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

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

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

________________________

TRAINING ON MOBILE DEVICES

The National Association of Attorneys General Training and Research Institute (NAGTRI) Mobile Devices: Evidentiary Considerations for Prosecutors training will take place in Washington, D.C. on June 9-10, 2014 at the Marriott Georgetown. Through funding provided by the Mission Foundation, NAGTRI will provide scholarships to Assistant Attorneys General to attend the training.

This 1.5 day course will provide attendees with an understanding of more complex evidentiary issues arising when mobile devices are an element in their cases. It is designed for attorneys with a working knowledge of search and seizure of evidence and who have handled cases involving digital evidence. Topics planned include mobile phone searches and considerations, mobile device data recovery, Fourth Amendment considerations and special concerns in searches of juveniles’ cell phones.

Please note this is an advanced course with limited attendance, so offices are not guaranteed a slot at the training. Applicants will be accepted on a first come, first serve basis, with priority given to wide state representation and no previous attendance at an advanced class.

For additional information, please contact Hedda Litwin, NAGTRI Program Counsel and NAAG Cyberspace Law Chief Counsel, at hlitwin@naag.org or (202) 326-6022 or Noreen Leahy, NAGTRI Program Specialist, at nleahy@naag.org or (202) 326-6252.
SUPREME COURT LIMITS RESTITUTION FOR CHILD PORN VICTIMS

On April 23, 2014, the U.S. Supreme Court, in an opinion by Justice Anthony Kennedy, ruled 5-4 in Paroline v. United States. 12-8561, that a victim of child pornography may be entitled to restitution under 18 USC § 2259, but only to the extent the defendant's offense proximately caused the victim's losses. Below is a summary of that ruling written by Dan Schweitzer, NAAG Supreme Court Counsel.

A provision of the Violence Against Women Act of 1994 requires district courts to order persons guilty of possessing child pornography “to pay the victim . . . the full amount of the victim's losses as determined by the court.” 18 U.S.C. §2259. A five-Justice majority held that where the defendant was one of thousands of individuals who possessed and viewed the images, a federal district court “should order restitution in an amount that comports with the defendant’s relative role in the causal process that underlies the victim’s general losses.” Petitioner Doyle Paroline pleaded guilty to possessing between 150 and 300 images of child pornography, including two images that depicted the sexual exploitation of a young girl, now a young woman, referred to in this litigation by the pseudonym “Amy.” In addition to damages suffered at the hands of her abuser, Amy suffered medical, psychological and economic damages as an adult from her knowledge of the widespread distribution of images depicting her abuse. Amy sought restitution under §2259, asking for $3.4 million (nearly $3 million in lost income and about $500,000 in future treatment and counseling costs). The district court applied a “but-for” theory of proximate causation, found the government failed to meet its burden to establish losses proximately caused by Paroline and denied any restitution. In an en banc decision, the Fifth Circuit reversed, holding §2259 does not limit restitution to losses proximately caused by the defendant. Rather, each defendant who possesses the images is liable for the victim’s entire losses, even though other offenders have contributed to those losses by possessing the images. In an opinion by Justice Kennedy, the Court vacated and remanded.

The Court first addressed “whether §2259 limits restitution to those losses proximately caused by the defendant’s offense conduct.” The Court held that it does. Section 2259 enumerates six categories of covered losses and a catchall category for “any other losses suffered by the victim as a proximate result of the offense.” The Court concluded common sense and the rules of statutory construction dictate the proximate-cause requirement in the final phrase applies to the five previously enumerated categories of loss. The Court then turned to “the more difficult question” of how to apply the statute’s causation requirements to Paroline. “The difficulty is in determining the ‘full amount’ of [Amy’s] general losses . . . that are the proximate result of the offense conduct of a particular defendant who is one of thousands who have possessed and will in the future possess the victim’s images but who has no other connection to the victim.” In a case like this, ordinary “but-for causation cannot be” shown because “it cannot be shown that [Amy’s] trauma and attendant losses would have been any different but for Paroline’s offense.” The Court concluded, however, that “tort law teaches alternative and less demanding causal standards are necessary in certain circumstances to vindicate the law’s purposes. It would be anomalous to turn away a person harmed by the combined act of many wrongdoers simply because none of those wrongdoers alone caused the harm.”

On the other hand, the Court found “[t]hese alternative causal standards . . . can be taken too far,” by treating each possessor as if he had in fact caused all of Amy’s trauma and attendant losses. “Congress gave no indication that it intended its statute to be applied in the expansive manner the victim suggests,” under which someone whose contributions to the victim’s harms were “very minor” is deemed to have caused all the victim’s harms. Amy
suggested someone like Paroline can be required to pay the full amount and then seek contribution from other offenders. The Court observed, however, there is no “clear statutory basis for a right to contribution in these circumstances.” Further, requiring someone in Paroline’s position to pay the full amount “might raise questions under the Excessive Fines Clause of the Eighth Amendment.”

That still left the question of precisely how much Paroline must pay in restitution. The Court concluded that “[i]n this special context,” the district court “should order restitution in an amount that comports with the defendant’s relative role in the causal process that underlies the victim’s general losses. The amount would not be severe in a case like this,” but it “would not be a token or nominal amount.” The district court “must assess as best it can from available evidence the significance of the individual defendant’s conduct in light of the broader causal process that produced the victim’s losses.” Although there is no rigid formula for determining this amount, the Court set forth a number of “rough guideposts” for district courts, including the number of defendants found to have contributed to the victim’s general losses; predictions of the number of offenders likely to be convicted in the future for crimes contributing to the losses; an estimate of the broader number of offenders involved, “most of whom will, of course, never be caught or convicted”; whether images of the victim were distributed by the defendant; whether the defendant was involved in “the initial production of the images”; and the number of images of the victim the defendant possessed.

Chief Justice Roberts filed a dissenting opinion, which Justices Scalia and Thomas joined. Their dissent concluded the statute does not permit any restitution here because “it is not possible to do anything more than pick an arbitrary number” for the “amount of losses sustained by” Amy as a result of Paroline’s crime — “[a]nd arbitrary is not good enough for the criminal law.” Chief Justice Roberts agreed with the majority that “if Paroline actually caused those losses, he also proximately caused them.” But the statute specifies that the losses be sustained “as a result of the offense’ — that is, his offense.” “Determining what amount the statute does allow — the amount of Amy’s losses Paroline’s offense caused — is the real difficulty of this case.” Chief Justice Roberts concluded “Amy’s injury is indivisible, which means Paroline’s particular share of her losses is unknowable. And yet it is proof of Paroline’s particular share that the statute requires.” Congress therefore “effectively precluded restitution in most cases involving possession or distribution of child pornography.” Although Chief Justice Roberts agreed “awarding Amy no restitution would be contrary to Congress’s remedial and penological purposes,” he reluctantly found “[t]he statute as written allows no recovery; we ought to say so, and give Congress a chance to fix it.”

Justice Sotomayor separately dissented, stating the statute mandates restitution be awarded for (in the words of §2259) the “full amount of the victim’s losses.” Justice Sotomayor maintained that requiring mandatory restitution is inconsistent with a “but-for” causation requirement, and therefore Congress must have intended to incorporate aggregate causation into §2259. In her view, because §2259 (b)(1) requires restitution for the “full amount of the victim’s losses,” each defendant is liable for the full amount of the loss. She explained the potential for unfairness is addressed by the district court’s statutory authority to schedule an appropriate payment schedule.

For a full text of PAROLINE v. UNITED STATES (Docket No. 12-8561), please see the link below: http://www.supremecourt.gov/opinions/13pdf/12-8561_7758.pdf.
ATTORNEYS GENERAL FIGHTING CYBER CRIMES

ALABAMA
Attorney General Luther Strange joined Jefferson County Sheriff Mike Hale to announce a final decision in a case involving electronic bingo in which the court ordered the machines destroyed and the monies forfeited pursuant to state law. Law enforcement officers had seized more than 500 illegal slot machines and gambling devices, as well as $69,240, from the Anchor Club casino. The decision was the culmination of a joint law enforcement effort by the Sheriff’s Office and Attorney General Strange’s Office.

ARKANSAS
Attorney General Dustin McDaniel’s Cyber Crimes Unit agents executed a search warrant at Christopher Boyd’s residence, arresting Boyd on 30 counts of possession of child pornography, a Class C felony. Investigators seized four computers and other electronic evidence for analysis at the Unit’s Forensic Lab. Special Agent Chad Meli of Attorney General McDaniel’s Office began investigating Boyd after suspecting child pornography was being possessed at Boyd’s residence. The U.S. Marshals Service and the Little Rock Police Department assisted in the investigation and arrest, with the police department also arresting Boyd for failure to register as a sex offender.

DELAWARE
Attorney General Beau Biden announced the arrest of Stephen Parsons pursuant to an investigation by the Delaware Child Predator Task Force. The Task Force and the State Police executed a search warrant at a residence, with Parsons taken into custody on 25 counts of Dealing in Child Pornography. Multiple computers and other digital media were seized and taken to the State Police High Technology Crimes Unit for forensic analysis. A forensic preview revealed a seized computer contained multiple images of child pornography.

ILLINOIS
Attorney General Lisa Madigan announced the state Senate had passed Senate Bill 3405, legislation crafted by her office and sponsored by Senator Daniel Bliss, to crack down on patent trolls acquiring patents to profit from frivolous infringement claims. The bill would ban patent demand letters 1) containing false or deceptive information; 2) sent by individuals without the right to license or enforce a patent; 3) falsely threatening litigation if a fee if not paid; and failing to identify the individual asserting the patent and failing to identify the alleged infringement.

LOUISIANA
Attorney General Buddy Caldwell’s Cyber Crimes Unit investigators executed a search warrant at Giles Thibodeaux, Jr.’s residence, and Thibideaux was arrested and charged with the production of child pornography, computer-aided solicitation of a minor, indecent behavior with juveniles, oral sexual battery and simple rape. The arrest resulted from a joint investigation involving Attorney General Caldwell’s Cyber Crime and Fugitive Apprehension Units; the State Police; Homeland Security Investigations; the FBI; the St. Landry Parish, Ascension Parish, Lafayette Parish, Jefferson Parish and Livingston Parish Sheriff’s Offices; and the U.S. Secret Service.

MASSACHUSETTS
Attorney General Martha Coakley’s Office hosted the third annual Cybercrime Conference on April 28-30. The conference featured a separate track of instruction for prosecutors, investigators and digital forensic examiners. Each track had multiple breakout sessions led by cybercrime experts.
MISSISSIPPI

Attorney General Jim Hood launched an online safety awareness campaign targeting state students. Attorney General Hood had reached out to the state Department of Education and to all state colleges and universities seeking assistance in getting the word out directly to the students. The campaign begins with the dissemination of two posters created for the campaign by Attorney General Hood’s Office to participating schools. The posters can also be viewed, downloaded and printed from Attorney General Hood’s website, in addition to a PSA provided to campus television and radio stations. Attorney General Hood is also organizing a press conference specifically for student reporters.

MONTANA

Attorney General Tim Fox submitted written testimony at the U.S. House Judiciary Committee hearing on Internet sales taxes. His testimony opposes the Marketplace Fairness Act and similar legislation requiring state businesses to collect sales taxes from out-of-state purchasers.

NEW JERSEY

Acting Attorney General John Hoffman’s Division of Criminal Justice obtained a state grand jury indictment charging Jeanette Rodriguez, a former unemployment insurance clerk for the State Department of Labor and Workforce Development, with stealing $21,055 in unemployment benefits by using her access to the department’s computer system to redirect benefits from six different claims to her own bank account. Rodriguez is charged with official misconduct (2nd degree), computer theft (2nd degree) and theft by deception (3rd degree). The charges resulted from an investigation by the state Department of Labor-Office of Internal Audit and the Division’s Specialized Crimes Bureau. The second degree charges carry a sentence of five to 10 years in state prison, including five years of parole ineligibility, and a $150,000 fine. The third-degree charge carries a sentence of three to five years in state prison, including two years of parole ineligibility, and a $15,000 fine.

NEW YORK

Attorney General Eric Schneiderman’s Office entered an agreement with GrubHub Inc., an Internet food delivery service created from the merger of GrubHub Inc. and Seamless North America LLC, requiring GrubHub to take steps to ensure the tips it collects from customers who order from the company’s website will be distributed in full to the workers for whom the tips were intended. An investigation by Attorney General Schneiderman’s Labor Bureau found Seamless charged a fee to its restaurant partners based on a percentage of food and drink, taxes and tips and returned the remainder to the restaurants. State law prohibits an employer from retaining a portion of an employee’s tips. The agreement requires all future GrubHub contracts to use a fee calculation excluding tips, and GrubHub must make efforts to transition old contracts to this method. GrubHub must also notify partners of their labor law obligations, including a notice on invoices stating tips are the property of the delivery workers who earned them. The case was handled by Assistant Attorney General Haeya Yim, Section Chief Andrew Elmore and Bureau Chief Terri Gerstein, all of the Bureau.

PENNSYLVANIA

Attorney General Kathleen Kane’s Child Predator Section agents arrested Wilhelm Justiniano on accusations he posted an online advertisement for sex and then traveled to meet who he believed was a 14-year-old girl. According to the criminal complaint, Justiniano used craigslist to post a sexually graphic advertisement soliciting sex from “females of any age.” Undercover agents posing as a 14-year-old girl responded and arrested Justiniano when he arrived at a predetermined meeting location. He is charged with two counts of unlawful contact with a minor and
one count of criminal use of a communication facility. The Lower Paxton Police Department and the U.S. Postal Inspectors Service assisted in the investigation. The case will be prosecuted by Senior Deputy Attorney General Christopher Jones of the Section.

RHODE ISLAND
Attorney General Peter Kilmartin authored legislation requiring entities experiencing a data breach to provide one year of credit monitoring at no cost to state residents who are victims of the breach. The legislation also requires those entities to provide affected consumers with the toll-free numbers and addresses of consumer reporting agencies and the Federal Trade Commission, in addition to information about fraud alerts and security freezes. The legislation, H7519, has been introduced by Representative Brian Kennedy.

SOUTH CAROLINA
Attorney General Alan Wilson’s Office hosted a special town hall meeting for parents and children as part of their Internet Crimes Against Children (ICAC) “Stay Safe Online” Week. Attorney General Wilson gave opening remarks, followed by Joe Laramie, former commander of Missouri’s ICAC Task Force and an online safety expert. The meeting was emceed by WIS-TV anchor Meaghan Norman and concluded with a panel discussion.

VERMONT
Attorney General William Sorrell announced the State’s case against MPHJ Technologies has been remanded to state court. In the case Vermont alleges MPHJ, claiming to have patents on scanning documents and sending them by email, sent unfair and deceptive demand letters to small businesses and nonprofits in the State.

VIRGINIA
Attorney General Mark Herring announced the state General Assembly passed compromise legislation crafted by Attorney General Herring’s Office to protect state businesses from patent trolling. The bills, SB150 and HB375, establish criteria for determining a patent infringement claim is being made in bad faith, including issuing a letter claiming infringement and including false statements, failing to identify the patent holder, failing to specify the basis for the infringement, demanding an unreasonable license fee or reasserting infringement claims previously declared baseless by a court. The bill empowers the Attorney General to investigate cases of patent trolling and allows the Attorney General and Commonwealth’s Attorneys to bring actions to recover civil penalties.

WASHINGTON
Attorney General Bob Ferguson’s Office resolved allegations Colorado-based DISH network, which sells and distributes digital entertainment programming via satellite to subscribers, violated the Consumer Protection Act when it began charging state consumers an unlawful monthly surcharge, described as a “WA State Surcharge” ranging from $1.00 to $1.09. DISH has agreed to refund approximately $2 million to state consumers; provide additional benefits to consumers; and pay $569,000 to Attorney General Ferguson’s Office in attorney’s fees and costs.

WISCONSIN
Attorney General J.B. Van Hollen’s Division of Criminal Investigation Special Agents arrested and charged Aaron Bouzek with possession of child pornography. The agents, with assistance from the Lancaster Police Department, responded to a citizen tip, and their consent search transitioned into a search warrant. During the search, an on-scene analyst identified a child pornography image on Bouzek’s cellular phone.
CYBER NEWS BRIEFS

WIRELESS COS. TO PROVIDE FREE ANTI-THEFT TOOLS

CTIA-The Wireless Association announced a “Smartphone Anti-Theft Voluntary Commitment,” whereby the largest mobile device manufacturers and carriers have agreed to provide a free anti-theft preloaded or downloadable anti-theft tool on smartphones sold in the U.S. after July 2015. The companies agreeing to the commitment include Apple, Samsung Electronics, Verizon Wireless, AT&T, U.S. Cellular, Sprint Corp. and T-Mobile US Inc. Owners’ options will incorporate remotely removing a smartphone’s data and preventing reactivation if a phone is stolen or lost. According to the Federal Communications Commission, one in three robberies in the U.S. involves phone theft.

THREAT REPORT FINDS BLACK MARKET FOR HACKERS

The cyber attacks leading to the massive data breach at Target last year were fueled by a black market industry catering to hackers and identity thieves, according to a quarterly threat report issued by computer security company McAfee Labs. The report noted that industry enabled the thieves to buy custom malware as well as quickly sell the credit card numbers stolen in the breach. McAfee also identified the following rising threats: 1) mobile malware; 2) ransom-ware (malicious attacks against company systems demanding ransoms to stop the attacks); and 3) suspicious URLs. The report also questioned the method web service providers use to authenticate trusted third parties, noting they can no longer rely on certificates as a sign on security on third party links and software. The report can be accessed at http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2013.pdf.

DRAFT MOBILE DEVICE SECURITY GUIDE PUBLISHED

The National Cybersecurity Center of Excellence, part of the National Institute of Standards and Technology, published a draft outlining how businesses and other organizations can secure mobile devices used for work. The draft proposes a mobile device management system, including the ability to remotely wipe sensitive data, verify the identity of the device’s user, update software and monitor unusual activity. The device security capabilities should include full disk encryption, and the app security features should include authentication for individual apps. The draft may be accessed at http://csrc.nist.gov/nccoe/Building-Blocks/NCCoE_Mobile_Device_Security_Building_Block_Draft_20140221.pdf.

SURVEY: FINANCIAL SERVICES HARDEST HIT BY CYBERCRIME

Thirty-nine percent of financial services companies suffering from economic crime in 2013 were victims of cybercrime, compared to 17 percent in other industries, according to the Global Economic Crime 2014 Survey by PricewaterhouseCoopers. The survey, based on responses from 1,330 companies in 79 countries, showed cybercrime was the second most common type of fraud reported by financial firms, with theft being the most common. The survey further found external fraudsters to be responsible for most of the economic crime. The survey can be accessed at http://pwc.com/gx/en/economic-crime-survey/

And see...

The Federal Financial Institutions Examination Council, an interagency group including the Federal Reserve and the Federal Deposit Insurance Corporation, advised banks to upgrade their systems as
soon as possible if they are vulnerable to the recently uncovered “Heartbleed” bug. The group further advised banks to set up temporary patches for any systems using the web encryption program known as OpenSSL. Group researchers revealed they found evidence of hackers scanning the Internet in search of web servers running OpenSSL. The group noted banks should ask customers and administrators to change their passwords after patching their systems.

DHS TO PROVIDE FREE SECURITY SERVICES TO STATES

The U.S. Department of Homeland Security (DHS) began work on a cooperative effort with the Center for Internet Security Multi-State Information Sharing and Analysis Center (MS-ISAC) to furnish managed security services to states and territories in conjunction with their adoption of the National Institute for Science and Technology Cybersecurity Framework. As part of this effort, MS-ISAC will provide Managed Security Services, including intrusion detection, intrusion prevention, netflow analysis and firewall monitoring, to states and territories free of charge. DHS and MS-ISAC will seek feedback and requirements from the states and territories and tailor technical assistance and best practice documents to meet their needs.

U.S. ISSUES ONLINE EDUCATION SERVICES GUIDANCE

The U.S. Department of Education issued guidance on the requirements and recommended practices for school management of online educational services directly involving students or their parents. The guidelines provide specific examples of federal protections for personal details, such as contact information, contained in a student’s record. Under the school outsourcing exception, online educational services cannot use protected student information they obtain for any other purpose other than that which was disclosed. In the new guidance, the Department recommends school districts establish direct control over the collection and use of students’ personal details through contracts with service providers. It also recommends districts avoid signing agreements allowing online education programs to alter their terms of service unilaterally. The guidelines can be accessed at http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services.

FREE IPAD CASE BRIEF APP AVAILABLE

An iPad app automating the creation of case briefs has been created by a third-year law student at the University of Michigan Law School and is available for free. The app allows a user to annotate PDFs of court decisions using nine customizable highlight colors, one for each facet of a case. The colors can also be edited and given user-designated labels. When the annotation is finished, tapping the “Brief” button will create a case brief, with highlights organized in bullet points under the labels for each color. There are no iPhone or Android versions, and additional features require a yearly subscription. The app can be downloaded at http://thebriefcaseapp.com/.

And see...

NASA has to date released 1,000 apps to the public in an effort to make more widespread use of its software and aggregate it into one catalogue. Although some apps in the catalogue are restricted by their intellectual property rights, many others are available to the general public. The apps cover a variety of applications, including structural analysis, aeronautics, image processing and project management. The apps are available at http://technology.nasa.gov.
REPORT: FEDERAL COURTS STREAMLINING ELECTRONIC SYSTEMS

The transition to the next generation of the federal courts’ case management/electronic case files system is underway, according to a report from the director of the Administrative Offices of the U.S. Courts. The report noted 33 bankruptcy courts have adopted the Judiciary Financial System to maintain case financial details, and 30 of the courts have converted to the Court Registry Investment System for court registry funds. The report may be accessed at http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/AdministrativeOffice/DirectorAnnualReport/annual-report-2013.aspx.

IRS: VIRTUAL CURRENCIES ARE PROPERTY

The Internal Revenue Service (IRS) released Notice 2014-21, guidance advising virtual currencies, such as bitcoin, are property and not currency for tax purposes. However, the notice stipulates wages paid to employees with bitcoin and other forms of virtual currency are taxable and subject to withholding and payroll taxes, as are payments to independent contractors and other service providers. With respect to virtual currency as property, the IRS emphasizes the character of the gain or loss from the sale or exchange of the currency determines whether it is a capital asset for the taxpayer, and a payment made using virtual currency is subject to information reporting to the same extent as any other payment made in property. Notice 2014-21 can be accessed at http://www.irs.gov/pub/irs-drop/n-14-21.pdf.

FCC RELEASES MORE AIRWAVES FOR WI-FI, BROADBAND

The Federal Communications Commission (FCC) released additional airwaves for Wi-Fi and wireless broadband, also allowing a broad range of airwaves to be used for outdoor unlicensed broadband. Unlike airwaves used for mobile phone traffic and are licensed to a specific company, unlicensed spectrum can be used by anyone and have led to innovations such as garage door openers, baby monitors and wireless microphones. The FCC also approved rules allowing it to sell 65 megahertz of airwaves known as Advanced Wireless Services bands at auction this year under new technical rules to make the segments more compatible. In another action, the FCC approved new rules prohibiting the top four broadcast stations in a single market from acting together to negotiate fees with cable networks and could result in higher prices. Cable networks generally pay local affiliates of the major broadcast networks for the right to distribute the broadcast signals in their cable service area. Additionally, the FCC voted to close a loophole in television station ownership rules by stopping a practice.

Yahoo experienced a significant drop in the number of government requests for data about its users in the second half of 2013, compared with the first half, according to its semiannual transparency report. The company reported 21,425 requests from 17 countries for information on 32,493 accounts, with the U.S. accounting for one-third of the requests. The figures excluded requests made by the U.S. under national security laws and the Foreign Intelligence Surveillance Act, allowed to be reported only in broad ranges and with a six-month delay. Yahoo also noted its new policy, made effective in July 2013, informing users about government data requests before fulfilling them. The report may be accessed at https://transparency.yahoo.com/index.htm.

YAHOO REPORT: DROP IN GOVERNMENT REQUESTS FOR DATA
known as joint sales agreements, allowing one station to sell advertising time on another station in the same market, even though the two stations have different owners. The stations use the agreements to cut operating expenses, but the FCC found it appeared the companies were instead circumventing rules limiting the number of stations a single owner can control in a given market. Further details of these FCC actions may be accessed at http://www.fcc.gov/events/open-commission-meeting-march-2014.

UN AGENCY TO MEASURE INTERNATIONAL CYBERSECURITY

The United Nations International Telecommunications Union (ITU) launched the Global Cybersecurity Index, an initiative to measure the levels of cybersecurity in member countries. The initiative will provide a comparison of different national cybersecurity strategies and best practices. Its goal is to help foster a global culture of cybersecurity and its integration at the core of information and communication technologies. Based on questionnaire responses received from ITU member countries, a first analysis of cybersecurity development in the Arab region has been compiled and another for the Africa region is in progress, with a goal of releasing a global status this year.

OPENING OF SILICON VALLEY PTO DELAYED

The opening of the Silicon Valley office of the U.S. Patent and Trademark Office (PTO) has been delayed several months, with a new opening date expected in spring 2015. The PTO announced additional time is needed to renovate the space at San Jose City Hall to meet the agency’s needs. In addition, current city employees will have to be relocated to make space available. PTO has been operating a smaller, more limited office in Silicon Valley in a temporary location, but staffing is minimal. It expects to staff the permanent office with 20 Patent Trial and Appeal Board judges and 60 patent examiners. PTO satellite offices were mandated in the 2011 America Invents Act, with other satellite offices located in Dallas, Denver and Detroit.

ABA APPROVES HYBRID JD PROGRAM

The American Bar Association approved a variance in its accreditation rules allowing the William Mitchell College of Law, located in St. Paul, Minnesota, to offer a four-year hybrid HD program allowing students to complete coursework both on-campus and online. The program will launch in January 2015, with enrollment closing on December 1, 2014. Students will take self-scheduled online courses for 11 or 12 weeks and attend a week-long on-campus seminar. They are also expected to participate in internships with local attorneys. The program will also include an option to focus on Indian law or law and business tracks.

SEC ISSUES PLAN TO ENSURE CYBERSECURITY ON WALL STREET

On April 15, the U.S. Security and Exchange Commission (SEC) posted a document containing examples of questions SEC commissioners might ask brokerages and asset managers during inspections to ensure they are prepared to detect and prevent cyberattacks. The document alerts these firms to be prepared to provide a comprehensive list of when they detected malware, suffered a denial of service attack or discovered a network breach since 2013. The SEC also plans examinations of more than 50 firms focusing on cybersecurity issues. The document also indicates the possibility of examiners gathering information about how firms protect customer information, including checking on how customers are authenticated to access online accounts and the security measures protecting PIN numbers.
VERIZON ISSUES ANNUAL DATA BREACH REPORT

Verizon released its 2013 Data Breach Investigations Report, relating there were almost 200 hacks in 2013 of the payment systems used by retailers, hotels and restaurants. The report also notes hackers successfully stole data from Point of Sales (POS) systems 198 times last year – down from previous years. In total, Verizon tabulated 1,367 data breaches in 2013 based on statistics from the U.S. government, cybersecurity companies and foreign law enforcement. This year’s report also features common incident patterns, including insights from 50 global organizations and more than 63,000 confirmed security incidents. The report can be accessed at http://www.verizonenterprise.com/DBIR/2013/.

WHITE HOUSE UPDATES PRIVACY POLICY

The Obama administration released an updated privacy policy, explaining how the government will gather the user data of online visitors to WhiteHouse.gov, mobile apps and social media sites. The policy also clarifies the status of online comments, both tirades and tributes, as being in the open domain. The policy promises the data of online visitors will not be sold, but states it cannot make the same assurances for users of third-party White House sites on Facebook, Twitter or Google. While there are not significant changes to actual practices under the new policy, legal jargon and bureaucratic language have been removed, making it easier for readers to understand. The policy may be accessed at http://whitehouse.gov/privacy.

FCC TO OK “FAST LANES” FOR PROVIDERS

The Federal Communications Commission (FCC) announced it would propose new rules to allow companies to pay Internet service providers for special, faster lanes to transmit video and other content to their customers. The proposal puts a big dent in net neutrality – the concept of no discrimination in the provision of legal Internet content by provider and equal access by users. Under the proposal, broadband providers would have to disclose how they treat all Internet traffic and on what terms they offer more rapid lanes. They would also be required to act in a “commercially reasonable manner.” The proposed rules would also require Internet service providers to disclose whether in assigning faster lanes they have favored their affiliated companies. The proposed rules will be released for public comment on May 15, 2014, and the FCC is likely to vote on them by year end.

IN THE COURTS

EXPECTATION OF PRIVACY: INVENTORIED CELL PHONE

State v. Granville, 2014 Tex. Crim. App. LEXIS 237 (February 26, 2014). The Texas Court of Criminal Appeals ruled a search warrant was required to search the contents of an inventoried cell phone. Anthony Granville was arrested for causing a disturbance on the school bus, a Class C offense, and his cell phone was taken during booking and put in the jail property room. Later that day, another officer learned Granville had taken an indecent photograph on his cell phone and took Granville’s cell phone from the jail property room and examined its contents without a warrant. The officer turned on the phone, found the photograph and printed a copy
of it, keeping the phone as evidence. Granville was charged with Improper Photography, a felony, and filed a motion to suppress, arguing the officer could not search his cell phone without a warrant. The officer contended he could search anything in the jail property room if he had probable cause. The trial court granted the motion to suppress, concluding Granville had a reasonable expectation of privacy in his cell phone, even when the cell phone was in the jail inventory. The State appealed, and the appeals court affirmed, finding Granville did not lose his reasonable expectation of privacy in the contents of the cell phone when it was stored in the jail property room. The court determined the officer could have seized the phone and held it while he obtained a search warrant, but even with probable cause, he could not activate and search the contents of the inventoried phone without one.

FOURTH AMENDMENT: WARRANTLESS SEARCH OF TEXT MESSAGES

State v. Hinton, 2014 Wash. LEXIS 159 (February 27, 2014). The Supreme Court of Washington ruled police improperly obtained the text messages without a warrant. Police arrested Daniel Lee for possession of heroin and seized his iPhone, which was handed over to a detective at the police station. The detective looked through the iPhone for about 5-10 minutes and saw a text message from “Z-Jon” containing drug terminology. The detective, responding as Lee, exchanged messages with Z-Jon and arranged a meeting to sell him heroin. When Jonathan Roden arrived for the transaction, he was arrested. Then the detective received a message from “Z-Shawn,” and again posing as Lee, responded to the message, arranged another drug transaction and arrested Shawn Hinton when he arrived for the meeting. Hinton was charged with attempted possession of heroin, and he moved to suppress the evidence obtained from the iPhone, arguing the detective violated his Fourth Amendment rights and the state constitution and privacy act. The trial court denied the motion and found Hinton guilty. He appealed on the constitutional issues and the Court of Appeals affirmed. The state Supreme Court granted Hinton’s petition for review to decide whether the detective’s conduct was unconstitutional. That court held the text messages were improperly obtained by the police without a warrant because Hinton’s text message conversations were private affairs protected by the state constitution from warrantless intrusion. The decision was reversed and the conviction vacated without prejudice.

Ed. Note: Jonathan Roden also sought review, and his decision was reversed and his conviction vacated without prejudice on the same grounds.

PUBLIC RECORDS REQUEST: RECORDED INTERVIEWS

Ingram v. State, 2014 Fla. App. LEXIS 2369 (February 21, 2014). The Florida Court of Appeal, Fifth District, found the trial court erred by failing to hold a hearing on the public records request. Lawrence Ingram, serving a life sentence for the sexual battery of a child, made a written public records request to the State Attorney’s Office requesting 1) the mirror images made of his hard drive in the form of DVDs or CDs and the analyses and reports from the forensic examination of his home computer, and 2) the recorded interviews of the victim and her mother. As to the recorded interviews, the State responded it was required by an exemption to the Public Records Act to first redact any information identifying the child victim, and it lacked the ability to do so. The State told Ingram he was required to obtain someone with that capability. Ingram again wrote the State, and the State reiterated its position. Ingram filed a motion to compel production of documents and requested a telephonic hearing on the motion, but the trial court dismissed the motion without a hearing. Ingram sought certiorari review of the order denying the motion, arguing the trial court failed to treat his motion as a petition for writ
of mandamus and failed to have a required hearing on his motion. The appeals court agreed with both arguments and quashed the order. Further, to give guidance to the trial court, the court determined if there was a videotaped interview of the minor child, an unredacted copy had to be provided to Ingram, as this information was not exempt from disclosure, and all other records requested had to be redacted in accordance with the statute.

Ed. Note: Kellie Nielan, Assistant Attorney General in the Florida Attorney General’s Office, represented the State.

SUBPOENA ENFORCEMENT: ANONYMOUS INTERNET REVIEWS

Yelp, Inc. v. Hadeed Carpet Cleaning, Inc., 2014 Va. App. LEXIS 1 (January 7, 2014). The Virginia Court of Appeals held the trial court properly enforced a subpoena seeking the identities of the anonymous Internet posters. Yelp, a Delaware corporation with its principal place of business in California, is a social networking site allowing its users to post reviews. In order to do so, the user must register with a valid email address, agree to Yelp’s Terms of Service and be a customer of the business on which they base their reviews. In October 2012, there were 75 reviews of Hadeed Carpet Cleaning in Virginia posted, and several were critical of Hadeed. Hadeed filed suit against the authors of seven critical reviews, alleging it was unable to match the reviewers with its customer database and could find no record the reviewers were Hadeed customers. Hadeed further alleged they had falsely represented themselves as customers, and the reviewers’ comments were defamatory because they falsely stated Hadeed had provided bad service. Hadeed served a subpoena duces tecum on Yelp’s registered agent in Virginia, seeking information about the authors of the reviews. Yelp filed written objections to the subpoena, and Hadeed moved to override the objections and enforce the subpoena. The trial court issued an order enforcing the subpoena, finding it had jurisdiction and the subpoena complied with both the First Amendment and Virginia code. Yelp refused to comply in order to protect its users’ rights, and Hadeed moved to have Yelp held in contempt. The trial court did so, imposing a monetary sanction and awarding Hadeed attorney’s fees, and Yelp appealed, arguing 1) the First Amendment requires a showing of merit on the law and on facts before a subpoena to identify an anonymous speaker is enforced; and 2) the trial court lacked jurisdiction. The appeals court found the First Amendment right to anonymity is subject to a substantial government interest in disclosure, as in the instant case. The court held the trial court properly asserted subpoena jurisdiction over the foreign Internet website company because its registered agent was served with the subpoena, constituting service of process under Virginia law and providing jurisdiction to the court. The order was affirmed.

STATUTE INTERPRETATION: “UPSKIRTING”

Commonwealth v. Robertson, 2014 Mass. LEXIS 115 (March 5, 2014). The Massachusetts Supreme Court held a female transit passenger wearing clothing on the private parts of her body is not “partially nude” and not covered by Mass. Gen. Laws ch. 272, § 105(b). Michael Robertson allegedly took a photo of the upper leg of a woman wearing a skirt while on the trolley and was seen by another passenger, who reported the incident to transit police. Later that day, another passenger reported she saw Robertson trying to photograph a woman’s crotch area, and she captured images of him doing so and sent them to transit police. Transit police set up a decoy operation on the trolley with a female officer wearing a dress, and Robertson was observed videotaping her crotch area. Officers arrested Robertson and secured his cell phone, noting it had been recording. Robertson was charged with two criminal complaints of attempting to commit the offense of photographing, videotaping or electronically surveilling a nude or partially nude person in viola-
tion of the previously cited statute. Robertson moved to dismiss, which was denied, and he sought interlocutory review. The state Supreme Court agreed with Robertson in interpreting “a person who is partially nude” to mean a person who is partially clothed but who has one or more private parts of the body exposed at the time the defendant secretly photographs her. The court held a female passenger on a trolley wearing a skirt, dress or the like covering those parts of her body is not a person who is “partially nude,” whether or not she is wearing clothing underneath the clothing. The court found the statute, as written, is only concerned with proscribing peeping Tom voyeurism of people who are completely or partially undressed, especially that voyeurism enhanced by electronic devices. The order denying the motion to dismiss was reversed.

Ed. Note: On March 7, 2014, two days after this decision, Massachusetts Governor Deval Patrick signed into law a bill banning “upskirting” by making it illegal to photograph or videotape the “sexual or other intimate parts” of women and children in public.

**CYBER STALKING: AUTHENTICATION OF TEXT MESSAGES**

*McGee v. State*, 2014 Tex. App. LEXIS 825 (January 25, 2014). The Texas Court of Appeal, Fifth District, ruled the State satisfied its burden to authenticate the text messages. David McGee called and sent excessive text messages to his ex-girlfriend who was trying to end their relationship. He then pushed her, damaged her car and garage door and tried to damage her cell phone when she called 9-1-1. McGee was arrested for assault and interfering with a 9-1-1 call. Upon release, McGee continued his excessive calls and sent humiliating and threatening texts to her work, home and cell phone. Police were called to the ex-girlfriend’s home numerous times on complaints of criminal mischief, but police had no proof it was McGee. The ex-girlfriend began recording his calls and saving his text messages and got a protective order against him, but the calls and text messages continued. McGee came to the ex-girlfriend’s workplace, and was arrested for stalking and violation of a protective order. McGee was convicted by a jury of stalking and appealed, arguing there was insufficient evidence he originated the calls and text messages and the trial court erred in admitting 72 text messages sent to the ex-girlfriend because the State did not authenticate them. The appeals court disagreed, finding sufficient evidence to support McGee’s conviction because 1) the ex-girlfriend testified the calls and text messages were from McGee; 2) the ex-girlfriend’s telephone records were in evidence; and 3) the ex-girlfriend testified some of the communications were threatening. The court further found the State satisfied its burden to authenticate the text messages because the ex-girlfriend testified it was the same number McGee used to contact her. The conviction was affirmed.

**STATE WIRETAP ACT: POINT OF INTERCEPTION**

*State v. Ates*, 2014 N.J. LEXIS 238 (March 18, 2014). The New Jersey Supreme Court upheld the constitutionality of the state Wiretap Act. Edward Ates was charged with first-degree murder of his son-in-law, among other charges. During the investigation of the crime, law enforcement officers had obtained court orders to intercept phone conversations, including conversations between persons located outside of New Jersey – namely, in Florida and Louisiana. Prior to trial, Ates moved to suppress the conversations with out-of-state persons, arguing law enforcement officers failed to ask the proper authorities in Florida and Louisiana to consent to the wiretaps and asserting the state Wiretap Act was unconstitutional because it permitted state authorities to act outside of their jurisdiction and wiretap individuals with no connections to the State. The motion was denied, and a jury found
Ates guilty on all counts. The trial court sentenced him to life imprisonment subject to 63.75 years of parole ineligibility. Ates appealed, renewing his constitutionality argument, and the Appellate Division affirmed his conviction. The state Supreme Court granted his petition for certification, and also granted leave for the state Attorney General to appear as amicus curiae. The state high court noted the language in the statute (N.J.S.A. 2A:156A-12h) providing a wiretap order “may be executed at any point of interception (defined as the site where the ‘officer is located at the time the interception is made’) within the jurisdiction of an investigative or law enforcement officer executing the order.” Thus, the court found a wiretap order signed by a New Jersey judge can empower investigators located in New Jersey to monitor intercepted conversations in the State, even if both parties to the call are outside the State. The court further noted federal circuit courts and state courts have consistently upheld wiretaps based on the location of the listening post. The court concluded the state Wiretap Act is constitutional under both the federal and state constitutions and affirmed the judgment.

Ed. Note: Deputy Attorney General Daniel Boorstein argued the case for the Office of the New Jersey Attorney General.

FIRST AMENDMENT: EAVESDROPPING STATUTE

People v. Melongo, 2014 IL 114852 (March 20, 2014). The Illinois Supreme Court found 720 ILCS 5/14-2 (2008), defining eavesdropping, was facially unconstitutional. Annabel Melongo was charged with computer tampering in an unrelated case; she failed to show at the arraignment but obtained an official court transcript stating she was present and arraigned. She tried to no avail to have the court reporter change the transcript and was referred to the supervisor, who told her disputes over transcript accuracy should be presented to the judge. Melongo surreptitiously recorded three subsequent telephone conversations with the supervisor and posted the recordings and transcripts of the conversations on her website. She was charged with three counts each of eavesdropping and of using or divulging information obtained through the use of an eavesdropping device.

Melongo moved to dismiss, arguing an exception to the statute allowed her to record a conversation under reasonable suspicion the other party is about to or has committed a criminal offense, and there is reason to believe the evidence of the offense may be obtained by the recording. The State argued the exception did not apply because the court reporter accused by Melongo was not a party to the recorded conversations, and the trial court granted the State’s motion in limine precluding Melongo from raising the defense at trial. Melongo’s ensuing motion to reconsider and her motion to dismiss on the basis the statute was unconstitutional under the due process clause were also denied. The trial resulted in a hung jury and mistrial and was reassigned. Melongo filed a motion to declare the statute unconstitutional, raising both First Amendment and due process claims. The court found the statute to be unconstitutional, finding it vague and a violation of due process. The State appealed, and the Illinois Supreme Court held the recording provision of the statute to be facially unconstitutional because it burdened more speech than was necessary to protect conversational privacy. The court also found the provision of the statute criminalizing the publication of the recording to be overbroad and therefore unconstitutional as well. The judgment of the trial court was affirmed.

KNOWING POSSESSION: SHADOW IMAGES

New v. State, 2014 Ga. App. LEXIS 253 (March 27, 2014). The Georgia Court of Appeals found sufficient evidence to support defendant’s
conviction. Matthew New, a former police officer, had encouraged his 14-year-old son and the son’s 13-year-old girlfriend to engage in strip wrestling and photographed the event. The son reported the incident to law enforcement, and officers went to the home to speak to New, seizing a computer from the residence. A forensic analysis of the computer revealed images of the strip wrestling as well as numerous images of child pornography. New was charged with and convicted by jury on 35 counts of sexual exploitation of children, two counts of child molestation and one count of enticing a child for immoral purposes. He appealed the exploitation charges, arguing the State failed to prove he knowingly possessed images of child pornography based on the location of the recovered images on his hard drive. The court noted a computer forensics expert had testified at trial the images were found as “shadow copies” in the system volume file created in the daily backups. The expert had also testified only one user account named “Matt” had been consistently utilized on the hard drive, and the guest account profile had never been used. Further, the expert testified LimeWire, a peer-to-peer file sharing program, had been installed on the computer, but it could not be determined if the shadow images of child pornography had only been viewed on a web page or whether it had been downloaded to the computer.

The appeals court found sufficient evidence existed to support the conviction based on the State’s presentation of circumstantial evidence of the shadow copies on New’s computer, evidencing prior possession of the images. Further, the court found that State presented expert testimony indicating searches for and downloads of child pornography and the number of child pornography images discovered. The court affirmed the conviction, but remanded for resentencing, finding the trial court had not imposed a split sentence on each count.

And see...

The People v. Petrovic, 2014 Cal. App. LEXIS 281 (March 26, 2014). The California Court of Appeals, Second Appellate District, found the evidence supported an inference defendant intentionally used his computer to peruse child pornography. Zoran Petrovic was arrested for a parole violation, and a subsequent forensic review of his computer by his parole agent revealed he had viewed child pornography. Petrovic was convicted of possession of child pornography with a prior conviction for child molestation. He appealed, contending there was no evidence he knowingly possessed child pornography because the evidence only showed he used his computer to visit child pornography sites, and he did not know his computer could automatically save images in a temporary file. The appeals court held the evidence was sufficient to support an inference Petrovic intentionally used his computer to view child pornography and display images on the screen. The court noted a computer expert’s report showed Petrovic repeatedly visited child pornography web sites, prohibited by his parole, and his false statement to the parole agent about his lack of access to the Internet indicated consciousness of guilt. Further, the court observed Petrovic made no showing of the inadvertent or unintentional acquisition of the pornographic material, and the expert’s testimony stating Petrovic had transferred the images from temporary Internet files to another location supported a finding he had knowledge of and access to the files. The judgment was affirmed.

Ed. Note: Lance Winters, Assistant Attorney General, and Linda Johnson and Gary Lieberman, Deputy Attorneys General, of the California Attorney General’s Office, represented the People.

ONLINE SOLICITATION: NO DIRECT CONTACT WITH MINOR

U.S. v. McMillan, 2014 U.S. App. LEXIS 4832 (7th Cir. March 12, 2014). The Seventh Circuit Court of Appeals found the evidence sufficient to
prove defendant intended to persuade a minor to engage in sexual activity. Harry McMillan, a law student at Southern Illinois University School of Law, posted an ad on craigslist soliciting sexual acts for pay and entitled “sell me your teenage daughter.” Undercover police investigator Mike Andrews saw the ad and arrested McMillan, charging him with one count of violating 18 U.S.C. § 2422(b) prohibiting the knowing persuasion or enticement of a person under the age of 18 to engage in criminal sexual activity. McMillan was convicted in the U.S. District Court for the Southern District of Illinois and sentenced to 132 months’ imprisonment, five years’ supervised release and a $500 fine. He appealed, arguing 1) the statute prohibits contact between a defendant and an underage person, but he only had contact with the father of a teenage girl; and 2) the prosecution failed to show he intended to persuade or entice the minor into the prohibited acts. As to McMillan’s first argument, the appeals court found the essence of the statute is the defendant’s effect or attempted effect on the child’s mind, and the statute does not require the minor to be the direct recipient of the defendant’s message. As to the second argument, the court found the online ad and the email exchange between McMillan and the undercover detective was sufficient to prove McMillan intended to persuade or entice the minor into the prohibited acts. The conviction was affirmed.

CONSENT TO SEARCH: CELL PHONE EVIDENCE

U.S. v. Rounds, 2014 U.S. App. LEXIS 6545 (5th Cir. April 9, 2014). The Fifth Circuit Court of Appeals found defendant’s motion to suppress was properly denied as he consented to the search. Trevin Rounds contacted a 14-year-old girl on the social networking site Tagged.com and began texting with her. The girl subsequently ran away from home and spent several nights with Rounds in a hotel.

While the two were driving, Rounds’ car was stopped for a traffic violation, and the officers obtained consent to search the car and Rounds’ iPhone found in the car. The officers took Rounds and the girl to the police station, where the officers again looked through the iPhone and uncovered a video of Rounds having sexual relations with the girl. Rounds was arrested and later found guilty by a jury in the U.S. District Court for the Western District of Texas of possession of child pornography and using a facility of interstate commerce to entice or coerce a juvenile to engage in sexual activity. Rounds appealed, questioning the sufficiency of the evidence and arguing the district court erred in denying his motion to suppress the photo and video evidence from his iPhone. The appeals court found the evidence was sufficient to convict Rounds as his sexually explicit text messages allowed a jury to find he intended to coerce the minor to have a sexual relationship with him. Further, the court found Rounds’ motion to suppress photo and video evidence found on his phone was properly denied because the district court determined Rounds had voluntarily consented to the search, and the officers had told him they wanted to examine the phone for evidence of sexual exploitation of the minor. The judgment was affirmed.

RECORDING OF CONVERSATION: ONE-PARTY CONSENT

Commonwealth v. Hearns, 2014 Mass. LEXIS 206 (April 8, 2014). The Massachusetts Supreme Court found the recording of a conversation between two gang members was proper under the one-party consent exception in Mass. Gen. Laws ch. 272, § 99©(1). Timothy Hearns, a known member of the H-Block gang, was indicted for the murder of a Heath Street gang member and the wounding of another member. The Commonwealth, believing the gangs were involved in the supply and sale of illegal goods, obtained a warrant and recorded a conversation between Hearns and other gang members in which he admitted to the murder. Hearns filed a motion to suppress the recorded conversation, arguing the evi-
idence was insufficient to establish the shooting was a “designated offense” occurring in “connection with organized crime,” and therefore the one-party consent exception to the recording of oral communications without the consent of all parties was inapplicable. The motion judge denied the motion to suppress, and Hearns sought leave to file an interlocutory appeal, making the same arguments, and leave was granted. The state high court found the recorded conversation was proper under the one-party exception as the police officer’s affidavit provided adequate information to conclude Hearns’ gang was an organized criminal group and contained information provided to the officer about Hearns being sent on a mission by senior members of the gang as part of an ongoing feud between turf-conscious criminal organizations involved in the sale of illegal goods. The court affirmed the denial of the motion to suppress, but reversed the motion to suppress with respect to statements Hearns made following his invocation of the right to remain silent.

FOURTH AMENDMENT: BROADNESS OF WARRANT

U.S. v. Gumbs, 2014 U.S. App. LEXIS 5740 (3rd Cir. March 28, 2014). The Third Circuit Court of Appeal ruled the search warrant was not an impermissible general warrant. Akeem Gumbs was indicted on 31 counts of production and possession of child pornography and aggravated rape. At trial, he challenged the propriety of the search warrant, seeking to exclude the laptop, camera and other electronic evidence seized during the search, but his motion was denied. Gumbs was found guilty on all counts in the U.S. District Court for the District of the Virgin Islands and was sentenced to 300 months’ imprisonment and a lifetime of supervised release. He appealed, renewing his impermissible search warrant argument. The appeals court noted the warrant directed officers to seize “images of child pornography and files containing images of child pornography in any form, wherever it may be stored or found,” and then set forth a list of computer-related devices as possible storage sites for such images or files. The court found Gumbs’ suppression motion was properly denied, as the search warrant, although broad, was not an impermissible general warrant. The judgment was affirmed.

LEGISLATIVE UPDATE

PUBLIC SAFETY COMMUNICATIONS

ALABAMA. On March 19, 2014, Governor Robert Bentley signed HB 54 into law, a bill making interference with official communications between law enforcement agencies, fire service4s and 911 communications a class C felony, punishable by up to 10 years in prison. The bill, codified as Act 2014-39, includes radio broadcasts, telephone communication and electronic channels allocated by the FCC. It becomes effective on June 1, 2014.

SOCIAL MEDIA PRIVACY

WISCONSIN. On April 8, 2014, Governor Scott Walker signed S.B. 223 into law, a bill prohibiting employers, educational institutions and landlords from requesting or requiring the passwords or other protected access to personal Internet accounts of students, employees and tenants. Viewing, accessing and using information from Internet accounts in the public domain, including social media, is allowed. Any person violating the law is subject to a fine of up to $1,000. The bill is codified as Act 208.

DISSEMINATION OF DIGITAL IMAGES

WISCONSIN. On April 9, 2014, Governor Scott Walker signed S.B. 367 into law, a bill prohibiting the posting or publishing of a sexually explicit image without consent. A person violating the statute will
be guilty of a Class A misdemeanor. The legislation has been codified as Act 243.

PATENT TROLLING

IDAHO. On March 26, 2014, Governor Butch Otter signed S.B. 1354 into law, a bill making bad faith assertions about patent infringement unlawful. Bad faith threats are defined as: 1) lacking the patent number or name and address of the alleged owner(s); 2) containing a demand for payment of a license fee or a response within an unreasonably short time; and 3) containing an offer to license the patent for an unreasonable amount. The bill grants the Attorney General enforcement authority and also provides for a private cause of action. The bill has been codified as Chapter 277.

ILLINOIS. On April 9, the Senate passed S.B. 3405, a bill to amend the state Consumer Fraud and Deceptive Business Practices Act making unfair or deceptive patent infringement demand letters unlawful. The bill would be effective January 1, 2015. It has been forwarded to the House.

ELECTRONIC COMMUNICATIONS

MARYLAND. On April 3, 2014, the Senate passed SB 924, a bill amending the state Electronic Communications Privacy Act (ECPA). The current ECPA requires a warrant for all content held by an Electronic Communications Service (ECS) for 180 days or fewer, and SB 924 would eliminate the under 180 days clause. SB 924 also eliminates the current ECPA provision allowing for the use of a subpoena with notice, a D order with notice or a warrant for older ECS or Remote Communications Service (RCS) content. The bill has been forwarded to the House. The effective date would be October 1, 2014.

MOBILE PHONE THEFT

CALIFORNIA. On April 1, 2014, the Senate Energy, Utilities and Communications Committee passed S.B. 962, a bill requiring any advanced mobile communications device sold in the State after January 1, 2015 to include a technological solution rendering its essential features inoperable when not in the possession of its rightful owner.

ONLINE SOLICITATION OF A CHILD

DELAWARE. On April 10, 2014, the House passed H.B. 256, a bill making current Code on the online sexual solicitation of a child more specific and elevating the offense from a Class C felony to a Class B felony when the solicitor or promoter meets in person, or attempts to meet in person, with a child. The bill would be effective immediately upon passage. It has been forwarded to the Senate.

DATA BREACH NOTIFICATION

FLORIDA. On April 23, the Senate passed S.B. 1524, a bill requiring notification of a breach to each affected state resident whose personal information was believed to be accessed not later than 30 days after determination the breach had occurred. The bill also delineates the method and contents of notification. If the breach affects more than 1,000 individuals, all credit reporting agencies must be notified as well. A violation of the legislation will be treated as an unfair or deceptive trade practice in any action, in addition to liability for a civil penalty of up to $500,000. The bill does not provide for a private cause of action. The effective date of the legislation is July 1, 2014.

ONLINE GAMBLING

FEDERAL. On March 26, 2014, Senator Lindsay Graham (R-SC) introduced S. 1259, and Representative
Jason Chaffetz (R-UT) introduced H.R. 4301, bills prohibiting the transmission of wagering information and applicable to Internet gambling. S. 1259 had been referred to the Judiciary Committee, and H.R. 4301 has been referred to the Subcommittee on Crime, Terrorism, Homeland Security and Investigations.

INTERNET GOVERNANCE

FEDERAL. On March 27, 2014, Representatives Marsha Blackburn (R-TN), John Shimkus (R-IL), Todd Rokita (R-IN), Joe Barton (R-TX), Bob Latta (R-OH) and Renee Ellmers (R-NC) introduced H.R. 4342, a bill prohibiting the relinquishment of the National Telecommunications and Information Administration’s responsibility over Internet domain name system functions pending a report to Congress. The bill has been referred to the Committee on Energy and Commerce.

ELECTRONIC DEVICE PRIVACY

FEDERAL. On March 27, 2014, Senator Al Franken (D-MN) introduced S. 2171, a bill requiring companies to secure permission of their users before gathering location data from smartphones, tablets and navigation devices used in cars. Consent would also be required before companies could share the information with third parties. The bill has been referred to the Judiciary Committee.

BLACK BOX DATA PRIVACY

FEDERAL. On April 9, 2014, the Senate Commerce, Science and Transportation Committee passed SB 1925, a bill sponsored by Senator John Hoeven (R-ND) prohibiting a person other than the driver or lessee of a vehicle from accessing data recorded or transmitted by an event data recorder installed in a passenger car unless 1) authorized by a court; 2) all owners or lessees consent; 3) pursuant to an NTSB investigation; 4) necessary to determine emergency medical response in a crash; or 5) retrieved for traffic safety research. When data is accessed pursuant to the enumerated exceptions, the disclosure of personally identifiable information is prohibited.

NEWS ARTICLES & REPORTS

“Trends in Unwanted Online Experiences and Sexting: Final Report”

This report by the Crimes Against Children Research Center summarizes key findings from the Third Internet Youth Safety Survey. Topics covered include youth reports of unwanted sexual solicitations, online harassment, uninvited exposure to sexual materials and sexting. The report may be accessed at http://www.unh.edu/ccrc/pdf/Full%20Trends%20Report%20Feb%202014%20with%20tables.pdf.

“Social Media and Police Leadership: Lessons from Boston”

This report by the National Institute of Justice discusses the Boston Police Department’s effective use of social media during the Boston Marathon investigation. It can be accessed at http://ncjrs.gov/pdffiles1/nij/244760.pdf.