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.

**FCC ISSUES GUIDE FOR SECURING SMARTPHONES**

The Federal Communications Commission (FCC) released the “Smartphone Security Checker,” an online tool containing a 10-step action plan that smartphone users can use to protect their personal data if their phones become infected with malware or are lost or stolen. The tool allows users to select from Android, Apple iOS, Blackberry and Windows Phone devices, and while many of the tips are the same or similar, they include links to OS-specific instructions. The site also features a general 10-step checklist which recommends that you:

1) Set PINs and passwords on your home screen, using a different password for each application, such as ebanking. Configure your phone to automatically lock after five minutes of idle time and use the SIM password capability.

2) Do not modify the original security settings.

3) Backup all of your data on your computer, a removable storage card or in the cloud.

4) Check an app’s legitimacy before downloading it, such as by checking reviews, confirming the legitimacy of the app store and comparing the app sponsor’s official website with the app store link to confirm consistency.

5) Be cautious about giving apps access to your personal information or letting apps perform functions on your phone. Check the privacy settings for each app before installation.
6) Install security apps that enable you to remotely locate and erase all of the data stored on your phone even if the GPS is off. A list of anti-theft protection apps can be accessed at http://www.ctia.org/consumer_info/safety/index.cfm/AID/12087.

7) Keep your operating software updated by accepting automatic updates or accepting updates when prompted by your service provider.

8) Limit your use of public hotspots and instead use protected Wi-Fi from a trusted network operator or mobile wireless connection. Be cautious when clicking web links, especially if you are asked to enter account or log-in information.

9) Wipe data off your old phone before you donate, resell or recycle it.

10) Report a stolen smartphone to your local law enforcement authority and register it with your wireless provider so it can be listed on a database and cannot be activated on any wireless network.

The FCC tool can be accessed at http://www.fcc.gov/smartphone-security.

ATTORNEYS GENERAL FIGHTING CYBER CRIME

ALABAMA

Attorney General Luther Strange’s agents joined with agents from the Walker County District Attorney’s Office to shut down “electronic bingo” operations at the Arrowhead Golf Course involving 15 machines. The agents also shut down an additional 20 machines at a nearby private building.

ARKANSAS

Attorney General Dustin McDaniel announced that two brothers who were previously arrested by his Cyber Crimes Unit agents pleaded guilty to multiple felony child pornography charges. Wendel Smith was sentenced to 40 years in prison, and an additional 40-year suspended sentence, after pleading guilty to 12 child pornography counts. William Smith was sentenced to 15 years in prison, and an additional 25-year suspended sentence, after pleading guilty to four child pornography counts. Both men will be required to register as sex offenders as a condition of their guilty pleas.

CALIFORNIA

Attorney General Kamala Harris issued recommendations for mobile application developers and the mobile industry to safeguard consumer privacy. The report, “Privacy on the Go: Recommendations for the Mobile Ecosystem,” provides guidance on developing strong privacy practices, translating those practices into mobile-friendly policies and coordinating with other mobile industry entities. The report is the result of an outreach effort that compiled input from stakeholders throughout the mobile industry. To accommodate the smaller screens of mobile devices, the report recommends the use of special notifications, such as icons or pop-up notifications, to inform consumers about how personally identifiable information is collected and shared.

HAWAII

Attorney General David Louis announced that a Tax Appeal Court has granted summary judgment for the State and ruled that online travel companies must pay approximately $150 million including interest in overdue state General Excise Taxes (GETs). The court found that the GET is a privilege tax imposed on businesses for the privilege of doing
business in Hawaii.

**ILLINOIS**

Attorney General Lisa Madigan’s investigators arrested Christopher McConnell after the execution of a search warrant at his residence revealed computer files depicting images and videos of alleged child pornography. McConnell was charged with 20 counts of possession of child pornography, a Class 2 felony, punishable by three to seven years in prison. The Canton Police Department assisted with the arrest, with assistance on the case also provided by the Fulton County State’s Attorney’s Office.

**LOUISIANA**

Attorney General James “Buddy” Caldwell announced that Philip deMahy, an advertising executive, pleaded guilty to 10 counts of possession of child pornography. Each count carries a maximum sentence of up to 10 years in prison. The case was prosecuted by Assistant Attorney General David Weilbaecher, Jr. and was the result of an investigation conducted by the State Police with assistance from the FBI.

**MARYLAND**

Attorney General Douglas Gansler announced the formation of an interdivisional unit which will focus on protecting the privacy of online users. The new Internet Privacy Unit will include Chief Deputy Attorney General Katherine Winfrey, Senior Advisor Antigone Davis, Consumer Protection Division Chief William Gruhn, Consumer Protection Deputy Chief Philip Ziperman and Assistant Attorney General Steve Ruckman, who is serving as Unit director. The Unit will monitor companies to ensure they are in compliance with state and federal consumer protection laws. It will also examine weaknesses in online privacy policies and work alongside major industry stakeholders and privacy advocates to provide outreach and education to businesses and consumers to broaden awareness about privacy rights so they are more equipped to manage online privacy challenges. Additionally, the Unit will pursue enforcement actions where appropriate to ensure consumer privacy is protected.

**MASSACHUSETTS**

Attorney General Martha Coakley’s Office and the National Federation of the Blind entered into an agreement with Monster Worldwide Inc. whereby the job search website and mobile application will become the first to provide job seekers who are blind with full access to all of its products and services. Monster will use screen access software that transforms on-screen information into Braille or speech. Monster will also train its customer service representatives to assist users who are blind and will establish a standing committee to oversee implementation of the agreement and other accessibility issues. The matter was handled by Assistant Attorney General Genevieve Nadeau and Paralegal Bethany Brown of the Civil Rights Division and Assistant Attorney General Maura Healey, Chief of the Public Protection and Advocacy Bureau.

**MISSISSIPPI**

Attorney General Jim Hood’s Cyber Crime Unit investigators arrested Michael Buckley on one count of possession of child pornography. The arrest is the result of an undercover Internet investigation conducted by Attorney General Hood’s Internet Crimes Against Children Task Force and the Louisiana State Police. The Pearl River County Sheriff’s Office assisted with the arrest. If convicted, Buckley faces up to 40 years in prison.
MISSOURI

Attorney General Chris Koster and Jackson County Prosecuting Attorney Jean Baker filed 17 felony charges against Terry Morrow, Jr. for an identity theft scam which spanned two states and involved more than $1 million in fraudulent car loans. The complex scam arose from the operation of Edge Auto Sales, an auto dealership owned by Morrow. Morrow acquired personal information of his victims through Edge’s car sales and online applications for auto financing. He allegedly used that information to forge dozens of fraudulent auto loans which he sold to automotive finance companies.

NEW JERSEY

Attorney General Jeffrey Chiesa announced the arrest of 24 men and one male juvenile in Operation Ever Vigilant aimed at the possession and distribution of child pornography. The sweep integrated more than 50 State Police troopers and agents from dozens of law enforcement agencies. The New Jersey Internet Crimes Against Children Task Force executed 25 search warrants in 25 different towns, with all of the warrants made by the State Police T.E.A.M.S. Unit. The charges stemming from the operation will be prosecuted by Attorney General Chiesa’s Division of Criminal Justice.

OHIO

Attorney General Mike DeWine’s Bureau of Criminal Investigation (BCI) agents arrested William Noble on eight counts of Pandering Obscenity Involving a Minor. The arrest was made after the agents served a search warrant at Noble’s home. The Chillicothe Police Department assisted with the arrest.

OREGON

Attorney General Ellen Rosenblum announced that Catalin Dulfu was sentenced to 15 years in prison after being convicted by a jury of 15 counts each of first and second degree encouraging child sexual abuse. Dulfu was also fined $5,000, which will go into a fund established for a young female victim forced to appear in some of the pornographic images found in Dulfu’s possession. The case was prosecuted by Assistant Attorney General Michael Slauson and investigated by Internet Crimes Against Children (ICAC) special agents Page McBeth and Mark Posler.

PENNSYLVANIA

Attorney General Kathleen Kane’s Child Predator Unit agents arrested Shane Niederriter, who is accused of using social media to pose as a modeling scout and solicit nude pictures from a mother and her 20-month-old daughter. The mother contacted the Knox Police Department which assisted with the investigation and arrest. Unit agents executed a search warrant of Niederriter’s computers which revealed hundreds of pictures and videos of child pornography. Niederriter is charged with 25 counts of possession of child pornography and one count of criminal use of a communication facility. The State Police also assisted with the investigation. The case will be prosecuted by Deputy Attorney General Anthony Marmo of the Unit.

SOUTH CAROLINA

Attorney General Alan Wilson announced that the Mount Pleasant Police Department, a member of Attorney General Wilson’s Internet Crimes Against Children Task Force, arrested Michael Francis on one count of possession of child pornography, a felony offense punishable by up to 10 years in prison. Francis sold a laptop to a pawn shop, but
when the shop staff prepared to wipe the laptop clean for resale, they discovered a file that suggested child pornography and alerted the police. A subsequent investigation confirmed the file contained child pornography, and Francis admitted to downloading it. Police also seized several computers and other media devices from Francis. The case will be prosecuted by Attorney General Wilson’s Office.

VERMONT

Attorney General William Sorrell announced that a shared investigation between his Office and the Vermont Internet Crimes Against Children Task Force has resulted in the arrest of Kevin Gallagher and David Faulkner on four counts each of felony Possession of Child Pornography. The investigation revealed that both men obtained child pornography over the Internet using peer-to-peer file sharing programs.

TEXAS

Attorney General Greg Abbott’s Cyber Crimes Unit arrested Forrest Johnson, who indicated he is a U.S. Customs and Border Protection agent assigned to the Austin-Bergstrom International Airport, on a second-degree felony charge for online solicitation of a minor. Johnson posted an explicit online advertisement and received a response from an individual he believed to be a 15-year-old girl but was actually an undercover police officer. Johnson was arrested when he arrived at a prearranged meeting place. If convicted, he faces two to 10 years in prison and up to a $10,000 fine.

VIRGINIA

Attorney General Ken Cuccinelli announced that Troy McDowell was sentenced to six years in prison after pleading guilty to the following child pornography counts: one count of distribution, two counts of possession with intent to distribute and seven counts of possession. McDowell was identified through an undercover investigation into the trading of child pornography over peer-to-peer networks on the Internet by a Southern Virginia Internet Crimes Against Children Task Force law enforcement officer. Officers executed a search warrant for McDowell’s residence, and McDowell admitted to downloading child pornography and allowing others to download files from him at that time. A forensic examination of the computers seized during the search confirmed the existence of hundreds of child pornography images. Assistant Attorney General Tommy Johnstone prosecuted the case.

WASHINGTON

Attorney General Bob Ferguson’s Office entered into a settlement with Arrow Outlet, resolving a lawsuit it brought over the bogus bids on Arrow’s Internet auctions. Bidders for electronics and other goods auctioned on ArrowOutlet.com thought they were competing against other people, but Arrow Outlet instead created bogus bids ("bidbots") that rigged results. According to the consent decree, Arrow Outlet is barred from running penny auctions and has agreed not to misrepresent online products and services. The company will pay $20,000 in attorney’s fees and $15,000 in penalties. It will also pay Attorney General Ferguson’s Office $50,000 to run a restitution fund for state consumers.

WISCONSIN

Attorney General J.B. Van Hollen announced that Grant Rondorf was charged with 14 counts of Possession of Child Pornography. The charges resulted from the execution of a search warrant at Rondorf’s home by Attorney General Van Hollen’s Division of Criminal Investigation special agents and agents from the U.S. Immigration and Customs En-
enforcement’s Homeland Security Investigations. Rondorf’s IP address and email account had been associated with child pornography, and during an interview at his residence, Rondorf admitted to agents that he possesses and distributes child pornography. A forensic preview of files from Rondorf’s laptop and removable storage device uncovered 10 video files and dozens of images of child pornography.

**AVAILABLE FEDERAL GRANTS**

The U.S. Department of Justice has announced the 2013 Bureau of Justice Assistance (BJA) Visiting Fellows Program. State agencies may submit nominations for the fellowship program, with a maximum stipend award of $225,000. Each selected nominee will be placed in the BJA Policy Office to work on one of the following areas: Adjudication and Law Enforcement, Justice Systems, Justice Information Sharing and Strategic Initiatives. Nominations are due on March 28, 2013. Additional information and application instructions are available at [http://www.grants.gov](http://www.grants.gov).

**CYBER NEWS BRIEFS**

**NTIA ANNOUNCES STATE FUNDING FOR SAFETY NETWORK**

The National Telecommunications and Information Administration (NTIA) announced state allocations of $122.5 million in federal grant funds to be used for planning the nationwide public safety network. The funding allocations are calculated mainly according to a formula weighted to favor higher populations. NTIA has capped the grant maximum at $6 million. The funds come with a matching requirement of at least 20 percent, either in cash or in-kind contributions. States must apply for their share of the funds by March 19 of this year. The application information may be accessed at [http://www.ntia.doc.gov/other-publication/2013/sligp-federal-funding-opportunity](http://www.ntia.doc.gov/other-publication/2013/sligp-federal-funding-opportunity).

**FTC ISSUES MOBILE PRIVACY GUIDELINES**

The Federal Trade Commission (FTC) issued a report suggesting privacy guidelines for mobile platform developers in a move aimed at protecting user privacy. Based on data gathered by trade associations, academia, privacy groups and the FTC’s own experience with mobile privacy issues, the report recommends that consumers should have to actively consent before apps can access “sensitive” information, such as geolocation, contacts, photos or media recordings. In addition, the FTC suggests a “dashboard” could be put in place allowing mobile users to see the content accessed by downloaded apps. While the guidelines are presently non-binding, the FTC asks mobile platform and app developers to consider implementing “Do Not Track” features so third parties, such as advertisers, would not be able to track users. The guidelines also suggest privacy policies should be easily accessible. Finally, the report asks for the creation of standardized app developer privacy policies, as well as education in privacy issues for consumers, with potential options being short-form privacy disclosures and self-regulatory bodies. The full report can be accessed at [http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm](http://www.ftc.gov/opa/2013/02/mobileprivacy.shtm).

**TWITTER: MOST REQUESTS ARE SUBPOENA-ONLY**

Most U.S. law enforcement agencies do not obtain a search warrant before they seek information about a Twitter user, according to the company’s second transparency report. Twitter said it received slightly more than 1,000 requests for information
between July and December 2012, mostly from the U.S., and it complied with 70 percent of the data requests. Most of the foreign data requests came from Japan, Brazil, Great Britain and France. According to the report, most U.S. government agency requests came with only a subpoena, and only 19 percent came with a search warrant, which the company requires for disclosure of the content of communications. Another 11 percent were accompanied by a court order. The transparency report can be accessed at https://transparency.twitter.com/overview.

NEW SITE TRACKS TERMS OF SERVICE CHANGES

Docracy.com has launched its Terms of Service Tracker, which enables users to track changes in the Terms of Service for about one thousand sites. Docracy uses Github-style version control to show exactly what is changing and when it changed. The tracker allows users to view terms of service of a site at a given point in time, as well as to compare an earlier version of terms of service with present terms, complete with strike-throughs and new sections highlighted in green. It works by crawling through each page daily, and whenever the tracker notices a change, it caches the new version. The tracker can be accessed at http://www.docracy.com/tos/changes.

IBM GRANTED MOST PATENTS IN 2012

IBM was granted 6,478 patents in 2012, the 20th consecutive year it has topped the patent rankings, according to the annual compilations by IFI Claims Patent Services. The company’s patent asset generates an estimated $1 billion per year in license revenue. One IBM invention granted a patent in 2012 was for the question-answering technology used in the IBM Watson computer that defeated human “Jeopardy” champions. Second place was Samsung Electronics with 5,081 patents. The big movers, however, were rivals Google and Apple. Google was granted 1,151 patents, a 170 percent increase over the previous year, no doubt benefiting from the filings it obtained from its acquisition of Motorola Mobility. It ranked 21st in 2012 compared with 65th in 2011. Apple was awarded 1,236 patents, a 68 percent increase over the previous year, ranking 22nd in 2012 compared with 39th in 2011.

And see this report on patents...

The increasing number of patents is driving the economies of U.S. cities, according to a study by the Brookings Institute, a nonprofit research and policy think tank. The study, “Patenting Prosperity: Invention and Economic Performance in the United States and its Metropolitan Areas,” also found that patent ownership has become broader, with 9,909 entities receiving patents in 2011 compared with 2,677 entities in 1967. However, most of the patent holders are clustered in 20 of the 360 statistical metropolitan areas in the U.S. where 34 percent of the population resides. Not surprisingly, San Jose, California leads in both total patents and rate of patenting per capita. The study finds that residents of patent-intensive metro areas have higher incomes, even when compared with residents of cities of comparable size and education levels. The report also addresses policy issues, finding that many high quality patents are the result of research and development funding from the U.S. government. The report also discusses ways in which the government might deal with non-practicing entities (NPEs), often called “patent trolls,” that buy up patent portfolios only to extract payments from companies. Finally, the report addresses the need for the U.S. Patent and Trademark office to improve the examination process. The report may be accessed at http://www.brookings.edu/-/media/research/files/reports/2013/02/patenting_prosperity_rothwell/patenting_prosperity_rothwell.pdf.
BUSINESS GROUP WARNS AGAINST CYBERSECURITY REGS

The Business Roundtable, an association of CEOs of U.S. companies, issued a report calling for nonregulatory cyber security policies. A key recommendation in the report was for improved public-private collaboration on cyber security. However, the association cautioned against efforts to regulate the cyber security practices of the private sector. The report may be accessed at http://businessroundtable.org/uploads/studies-reports/downloads/More_Intelligent_More_Effective_Pre-Publication.pdf.

And see Senate survey...

Many Fortune 500 companies support the creation of federal cyber security standards to protect them from Internet threats if the standards are voluntary, according to a survey conducted by staff of the Senate Committee on Commerce, Science and Transportation. The report resulted from letters sent to Fortune 500 companies by the Committee’s chairman, Senator Jay Rockefeller (D-WV). Approximately 300 companies responded to the survey, which showed broad support for the effort to enact cyber security laws and for collaboration with the federal government. However, the report also indicated concerns that new standards would become mandatory, inflexible or duplicative. The Committee staff’s memo to Senator Rockefeller summarizing the results may be accessed at http://commerce.senate.gov/public/?a=Files.Serve&File_id=5a85f211-aSc9-4306-9c84-d3a6.

STUDY NAMES TOP BROADBAND-FRIENDLY STATES

Washington, Massachusetts and Delaware have made the most progress in promoting broadband and in providing a broadband-friendly environment, according to a study by trade group TechNet. Maryland and California round out the top five states in the Technet Broadband Index, which rates states on broadband adoption, network quality and segments of the economy supporting broadband. The study looked at broadband adoption in recent years as well as the pace of growth in adoption. It also looked at network speeds, based on information from Akamai and the Fiber to the Home Council, and at the economic structure supporting broadband, including the percentage of jobs in the information and communication technology sectors and an estimate of the number of app developer jobs in each state. The study can be accessed at http://www.technet.org/technet-state-by-state-broadband-report.

CALIFORNIA ALLOWS HAIL-A-RIDE APP

The California Public Utilities Commission reached an agreement that will allow Zimride, the maker of hail-a-ride app Lyft, to operate. Lyft allows individuals to give rides to others in their own cars in return for “donations.” The Commission had previously fined Lyft $20,000, but subsequently suspended its cease-and-desist order. The Commission plans to oversee Zimride temporarily to ensure it adheres to safety requirements, such as proof of insurance, national criminal background checks for drivers and Department of Motor Vehicle checks. The final decision regarding hire-a-car businesses is expected around June.

THREAT REPORT: MOBILE DEVICES ARE HOT TARGETS

The latest threat report from security firm McAfee highlights the need for vigilance on mobile devices, with smartphones and tablets becoming hot targets for cyber-criminals. The amount of malware detected on these devices by McAfee in 2012 was 44 times what it was the previous year. McAfee estimates that 95 percent of all mobile malware has
been created in the past year alone, with the vast majority made for the Android operating system. These portable devices are tantalizing targets for criminals because they are rife with both personal and financial information. The report also found that the volume of suspicious URLs increased significantly in the latter months of 2012, averaging 4.6 million per month. The full report can be accessed at http://www.mcafee.com/us/resources/reports/tp-quarterly-threat-q3-2012.pdf.

ABA: JUDGES MUST BE CAREFUL IN SOCIAL MEDIA USE

On February 21, the American Bar Association’s (ABA’s) Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 462 addressing judges’ use of social media. While acknowledging that “judicious use” of social media can be a valuable tool for public outreach, the opinion cautions judges that their participation in social networking must adhere to the ABA Model Code of Judicial Conduct. The opinion also discusses some factors that the judiciary should consider. First, it notes that since judges are barred from publicly endorsing or opposing candidates for public office, they should refrain from clicking a “like” button on political campaign sites. Judges should take care not to form relationships that convey a position of influence on their decisions and should avoid comments that may be interpreted as ex parte. They should also be aware that any information they post could be transmitted without their knowledge to others. The full opinion may be accessed at http://www.americanbar.org/content/dam/aba/administrative/professionalresponsibility/formal_opinion_462/authcheckdam.pdf.

IN THE COURTS

MOTION FOR SUPPRESSION: PROBABLE CAUSE

U.S. v. Brown, 2012 U.S. App. LEXIS 25012 (4th Cir. December 6, 2012). The Fourth Circuit Court of Appeals found that detectives had probable cause to believe the computer harbored evidence of child pornography. An investigation of an IP address associated with a computer that had downloaded files containing child pornography revealed that the subscriber was a private ambulance service. Detectives searched the business’s building, pursuant to a search warrant, but found no relevant computers. They asked employee Daniel Brown to retrieve his laptop from an ambulance, and a search of it found child pornography. Brown was charged with one count each of receiving and possessing child pornography. He moved to suppress the images found on his laptop on Fourth Amendment grounds, which was denied by the U.S. District Court for the Western District of Virginia. A jury found Brown guilty on both charges; the district court vacated the possession conviction, which carried the more lenient penalty, and sentenced him on the receipt conviction. Brown appealed the denial of his suppression motion, but the Fourth Circuit found suppression was not warranted because detectives had probable cause to believe that any computer used by Brown or his co-worker during their work shifts contained child pornography. Further, the court held that under the exigent circumstances exception, it was reasonable for officers to seize the laptop to prevent it or its contents from being damaged or destroyed. The court affirmed the district court decision.

FOURTH AMENDMENT: DELAY IN APPLICATION FOR SEARCH WARRANT

of Appeals held that the government acted reasonably in obtaining the search warrant. David Laist pled guilty conditionally in the U.S. District Court for the Middle District of Georgia to both possession and receipt of child pornography, reserving the right to appeal the court’s denial of his motion to suppress all evidence retrieved from his personal computer and five external hard drives. At issue in the appeal was whether the government’s 25-day delay in submitting an application for a search warrant while holding Laist’s computer based on probable cause was an unreasonable seizure under the Fourth Amendment. The Eleventh Circuit acknowledged that Laist had a significant possessory interest in the computer, and that there was substantial interference with his possessory interest. However, the court also noted that Laist’s possessory interest was diminished because he was afforded the opportunity to remove whatever he wanted to download from both the computer and the hard drives. Therefore, the court concluded that the government’s efforts were sufficiently diligent to pass muster under the Fourth Amendment. The court found that while a 25-day seizure based solely on probable cause was far from ideal, noting that shorter delays had been found unreasonable under different circumstances, in the instant case the totality of the circumstances showed that the government’s actions were reasonable. The district court’s denial of the suppression motion was affirmed.

FOURTH AMENDMENT: INSTALLATION OF VIDEO CAMERA

U.S. v. Anderson-Bagshaw, 2012 U.S. App. LEXIS 26220 (6th Cir. December 19, 2012). The Sixth Circuit Court of Appeals found that any potential violation of defendant’s Fourth Amendment rights was harmless. Karen Anderson-Bagshaw was found guilty of receiving disability payments by misrepresenting her physical abilities and was convicted in the U.S. District Court for the Northern District of Ohio of one count of mail fraud and 13 counts of providing false statements to obtain federal employees’ compensation. To obtain evidence, the government had installed a video camera on a utility pole overlooking Anderson-Bagshaw’s backyard. She appealed, arguing her Fourth Amendment rights had been violated since the camera captured images of her property. The Sixth Circuit held that, even if it concluded that use of the camera violated the Fourth Amendment, the violation was harmless because there was other visual evidence showing the extent of Anderson-Bagshaw’s physical injuries that made the video clips insignificant to her convictions, which the court affirmed.

FOURTH AMENDMENT: SECURITY CAMERA RECORDINGS

State v. Wallace, 2012 Ohio App. LEXIS 5443 (December 31, 2012). The Court of Appeals of Ohio, Seventh Appellate District, found no Fourth Amendment violation since the recordings were made by a private party. Amanda Wallace and other cabaret dancers were charged with prostitution because computers seized from the cabaret pursuant to a warrant showed security camera recordings of them performing dances for patrons in private rooms. They moved to suppress the recordings and for dismissal, both of which were granted by the trial court. The State appealed, and the appellate court found that since the recordings were made by a private party, there was no Fourth Amendment violation. Further, the court found that the recordings did not qualify as “wire, oral or electronic communication” under the wiretap statute. The court reversed the judgment of the trial court and reinstated the charges against Wallace et al.

INTERCEPTION UNDER ECPA: TECHNOLOGY TEST BY ISP

Kirch v. Embarq Management Co., 2012 U.S. App. LEXIS 26607 (10th Cir. December 28, 2012). The Tenth Circuit Court of Appeals found that the
ISP did not engage in an “interception” under the Electronic Communications Privacy Act (ECPA). Kathleen and Terry Kirch claimed that Embarq Management Co. intercepted their Internet communications, in violation of ECPA, when it authorized an online advertising company to conduct a technology test for direct online advertising to users most likely to be interested in the ads. Embarq moved for summary judgment, which the U.S. District Court for the District of Kansas granted. The Kirch couple appealed, but the appeals court found that Embarq could not be liable as an aider and abettor. The court concluded that because the access was only done in the ordinary course of providing Internet services as an ISP, it did not constitute an interception within the meaning of ECPA because of the ordinary-course-of-business exclusion from the definition of interception. The court affirmed the judgment of the district court.

EMAILS BETWEEN HUSBAND AND WIFE: MARITAL PRIVILEGE

U.S. v. Hamilton, 2012 U.S. App. LEXIS 25482 (4th Cir. December 13, 2012). The Fourth Circuit Court of Appeals found no abuse of discretion in the lower court’s decision that the emails between husband and wife were not subject to the marital communications privilege. Phillip Hamilton was charged with bribery and extortion under color of official right because while a state legislator, he secured state funding for a public university in exchange for employment by the university. A jury convicted him in the U.S. District Court for the Eastern District of Virginia, and he appealed, arguing among other things that the district court abused its discretion in admitting emails between Phillips and his wife. The appeals court found no such abuse, noting that Phillips did not take steps to protect the emails. The court found that the decision accorded with the admonition in Wolfe v. U.S., 291 U.S. 7, 14 (1934) against freely extending the privilege to communications outside of which marital confidences could otherwise reasonably be preserved. Further, the court said it accorded with the principle that one who was on notice that allegedly privileged material was subject to search could waive the privilege when he made no efforts to protect it. The court affirmed the judgment.

HARASSMENT: OFFENSIVE EMAILS TO GOVERNMENT OFFICIALS

State v. Wooden, 2013 Mo. LEXIS 3 (January 8, 2013). The Supreme Court of Missouri found that defendant’s emails to public officials were not protected by the First Amendment. Mark Wooden sent emails to several public officials, including an alderwoman, who received an email from him with an audio attachment in which he made reference to a sawed-off shotgun, murders and assassinations and called himself a terrorist. The State charged him with one count of harassment under Mo. Rev. Stat. § 565.090.1(2) (knowingly uses course language offensive to one of average sensibilities and therefore puts such person in reasonable apprehension of offensive physical contact), one count of harassment under Mo. Rev. Stat. § 565.090.1(5) (knowingly makes repeated unwanted communications to another person) and one count of possession of marijuana. He moved to dismiss the harassment charges as a violation of his First Amendment rights, which the trial court overruled, and a jury found him guilty on all charges. He appealed, and the Supreme Court of Missouri agreed that Wooden’s emails inflicted injury and therefore were not protected by the First Amendment. The court found that § 565.090.1(2) punished Wooden for his unprotected communications and was not unconstitutional as applied, and a juror could reasonably find that the alderwoman was placed in reasonable apprehension of offensive physical contact. However, the court reversed Wooden’s conviction under § 565.090.1(5), finding it unconstitutionally overbroad. The remainder of the judgment was affirmed.
STORED COMMUNICATIONS ACT: PERSONAL CELL PHONE DATA

Garcia v. City of Laredo, Texas, 2012 U.S. App. LEXIS 25370 (5th Cir. December 12, 2012). The Fifth Circuit Court of Appeals concluded that the Stored Communications Act (SCA) does not apply to data stored in a personal cell phone. Fannie Garcia, a former police dispatcher, sued the City of Laredo and city officials, alleging that they violated the SCA by accessing the contents of her cell phone without permission. She claimed that a police officer’s wife removed the phone from Garcia’s unlocked locker, accessed Garcia’s text messages and images and showed them to city officials. A subsequent investigation resulted in the conclusion that Garcia had violated police department rules, and she was terminated. The City moved for summary judgment, which the U.S. District Court for the Southern District of Texas granted, and Garcia appealed. The appeals court found that Garcia’s cell phone was not a “facility” protected by the SCA, which applies to facilities operated by electronic communications service providers. The court held that even if the cell phone were a facility, storage of text messages and images on the cell phone did not fit within the statute’s definition of “electronic storage,” which encompasses only information stored by an electronic communications service provider. In response to Garcia’s argument, the court found that Garcia’s personal cell phone did not provide an electronic communication service just because it enabled the use of electronic communication services. The court affirmed the district court judgment.

FIRST AMENDMENT: SEX OFFENDER BAN ON SOCIAL MEDIA USE

Doe v. Prosecutor, Marion County, Indiana, 2012 U.S. App. LEXIS 1528 (7th Cir. January 23, 2013). The Seventh Circuit Court of Appeals found that the Indiana statute prohibiting registered sex offenders from using social media was unconstitutional. Convicted sex offender Doe filed a class action suit against the Prosecutor of Marion County, Indiana alleging that Ind. Code § 35-42-4-12, which prohibited most registered sex offenders from using social networking websites, instant messaging services and chat programs, violated his First Amendment rights. The U.S. District Court for the Southern District of Indiana upheld the statute and entered judgment for the Prosecutor. Doe appealed. The appeals court noted that the Indiana law was content neutral because it restricted speech without reference to the content of the speech. The State asserted an interest in protecting public safety, specifically in protecting minors from harmful online communications, and that the statute’s breadth was necessary to achieve its goal. Doe argued that the statute burdened more speech than necessary to serve the intended interest. The appeals court found nothing dangerous about Doe’s use of social media as long as he did not improperly communicate with minors. The court noted there was no disagreement that illicit communications was but a miniscule subset of social network activity. The court found that the Indiana statute targeted substantially more activity than the evil it sought to prevent, finding that the State could have more precisely targeted illicit communications. It reversed the decision of the district court and remanded with instructions to enter judgment in favor of Doe and to issue a permanent injunction.

FOURTH AMENDMENT: GPS PLACE-MENT ON SEIZED VEHICLE

State v. Brereton, 2013 Wisc. LEXIS 15 (February 6, 2013). The Supreme Court of Wisconsin ruled that the seizure of defendant’s vehicle, during which officers installed a GPS device, did not constitute an unreasonable seizure under the Fourth Amendment. James Brereton pled guilty to several burglary counts after his motion to suppress evidence obtained through monitoring by a GPS system attached to his vehicle was denied. The Wisconsin-
sin Court of Appeals affirmed, and Brereton appealed, arguing that the court of appeals erred by upholding the denial of his motion to suppress. The supreme court disagreed, finding that the officers’ decision to obtain a warrant was proper. Further, the court found that the three-hour seizure of Brereton’s vehicle was supported by probable cause that the vehicle contained evidence of a crime and was therefore permissible. The court noted that the seizure was supported by witnesses’ reports that a car matching the make, model and license plate number of Brereton’s vehicle had been seen at the locations of several area burglaries. Further, the court found that the real time updates of the vehicle’s movements provided by the device did not alter the kind of information to be obtained under the warrant or the nature of the intrusion allowed. The court affirmed the judgment.

Ed. Note: The State’s case was argued by Daniel O’Brien, Assistant Attorney General in the Wisconsin Department of Justice.

And see another GPS placement case on a different issue...

USE OF GPS DEVICE: FAILURE TO MOVE TO SUPPRESS

State v. Allen, 2013 Ohio App. LEXIS 392 (February 8, 2013). The Court of Appeals of Ohio, 11th Appellate District, ruled that defendant’s counsel had a duty to raise the warrantless use of a GPS device in a motion to suppress. Brian Allen, Sr. was convicted of three charges of receiving stolen property. He appealed his convictions, arguing that his counsel’s failure to file a motion to suppress evidence obtained with the warrantless use of a GPS device was tantamount to ineffective assistance of counsel. The appellate court agreed, finding that counsel had a duty to raise the issue at trial because there was no strategic basis for not doing so, and therefore counsel’s performance fell below an objective standard of reasonableness. The court found that there was a reasonable probability that the outcome of Allen’s case would have differed had the motion been filed because the U.S. Supreme Court’s holding that a GPS device could not be attached to a suspect’s vehicle without a warrant would have dictated a reversal. The court reversed Allen’s convictions and remanded the case.

COMPUTER MANIPULATION: GAIN OF “PROPERTY”

Dent v. State, 2013 Fla. App. LEXIS 1846 (February 6, 2013). The Florida Court of Appeal, Fourth District, ruled that defendant did not obtain “property” when she manipulated the computer system. The State of Florida charged and proved that Kathy Dent manipulated the sheriff’s overtime assignment computer system to secure more hospital guard overtime assignments than the sheriff’s policy allowed. As a result, Dent worked those assignments and earned overtime pay. The State theorized that the overtime system manipulation prevented other deputies from signing up for overtime, so other deputies lost the opportunity to get the assignments and earn overtime pay. A trial court jury convicted Dent of engaging in an organized scheme to defraud, in violation of Fla. Stat. § 817.034(4), and Dent appealed. The appellate court found that the State failed to prove that Dent obtained “property” within the meaning of the statute, only proving the inability of other deputies to sign up for the opportunity to obtain overtime. The court further found that Dent’s conduct was not a crime because the hallmarks of property, exclusivity and transferability were not present in the lost opportunity to work overtime. The court stated that Dent’s conduct may have violated department policies, but there was no violation of the statute. The court ordered the judgment reversed and Dent’s conviction and sentence vacated.

Ed. Note: The State’s case was argued by Assistant Attorney General Mark Hamel of the Office of the Florida Attorney General.
LEGISLATIVE NEWS

Internet Gambling

NEW JERSEY. On February 26, Governor Chris Christie signed S. 1565, a bill legalizing Internet gambling, into law, making New Jersey the third state to do so. The new law allows the online playing for money of any game currently offered by Atlantic City’s 12 casinos. Players would have to set up online accounts with a particular casino and could set daily limits on the amount of money put into play. They would also be subject to the same personal limits as gamblers physically present in casinos. The law also allows gamblers in other states to place bets in New Jersey if regulators determine such activity is not prohibited by federal law or any other state law. The new law will take effect when the state Division of Gaming Enforcement sets a start date, projected to be between three and nine months from the date the bill was signed.

Technology-Based Crimes

NEVADA. On February 4, S. 25 was referred to the state Senate Government Affairs Committee. The bill would authorize the Attorney General’s Office to investigate and prosecute alleged technological crimes, to pursue the forfeiture of property related to those cases and to seek ways to prevent a recurrence of those crimes. If enacted, the legislation would become effective on July 1, 2013.

Photoshopping

GEORGIA. On January 11, HB 39, a bill that would make altering a photograph that “causes an unknowing person wrongfully to be identified as the person in an obscene depiction” a misdemeanor. A person convicted of that crime would be subject to a fine of not more than $1,000 or imprisonment for one year, or both.

NEW RESOURCES

Children Exposed to Violence


National Crime Victims Week 2013


TECHBeat


Community Justice

This report provides highlights from a roundtable discussion with local, state and federal policymakers and practitioners about engaging the public in
Social Media Outreach

This article features the Johnson County, Kansas Sheriff’s Office discussion of their “tweet-along.” Access at http://www.ncjrs.gov/nicreleases/tweet-along.html.

Strategic Planning Assessment Strategies


Juvenile Statistics

These FAQs address juvenile offending, victimization and involvement in the juvenile justice system. Access at http://www.ojjdp.gov/ojstatbb/faqs.html.