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.

Left: NAAG President and Maryland Attorney General Douglas Gansler at his Presidential Initiative Summit on “Privacy in the Digital Age.”

ATTORNEYS GENERAL AND FACEBOOK LAUNCH ONLINE SAFETY CAMPAIGN; ATTORNEY GENERAL GANSLER HOSTS PRESIDENTIAL SUMMIT

The National Association of Attorneys General (NAAG) and Facebook launched a consumer education program designed to provide teens and their parents with tools and tips to manage their privacy and visibility on Facebook and, more broadly, on the Internet. The announcement was made by NAAG President and Maryland Attorney General Douglas Gansler during his Presidential Initiative Summit on “Privacy in the Digital Age,” held at National Harbor on April 14-16.

State-specific public service announcements (PSAs) with 19 Attorneys General and Facebook Chief Operating Officer Sheryl Sandberg have been distributed. “What You Can Do to Control Your Information” introduces an Internet safety video answering top questions about privacy, bullying prevention...
and overall Internet safety. The PSA, video and a privacy tip sheet will be shared with consumers on Facebook at www.facebook.com/fbsafety and on participating Attorneys General Facebook pages and office websites.

Attorney General Gansler’s Summit addressed the latest legal and policy issues on digital privacy. Prominent speakers addressed such topics as cybersecurity, data mining, children’s online privacy, government responses and market solutions to Internet privacy. A copy of the agenda as well as a video of the sessions and meeting materials is available on the NAAG website at http://www.naag.org/md-ag-pi-summit-registration.php.

ATTORNEYS GENERAL FIGHTING CYBER CRIME

MULTI-STATE

The Attorneys General of 38 states and the District of Columbia entered into a $7 million settlement with Google over privacy concerns involving the company’s collection of data from unsecured wireless networks during operation of its Street View service. Google’s Street View cars were equipped with antennae and open-source software that the company acknowledged collected information for its geolocation services, but also collected and stored “payload” data from unsecured business and personal wireless networks. Although Google represented it was unaware of the collection of payload data, the agreement of voluntary compliance acknowledged this information may have been included in their collection. Google has since disabled or removed the equipment and software used in the collection of this data and, according to the agreement, this information will be destroyed as soon as legally practicable. Other key elements of the agreement require Google to conduct an employee training program about privacy and confidentiality of user data for at least 10 years, as well as conduct a public service advertising campaign to educate consumers about better securing their personal information when using wireless networks. The executive committee negotiating the settlement included the Attorneys General of Connecticut, Arizona, Florida, Illinois, Kentucky, Massachusetts, Missouri and Texas. Additional states participating in the settlement were: Alaska, Arkansas, California, Colorado, Delaware, Hawaii, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee, Vermont, Virginia and Washington.

ALASKA

Attorney General Michael Geraghty announced the arrest of Michael Padilla on more than 20 counts of distribution of indecent material to minors. The arrest resulted from a proactive peer-to-peer investigation by the Alaska State Troopers in connection with the Alaska Internet Crimes Against Children (ICAC) Task Force. Padilla had more than 100 images and videos of child pornography on his digital devices.

ARKANSAS

Attorney General Dustin McDaniel’s Cyber Crimes Unit agents arrested Clint Fields on 22 counts of possession of child pornography, a Class C felony. The agents executed a search warrant at Fields’ residence and seized a laptop computer, which will be analyzed by the Unit’s Forensic Lab. The arrest resulted from an investigation by Special Agent Chris Cone upon suspicion of child pornography located at Fields’ residence. The Paragould Police Department assisted in the investigation, and the case will be prosecuted by the Second Judicial District Prosecuting Attorney.

CALIFORNIA

Attorney General Kamala Harris filed criminal charges against Shou Lin Wen and Yuting Tan, who
allegedly bought large numbers of stolen smartphones in California for resale in Hong Kong, raking in nearly $4 million in less than a year. The charges follow a six-month multi-state investigation into the trafficking of stolen smartphones by Attorney General Harris’ eCrime Unit. Unit Special Agents conducted surveillance operations and tracked shipments, intercepting four of the 110 parcels shipped. Wen and Tan were charged with eight felony counts of money laundering, grand theft, possession of stolen property and conspiracy. According to the arrest warrant, co-conspirators enlisted homeless people to purchase multiple smart phones from carriers and then deliver the phones to the co-conspirators for a nominal payment. It is alleged that the straw purchasers never intended to honor the phones’ service contracts which, under state law, constitutes theft by false pretenses and designates the phones as stolen property. Hundreds of these stolen phones were then sent to Wen and Tan, who shipped them to Hong Kong, where iPhones can sell for up to $2,000.

KENTUCKY

Attorney General Jack Conway announced the arrest of Timothy Johnston following an investigation by Attorney General Conway’s Cybercrimes Unit. Johnston was arrested by the Independence Police Department on five counts of distribution, and one count of possession, of child pornography. The charges follow a month-long investigation after the Unit received a complaint from the National Center for Missing and Exploited Children and AOL that an Internet user had transmitted child pornography images via email. Unit investigators executed a search warrant at Johnston’s residence, and an arrest warrant was issued after a review of computers seized from the home uncovered suspected child pornography. Unit investigators also contacted the state Cabinet for Health and Family Services after learning that Johnston had two foster children in his care. The charges against Johnston are Class D felonies carrying a penalty of one to five years in prison and registration as a sex offender if he is convicted.

LOUISIANA

Attorney General Buddy Caldwell announced that Richard Wells-Lightsey was arrested on child pornography charges. The arrest was part of a joint investigation involving Attorney General Caldwell’s High Technology Crime and Fugitive Apprehension Units, Homeland Security Investigations and the East Baton Rouge Parish Sheriff’s Office. Wells-Lightsey is charged with one child pornography count and one count of unauthorized use of a wireless router system to access child pornography. If convicted, he could face up to 30 years in prison.
MASSACHUSETTS

Attorney General Martha Coakley announced the indictment of Daniel Goichman on three counts of possession, and six counts of dissemination, of child pornography. State Police assigned to Attorney General Coakley’s Office learned a registered sex offender was allegedly soliciting minors over the Internet. They executed a search warrant at Goichman’s residence and seized evidence of suspected child pornography. With assistance from the Southborough Police Department, the State Police officers arrested Goichman at his residence. Further investigation of the evidence seized indicated Goichman was allegedly distributing child pornography over the Internet. The case will be prosecuted by Assistant Attorney General Timothy Wyse of Attorney General Coakley’s Cyber Crime Division. Attorney General Coakley’s Computer Forensics Lab investigators participated in the case.

NEW JERSEY

Attorney General Jeffrey Chiesa announced that Daniel Derringer was arrested by State Police at his home on charges that he used the Internet to coerce a 15-year-old girl from Minnesota into posing nude and engaging in sexual conduct on a webcam. Derringer was charged with manufacturing (2nd degree) and possessing (4th degree) child pornography. The charges resulted from an investigation by the State Police Digital Technology Investigations Unit, led by Detective G. Michael Williams, and Derringer will be prosecuted by Supervising Deputy Attorney General Kenneth Sharpe of Attorney General Chiesa’s Division of Criminal Justice Financial & Computer Crimes Bureau. Minnesota police traced the girl’s communications to Derringer’s address and alerted the New Jersey State Police, who executed a search warrant at Derringer’s home and seized his laptop computer, finding videos of the girl.

NEW MEXICO

Attorney General Gary King’s Office obtained an indictment against Alberto Villavisencio on 40 counts of manufacturing and two counts of distributing child pornography. A tip to the Bernadillo County Sheriff’s Office led to the execution of a search warrant at Villavisencio’s home, where computer images of child pornography were discovered. Villavisencio was arrested by the Bernadello County Sheriff’s Office and will be prosecuted by Attorney General King’s Office. If convicted, he faces more than 360 years of incarceration.

OHIO

Attorney General Mike DeWine’s Crimes Against Children initiative, which operates as a division of the Ohio Bureau of Criminal Investigation, simultaneously served search warrants at homes across the state as part of “Operation Download.” Each home had been identified by investigators as a site illegally possessing and downloading child pornography. Investigators with the Lake County and Vinton County Sheriff’s Offices; the Mentor, New Richmond and Perrysburg Township Police Departments; and the FBI Child Exploitation Task Force assisted in serving the warrants.

SOUTH CAROLINA

Attorney General Alan Wilson’s Office hosted a town hall meeting for parents, children and teachers as part of his Internet Crimes Against Children (ICAC) “Stay Safe Online” Week. Attorney General Wilson’s Office also made presentations at public schools throughout that week.

TEXAS

Attorney General Greg Abbott’s Cyber Crimes Unit, in a joint undercover operation with the McAllen and Rio Grande City Police Departments, arrested Alberto Gomez for online solicitation of a minor. Gomez initiated online chats and exchanged sexually graphic text messages with someone he
thought was a 14-year-old girl, but was actually an undercover Unit officer. Gomez sexually propositioned the “girl” and arranged to meet. He was arrested after a chase when he arrived at the meeting place. Officers confiscated his cell phone, which revealed the sexually explicit messages he had exchanged.

WASHINGTON

Attorney General Bob Ferguson’s Office filed a court order signed by T-Mobile and effective nationwide that ensures the company clearly communicates the limitations of its “no contract” wireless service plan and allows consumers duped by its deceptive ads to exit their contracts with no penalty. After an investigation of the company’s practices, Attorney General Ferguson’s Office learned T-Mobile failed to disclose that customers who purchase a phone with the 24-month payment plan must carry a wireless service agreement with them for the entire 24 months, or pay the full balance owed if they cancel earlier. Under the Assurance of Discontinuance, T-Mobile agrees to stop misrepresenting that wireless service and phone equipment can be obtained without restrictions and stop failing to disclose that customers who terminate their T-Mobile wireless service before their device is paid off will have to pay the balance due at time of cancellation. T-Mobile will also pay $26,046.40 in attorney’s fees and costs to Attorney General Ferguson’s Office.

WISCONSIN

Attorney General J. B. Van Hollen’s Division of Criminal Investigation (DCI) special agents, with assistance from the Milwaukee Police Department, a member of Attorney General Van Hollen’s Internet Crimes Against Children (ICAC) Task Force, arrested Alejandro Arguello on five counts of possession of child pornography. According to the criminal complaint, agents executed a search warrant at Arguello’s home and seized a laptop computer. Forensic reviews of images recovered from the laptop were consistent with child pornography. The Milwaukee County District Attorney’s Office will prosecute the case.

IN THE COURTS

GPS TRACKING DEVICE: PROBABLE CAUSE

Commonwealth v. Burgos, 2013 Pa. Super. LEXIS 74 (February 20, 2013). The Superior Court of Pennsylvania ruled the facts of the case supported the requisite probable cause for authorizing the installation of the GPS tracking device. Informants described how Edwin Burgos traveled to Georgia and Michigan to obtain his supply of marijuana, bringing it back in a hidden compartment in his pickup truck. Conversations intercepted in court-ordered wiretaps corroborated that information. Officers obtained an order authorizing the installation and use of a GPS tracking device pursuant to Pa. C.S. § 5761, and Burgos’ truck was traced. After the truck was stopped, officers obtained a search warrant for the truck and found marijuana in the hidden compartment. At trial, Burgos moved to suppress all evidence obtained from the use of the GPS and the stop and search of his truck due to lack of probable cause and a warrant to attach the GPS, a motion which was first denied, then granted by the trial court. The appellate court did agree that police needed probable cause to attach and monitor a GPS on an individual’s vehicle. The court concluded that the wiretap orders in the instant case served as the functional equivalent of traditional search warrants. Therefore, the court found that the issuance of the order authorizing the GPS device was proper. The order granting the motion to suppress was reversed and the cases remanded for further proceedings.
SUPPRESSION OF WARRANT STATEMENTS: GOOD FAITH EXCEPTION

U.S. v. Woerner, 2013 U.S. App. LEXIS 3742 (5th Cir. February 22, 2013). The Fifth Circuit Court of Appeals found that suppression was not justified due to the good faith exception to the exclusionary rule. Mark Woerner was convicted in the U.S. District Court for the Southern District of Texas on two counts of possession, and three counts of distribution, of child pornography. He appealed, challenging the district court’s denial of his motion to suppress email records, arguing that the warrant authorizing their seizure was supported by his own statements that were later suppressed as fruits of an unlawful search. The Fifth Circuit found that suppression of the emails was not warranted because the good faith exception to the exclusionary rule applied, since any police misconduct leading to the inclusion of Woerner’s statements in the warrant application was at most the result of negligence. The court added that the affiant could not have known that the statements would later be suppressed. The court found there was sufficient evidence to convict Woerner and affirmed his conviction.

RESTITUTION: SHOWING OF PROXIMATE CAUSE

U.S. v Gamble, 2013 U.S. App. LEXIS 4008 (6th Cir. February 27, 2013). The Sixth Circuit Court of Appeals ruled that a showing of proximate cause was required for establishing restitution. James Gamble and Shawn Crawford pled guilty to possession and receipt of child pornography in the U.S. District Court for the Eastern District of Tennessee. The district court then ordered them jointly and severally under 18 U.S.C.S. § 2259 to pay over $1,000,000 in restitution to “Vicky,” the pseudonym of an individual depicted in the images they possessed or received. Crawford appealed. The appellate court noted that although the district courts did not require a showing of proximate cause between the losses and the defendants’ offenses, the Fifth Circuit had such a requirement. The court found the cases had to be remanded so that the analysis of proximate cause could take place. On remand, the district court had to reconsider the extent to which defendants had to pay restitution where they shared responsibility for “Vicky’s” injuries with hundreds of other viewers of child pornography.

But see...

U.S. v. Fast, 2013 U.S. App. LEXIS 4807 (8th Cir. March 11, 2013). The Eighth Circuit Court of Appeals found the victim’s losses were not clearly traceable to defendant’s crime. Robert Fast pled guilty to one count of receiving and distributing child pornography. The U.S. District Court for the District of Nebraska ordered him to pay $3,333 in restitution under 18 U.S.C.S. § 2259 to “Vicky,” a victim whose images were on Fast’s computer. The victim challenged the amount of the restitution award by appeal and by a petition for mandamus, seeking $952,759.81 in restitution based on losses which she documented from her sexual abuse and the distribution of the pornographic images (having previously collected $271,937.23 from other defendants.) Fast moved to dismiss the appeal. The circuit court agreed with the district court that Fast could not have caused, and therefore could not be liable for, losses before the date Fast first possessed images of the victim. The court concluded that all $952,759.81 of the victim’s losses were not clearly and indisputably traceable to Fast’s crime. The court granted Fast’s motion to dismiss and denied the petition for mandamus.

DEFINITION OF “DUPLICATES:” DOWNLOADING IMAGES

State v. Pugh, 2013 Ore. App. LEXIS 186 (February 21, 2013). The Court of Appeals of Oregon ruled the statutory definition of “duplicates” includes downloading. Charles Pugh was convicted of first-degree encouraging child sexual abuse under Or. Rev. Stat. § 163.684. He appealed, arguing the evidence that he downloaded child pornography im-
ages from the Internet was insufficient to show he “duplicated” them for purposes of the statute. The appellate court disagreed, finding 1) the statutory term “duplicates” includes downloading images from the Internet and saving them; and 2) he engaged in this activity knowing the images contained child pornography based on the names he gave the file folders in which he stored them. The convictions were affirmed.

Ed. Note: Ryan Kahn, Assistant Attorney General in the Oregon Department of Justice, argued the case for the State.

FOURTH AMENDMENT: USE OF VIDEO CAMERA IN RESIDENCE

Commonwealth v. Dunnavant, 2013 Pa. Super. 38 LEXIS 83 (February 27, 2013). The Superior Court of Pennsylvania ruled that the use of a hidden digital camera was an unreasonable warrantless search of defendant’s residence. The Commonwealth sought review of an order granting Gerald Dunnavant’s suppression motion prohibiting the use at trial of evidence obtained from a hidden video camera worn by a confidential informant inside Dunnavant’s residence. Finding that Dunnavant had a legitimate expectation of privacy in his home, the court concluded that the hidden digital camera was a warrantless search of Dunnavant’s home; thus, it was per se an unreasonable search under the Fourth Amendment. The court also found it could not be defended under any established exception to the warrant requirement. The court affirmed the trial court’s order.

FOURTH AMENDMENT: SEARCH OF PROBATIONER’S HOME:

State v. Bogert, 2013 Vt. LEXIS 11 (February 22, 2013). The Supreme Court of Vermont ruled that the search of defendant’s home did not violate his rights under the Fourth Amendment. Thomas Bogert, Jr. pled guilty to possession of child pornography, sexual assault and aggravated sexual assault. He was convicted and sentenced, also signing a probation order that included 35 conditions, including a condition that he not possess child pornography. During a “sex offender compliance check” at Bogert’s home, evidence was collected from his computers demonstrating a violation of the terms of his probation. He moved to suppress that evidence, which was denied, and he appealed, alleging a violation of his Fourth Amendment rights. The Vermont Supreme Court disagreed, finding that Bogert’s expectation of privacy, in light of his conditional reentry status, was outweighed by the State’s supervision goals. The judgment of the lower court was affirmed.

FOURTH AMENDMENT: BORDER LAPT- TOP SEARCHES

U.S. v. Cotterman, 2013 U.S. App. LEXIS 4731 (9th Cir. March 8, 2013). The Ninth Circuit Court of Appeals held that the forensic examination of defendant’s laptop required a showing of reasonable suspicion under the Fourth Amendment. Border agents seized Howard Cotterman’s laptop at the U.S.-Mexico border in response to a Treasury Enforcement Communication System (TECS) alert based in part on Cotterman’s previous conviction for child molestation. Their initial search of the laptop at the border did not reveal any incriminating evidence. The laptop was then shipped to a facility almost 170 miles away for a comprehensive forensic examination, during which images of child pornography were discovered. Cotterman filed a motion to suppress the evidence of child pornography in the U.S. District Court for the District of Arizona, arguing the search of his laptop 170 miles away from the point of entry was a non-routine border search requiring reasonable suspicion. The district court granted the motion, and the government appealed. The appeals court, agreeing that the forensic examination of the laptop required a showing of reasonable suspicion, found Cotterman’s TECS alert, prior child molestation conviction, frequent travel, crossing from a country known for sex tourism -- taken collectively -- gave rise to reasonable suspicion of criminal activity.
Those factors, combined with the fact that a border agent encountered at least one password-protected file on the laptop, provided the basis for reasonable suspicion to conduct a forensic examination. The order granting the motion to suppress was reversed.

FOURTH AMENDMENT: TIME LAPSE IN FORENSIC EXAMINATION

_The People v. DeProspero_, 2013 NY Slip Op 1992 (March 26, 2013). The New York Court of Appeals found that the search warrant and the custody of evidence it authorized continued to be valid. Stephen DeProspero pled guilty to predatory sexual assault in the first degree after denial of his motion to suppress evidence consisting of still-frame digital images depicting him engaged in a sexual act with a child. The images were found on a memory card of a digital camera seized pursuant to a May 4, 2010 warrant, although the forensic examination of the memory card was not performed until January 2010. DeProspero appealed, arguing that by the time the forensic examination was performed, the authority provided by the warrant had lapsed, so the search of those images in January 2010 was illegal under the Fourth Amendment. The appeals court disagreed, holding that DeProspero had no relevant expectation of privacy to ground a suppression claim based on the Fourth Amendment. The court further held that the predicate for the seizure and examination of DeProspero’s digital media was as compelling in January 2010 as it was in May 2009, and it affirmed the decision.

FOURTH AMENDMENT: SCOPE OF WARRANT

_U.S. v. Hager_, 2013 U.S. App. LEXIS 6294 (8th Cir. March 29, 2013). The Eighth Circuit Court of Appeals determined that suppression of the evidence was not warranted. During a child pornography investigation, agents found emails evidencing a sexual interest in children from an account registered in Benjamin Hager’s name at Hager’s address. An agent obtained a warrant to search Hager’s residence and found child pornography on VHS tapes. Hager was charged with receiving and possessing child pornography in the U.S. District Court for the District of North Dakota. He moved to suppress the evidence, arguing that the warrant only authorized a search for the metadata of the sexually suggestive images, and the VHS tapes could not contain metadata. The district court denied the motion, and Hager entered a conditional guilty plea, and then appealed. The appellate court found the agents did not exceed the scope of the warrant because his affidavit revealed that he sought to recover the metadata in addition and not to the exclusion of, the images themselves. The appellate court affirmed.

And see also...

_U.S. v. Suining_, 2013 U.S. App. LEXIS 7215 (8th Cir. April 10, 2013). The Eighth Circuit Court of Appeals determined that suppression of the evidence was not warranted. While CCTF, a federal task force, was investigating Douglas Suining for child pornography, a deputy, in an unrelated event, stopped him and obtained his consent to search his vehicle. Based on a drug dog’s alert, the deputy brought the vehicle to the sheriff’s office for a more thorough search. His supervisor found child pornography while searching the contents of a computer in the vehicle for evidence of drug activities. The supervisor then shut the computer down, obtained a search warrant and found more child pornography on the hard drive. The CCTF obtained additional search warrants and found child pornography at Suining’s apartment. Suining filed a motion to suppress the evidence, citing a violation of his Fourth Amendment rights, which the U.S. District Court for the District of Nebraska denied. He then entered a conditional guilty plea to one count of producing and manufacturing child pornography, and appealed. The appellate court found suppression was not warranted because the supervisor did not exceed the scope of Suining’s consent to search his vehicle by searching the computer since the supervisor did not abandon his drug
search for a new, extended search for child pornography without judicial authority. The court affirmed the denial of the motion to suppress.

**PROBABLE CAUSE: ROOMMATE’S STATEMENTS**

*Lamarre v. State*, 2013 Tex. App. LEXIS 2036 (March 1, 2013). The Court of Appeals of Texas, Fourth District, found that the trial court did not abuse its discretion in denying defendant’s motion to suppress. A trial court convicted Paul Lamarre of 22 counts of possession of child pornography. He appealed, arguing the trial court erred in 1) denying his motion to suppress, and 2) admitting the testimony of two witnesses during the punishment phase of the trial. The court of appeals found that when the deputy seized Paul Lamarre’s computer, he was legitimately in the home and had probable cause to believe the computer contained child pornography, based on the statements of Lamarre’s roommate and her son. Further, the court found that the trial court did not abuse its discretion by overruling Lamarre’s objections to the admission of the testimony of his former stepdaughters about the sexual and physical abuse Lamarre inflicted on them. Their testimony was not victim impact testimony, as it was not evidence of the effect of an offense on someone other than the stepdaughters. The trial court’s judgment was affirmed.

**WEB POSTING THREATS: DEFINITION OF “SENDING”**

*O’Leary v. State*, 2013 Fla. App. LEXIS 4221 (March 18, 2013). The Florida Court of Appeal, First District, ruled that defendant posted the threats and thereby “sent” them to his designated users. Timothy O’Leary posted a statement on his personal website which threatened an individual and was seen by the individual’s relatives. O’Leary was charged with two counts of sending written threats to kill or do bodily harm in violation of § 836.10, Fla. Stat. He moved to dismiss, arguing that, because the threats were only posted on his personal web page, they were not “sent” as required by the statute. The lower court denied the motion, and O’Leary then pled no contest to one count, specifically reserving the right to appeal the denial of his motion. On appeal, the appellate court held that by composing a statement of thought and displaying it so another could see it, O’Leary satisfied the first prong in the definition of “sending.” The court found that receipt of the threatening communication by a family member of the person threatened fulfilled the second prong. The court affirmed the denial of O’Leary’s motion to dismiss.

*Ed. note: Angela Hensel, Assistant Attorney General in the Office of the Florida Attorney General, argued the case for the State.*

**PROBABLE CAUSE: GPS “PINGING”**

*U.S. v. Barajas*, 2013 U.S. App. LEXIS 4475 (10th Cir. March 4, 2013). The Tenth Circuit Court of Appeals found that the affidavit contained facts indicating that communications between the suspects might be found in the GPS data. Samuel Barajas was convicted of conspiracy to distribute, and aiding and abetting possession with intent to distribute, methamphetamine and using a communication facility in facilitating the conspiracy in the U.S. District Court for the District of Kansas. On appeal, he challenged the denial of his motion to suppress evidence obtained from a wiretap surveillance and GPS pinging of certain cell phones. arguing the GPS pinging should not have been covered by the wiretap orders because there was no probable cause in the affidavits to support the search for GPS data. As to the wiretaps, the appeals court held that the government met its burden of showing the wiretaps were necessary. It also found the affidavit contained facts indicating the GPS data might contain communications between the suspects. The court also found no reason why GPS data could not be obtained through a wiretap order, and affirmed the conviction.
COPYRIGHT INFRINGEMENT: SAFE HARBOR PROVISION

Columbia Pictures Industries, Inc. v. Fung, 2013 U.S. App. LEXIS 5597 (9th Cir. March 21, 2013). The Ninth Circuit Court of Appeals ruled that the film studios carried their burden of proving defendants’ liability. Columbia Pictures and other film studios sued Gayr Fung, a website operator, and his company, alleging that they were liable for vicarious and contributory copyright infringement. The U.S. District Court for the Central District of California granted the film studios’ motion for summary judgment on liability and permanently enjoined Fung and his company, who appealed under the safe harbor provision of 17 U.S.C.S. § 512(a). The appeals court noted that three of Fung’s websites collected and organized torrent files, and one website automatically modified the torrent files by adding additional backup trackers to them. The court found that the film studios had proved Fung’s liability for inducing others to infringe their copyrights because 1) the inducement copyright doctrine also applied to services available on the Internet; 2) there was evidence that the predominant use of Fung’s services was to infringe copyrights; and 3) Fung actively encouraged the uploading of torrent files with copyrighted content. The court further found that the safe harbor provision was not available to Fung’s trackers because they were not “service providers” and were only “conduits” between computer users. The court affirmed the grant of summary judgment on liability and safe harbor claims, but reversed in part with regard to the injunctive relief.

JURISDICTION: EMAIL THREATS

State v. Chase, 2013 Colo. App. LEXIS 350 (March 14, 2013). The Colorado Court of Appeals, Division Six, held that a Colorado court had jurisdiction over the charges against defendant. Jerry Chase, a Colorado resident, sent threatening emails to other residents while he was in Boston, although the victims read them when they were located in Baltimore. The State convicted him on stalking charges, and he appealed, citing lack of jurisdiction. The appellate court found that the trial court had jurisdiction because Chase was a Colorado resident and knew the victims lived and would return to Colorado. The conviction was affirmed.

Ed. Note: Assistant Attorney General Patricia Van Horn represented the State.

IN THE HIGH COURT

On March 18, the U.S. Supreme Court denied certiorari in Thomas-Rasset v. Capital Records, no. 12-715, leaving intact the award of $222,000 against Thomas-Rasset for illegally downloading music files via the Kazaa file-sharing service. Thomas-Rasset had been sued in 2006 under the U.S. Copyright Act by several recording companies. Although the suit focused on 24 recordings, the lower court noted evidence that her Kazaa account contained 1,700 recordings.

CYBER NEWS BRIEFS

FTC UPDATES GUIDELINES FOR ONLINE/MOBILE ADS

The Federal Trade Commission (FTC) updated its guidelines for mobile and online advertisers to follow when placing disclosure information on its ads. For example, the FTC states that hyperlinks should be avoided in disclosing information about the cost of a product or health and safety data. If hyperlinks are used, the report directs advertisers to place them near relevant information and make it noticeable to consumers. The FTC also warns against including disclosures in pop-ups, which are often blocked on web browsers. In addition, the report suggests advertisers should consider whether people will be able to scroll down on a webpage or mobile site to read about the product’s disclosure information, notably because some browsers or mobile devices may not prompt them to scroll down. The
guidance also warns against using banners to lead to disclosures, but rather suggests including the disclosure information within the actual banner. The guidelines may be accessed at http://www.ftc.gov/os/2013/03/130312dotcomdisclosures.pdf.

**SIXTH CIRCUIT ALLOWS E-DEVICES AT ORAL ARGUMENT**

The Sixth Circuit Court of Appeals issued a new policy permitting the use of electronic devices by counsel during oral argument. Previously, the court prohibited the use of such devices at oral argument, but in light of electronic records and briefings, counsel needed access to the record. Initially, the court adhered to an informal policy allowing counsel to send a letter in advance of oral argument to the panel requesting permission to use an electronic device, but the court saw a need to formalize the process. It should be noted that the court does not provide Wi-Fi access in the courtrooms. The new policy may be accessed at http://www.ca6.uscourts.gov/internet/court_calendars/documents/Electronic_Devices.pdf.

**REPORT: MILITARY NETWORKS VULNERABLE TO CYBER ATTACK**

The U.S. military “cannot be confident” that its computer networks will continue to work in the event of a cyberattack from a reasonably competent enemy, according to an 18-month study by the Defense Science Board (DSB). The DSB is a federal advisory committee established to provide independent advice to the Secretary of Defense. Further, the study found that the military’s dependence on “flimsy” security systems “is a magnet to U.S. opponents,” who are becoming increasingly capable of attacking with potentially devastating consequences. The report may be accessed at http://acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

More federal programs violated data security standards in 2012 than in the previous year, yet computer security costs increased by more than $1 billion, according to the executive branch yearly report on compliance with the Federal Information Security Management Act (FISMA). Inadequate training was a prime reason for the decline, with 88 percent of personnel with system access privileges receiving annual security awareness instruction, compared to 99 percent in 2011. Other factors included not using smartcards to restrict network access and not automatically configuring system settings. The Defense, Homeland Security and Treasury Departments spent the most on IT security, with expenditure of $12 billion, $615.5 million and $404 million, respectively. Agencies reported experiencing about 49,000 computer security incidents during 2012; most were the result of lost or stolen equipment and data, rather than unauthorized access. The report may be accessed at http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

**11 WESTERN STATES UNITE FOR BROADBAND EFFORT**

A group of 11 Western states have decided to coordinate their resources and efforts associated with the 700 MHz nationwide broadband network to be built by FirstNet. For the original National Telecommunications and Information Agency (NTIA) proceeding, six states – Idaho, Montana, Nevada, South Dakota, Utah and Wyoming – submitted a response. Since then, five other states – Arizona, California, Nebraska, New Mexico and Oregon – have joined the group, now known as the Western States Alliance. Of particular interest to the group is the development of a sustainable business model that will deliver an effective broadband network at a price that user groups can afford.
MICROSOFT RELEASES LAW ENFORCEMENT REQUEST REPORT

Microsoft for the first time released information on law enforcement requests for customer data, covering all Microsoft services, such as Hotmail, Outlook.com, Xbox LIVE and Office 365, with a separate breakdown for requests related to Skype, which it acquired in 2011. The 2012 Law Enforcement Requests Report breaks down by country the 75,378 requests that potentially affected 137,424 accounts. Microsoft also disclosed the kind of information – content or non-content - it provided to law enforcement in each country. According to the report, law enforcement in 49 countries requested customer information. The countries with the highest volume of requests in 2012 were Turkey (11,434); the U.S. (11,073); France (8,603); Germany (8,419); Taiwan (4,381); Australia (2,238); and Brazil (2,214). The report may be accessed at http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency.

SEC: COMPANY ANNOUNCEMENTS ON SOCIAL MEDIA OK

The Securities and Exchange Commission (SEC) stated that companies may now use Twitter, Facebook and other social media to make key announcements as long as they tell investors which sites they will use. This change in the disclosure rule, known as Regulation Fair Disclosure or Reg FD, has been highly controversial, as companies have complained that it is outdated because social media has revolutionized the way they share news and attract customers. Under the new guidelines, companies could take steps such as noting on websites and press releases that they will use social media to make announcements and giving web addresses for their pages.

THREAT REPORT: SPAM DOWN, TARGETED ATTACKS UP

Spam accounted for 69 percent of emails in 2012, down from 75 percent in the previous year, but still totaling for 30 billion spam messages daily, according to Symantec’s Internet Security Threat Report 2013, which captured information from more than 69 million attack sensors in 157 countries. The report also noted that junk emails selling sex or dating products and services now account for 55 percent of all spam messages. Further, one out of every 291 email messages contains malware, with 23 percent of those with malware offering links to malicious web sites. Approximately 247,350 daily malware attacks were blocked in 2012, a 30 percent rise over 2011, according to the report. The number of targeted attacks rose 42 percent last year, averaging about 116 per day and triggering a comparable increase in data theft and industrial espionage. Small businesses with fewer than 250 employees were targeted in 31 percent of those attacks. The report may be accessed at http://www.symantec.com/security_response/publications/threatreport.jsp.

And see...

DATA BREACH REPORT: 621 CONFIRMED IN 2012

There were 621 confirmed data breaches and 47,000 reported security incidents in 2012, according to the Verizon 2013 Data Breach Investigations Report. The report noted that 92 percent of the attacks are from external sources, while 14 percent are attributable to insiders. Notably, business partners were responsible for one percent of the attacks. Further, 76 percent of network intrusions exploited weak or stolen credentials (user name, password); 40 percent incorporated malware (malicious software, script or code used to compromise information); 35 percent involved physical attacks (i.e., ATM skimming); and 29 percent leveraged social tactics (i.e., phishing). Additionally, the
compromise-to-discovery timeline is still measured in months, with 69 percent of the breaches detected by third parties. The report may be accessed at http://www.verizonenterprise.com/DBIR/2013/.

LEGISLATIVE UPDATE

Cell Phone Location Data
TEXAS. The Texas House Committee on Criminal Jurisprudence favorably reported out HB 1608, a bill that would require a warrant for location tracking of cell phones, except in the case of life threatening emergencies. The bill would also allow an order permitting tracking to be sealed for up to 180 days unless the court finds good reason to extend the seal. The bill requires police agencies to report information about the amount, type and outcome of locational tracking. If enacted, the bill would become effective on September 1, 2013.

Driving With Head-Mounted Displays
WEST VIRGINIA. A bill banning the use of head-mounted gadgets while driving was introduced. HB 3057 defines such a device as “a computing device which is worn on the head and projects visual information into the field of vision of the wearer.” First offenses would result in a $100 fine; second offenses would cost the driver $200; while subsequent offenses would result in $300 fines. If enacted, the bill would be effective on July 1, 2013. The bill was referred to the House Roads and Transportation Committee.

Service of Process Via Social Media
TEXAS. A bill introduced in the Texas House would allow service of process via social media. HB 1989 would allow such service if 1) the defendant maintains a social media page; 2) the profile on the social media page is that of defendant; 3) the defendant regularly accesses the social media page account; and 4) the defendant could reasonably be expected to receive actual notice if the electronic communication were sent to the defendant’s account. The bill was referred to the Judiciary and Civil Jurisprudence Committees.

Online Privacy
CALIFORNIA. AB 1291 was introduced, which would require online companies which retain a consumer’s information to provide a copy of that information to the consumer at no charge and within 30 days of request. The bill was referred to the Assembly Judiciary Committee.

Internet Cafes
FLORIDA. On April 10, Florida Governor Rick Scott signed HB 155 into law, a bill that would prohibit electronic gambling devices related to drawings by chance offered by nonprofit organizations, game promotions in connection with the sale of consumer goods or services, amusement games or machines, amusement centers, racketeering activity and promotional offers. It makes violations unfair and deceptive trade practices. The bill became effective immediately and was chaptered as Chapter 2013-2.

Cybersecurity
U.S. HOUSE. On April 18, the U.S. House passed HR 624 (CISPA), a bill sponsored by Representative Mike Rogers (R-MI) that would establish procedures for sharing of information about cyber threats with federal, state and local authorities. It sets forth requirements regarding the use and protection of shared information and prohibits a civil or criminal action against a cybersecurity provider acting in good faith to obtain cyber threat information. The bill has been referred to the Senate Committee on Intelligence.
NEW RESOURCES

Forensic Science

“A Simplified Guide to Forensic Science” is an online guide launched by the National Forensic Science Technology Center with funding from the Bureau of Justice Assistance. It is designed for nonscientists and covers the core concepts, capabilities and limitations of key forensic science disciplines. It is available at http://www.ncjrs.gov/bjareleases/sg2fs.html.

Digital Data Device Test Results


Mobile Acquisition Device Test Results

This series of reports presents test assertions, environments and results on various mobile data devices and other alternatives.

“Test Results for Mobile Device Acquisition Tool: Micro Systemation XRY v6.3.1” is available at https://ncjrs.gov/pdffiles1/nij/241151.pdf.


“Test Results for Mobile Device Acquisition Tool: Device Seizure v5.0 build 4582.15907” is available at https://ncjrs.gov/pdffiles1/nij/241153.pdf.

“Test Results for Mobile Device Acquisition Tool: Lantern v2.3” is available at https://ncjrs.gov/pdffiles1/nij/241154.pdf.