanded.

SEARCH AND SEIZURE: VALIDITY OF CONSENT

People v. Lyons, 2013 Ill. App. LEXIS 367 (June 10, 2013). The Illinois Appellate Court, Second District, ruled defendant’s wife could consent to the search. Kevin Lyons appealed his conviction for possession of child pornography, challenging the denial of his motion to suppress evidence from electronic media his wife gathered from their home and delivered to the police. The appellate court found Lyons did not reserve the metal cabinet or the disks inside for his use only, either by installing security measures or directives to his wife and, therefore, she could give valid consent to the search. The judgment was affirmed.

POST ARREST SEARCH: VALIDITY OF WARRANT

U.S. v. Smith, 2013 U.S. App. LEXIS 11365 (8th Cir. June 6, 2013). The Eighth Circuit Court of Appeals ruled the post-arrest warrant to search defendant’s bag was valid. An agent began investigating an individual who posed as a bank customer’s
employee, contacted the bank and tried to set up a “cash vault delivery.” The agent linked cash vault questionnaires to a user name, linked the user name to an online account and saw Mario Smith in several videos belonging to the account. An agent identified Smith’s voice on the suspect’s phone recording. Agents then arrested Smith and seized a messenger bag containing a laptop, a cell phone and bank records. Smith moved to suppress evidence from the contents of the bag, which the U.S. District Court for the Eastern District of Missouri denied. Smith entered a conditional guilty plea to one count of bank fraud, three counts of aggravated identity theft and one count of conspiracy, and then appealed. The appellate court determined that suppression was not warranted because 1) agents had probable cause to arrest Smith since he was a suspect in a similar scheme and his voice was identified as the individual calling the bank to set up the scheme; 2) the seizure of the bag was justified to preserve evidence; 3) the inventory search of the bag was not merely a pretext to search for evidence; and 4) the post-arrest warrant to search the bag was valid since any allegedly false statement or omission was not intentionally made. The lower court ruling was affirmed.

**LEGISLATIVE UPDATE**

**Email Privacy**

TEXAS: ENACTED. On June 14, Governor Rick Perry signed HR 2268 into law, a bill requiring law enforcement to obtain a search warrant before accessing stored electronic communications. The new law, which amends Texas Article 18-02 on criminal procedure, is applicable to search warrants issued both in state and out of state. Further, it stipulates an ISP receiving a subpoena or court order for a subscriber’s electronic data may not inform the subscriber of the issuance of that subpoena. The law is effective immediately.

**Internet Sales Taxes**

PASSED SENATE. On May 6, the U.S. Senate passed S. 743, the Marketplace Fairness Act, a bill co-sponsored by Senators Richard Durbin (D-IL) and Mike Enzi (R-WY) authorizing each state to collect taxes on the sale of remote goods and services. The bill was forwarded to the House, where it has been referred to the Judiciary Committee.

**NEW RESOURCES**

**Cell Phones in Prisons; Camera Surveillance Systems**


**Digital Data Device Test Results**

“Test Results for Digital Data Acquisition Tool: FTK Imager CLI 2.9.0_Debian” reports the results from testing FTK Imager CLI 2.9.0_Debian against the Digital Data Acquisition Tool. It can be accessed at [http://ncjrs.gov/pdfiles1/nij/242138/pdf](http://ncjrs.gov/pdfiles1/nij/242138/pdf).

**Justice System Marginal Costs**


**State Crime Trends and Grant Statistics**

“The BJA State and Territory Fact Sheets” provide information about Byrne Justice Assistance
grant program highlights, as well as statistics and information on crime trends and criminal justice agencies. It can be accessed at http://www.ncjrs.gov/bjareleases/stateterritoriesfs.html.

**Crime Victim Services**

“Vision 21: Transforming Victims Services Final Report” is a comprehensive assessment of the crime victim services field and includes findings, recommendations and strategies. It can be accessed at http://ovc.ncjrs.gov/notices/email/vision21/v21_justinfo.html.

**Childhood Bullying**

This recently published research indicates that victims of childhood bullying have a greater risk of developing mental health problems later in life. It can be accessed at http://archpsyc.jamanetwork.com/article.aspx?articleid=1654916#METHODS.