

their number might permit the common area to be searched.

An officer can also rely on the consent of one who seems authorized to give consent, regardless of whether or not that person has the actual authority to grant consent. The Supreme Court set forth an objective standard: would all of the facts available to the officer at that moment warrant a man of reasonable caution in the belief that the consenting party had authority over the object of the search. *Illinois v. Rodriguez*, 497 U.S. 177 (1990). In other words, if a police officer, taking all of the circumstances available to him at the time, could reasonably believe that the person granting consent had mutual use or control for most purposes over the object of the search, he may rely on that consent. If the police officer received consent to search a house from a woman who claimed to live there and who also produced a key, it would likely be reasonable for the police to rely on her consent. The analysis becomes trickier, however, when the object to be searched is a computer or other digital device.

The Fourth Amendment is implicated only when there is a governmental intrusion that infringes on an individual's legitimate expectation of privacy. *United States v. Jacobsen*, 466 U.S. 109 (1984). In *Katz v. United States*, 389 U.S. 347 (1967) the Supreme Court adopted a two part test to determine whether the person's expectation of privacy is legitimate: first, the person must hold an actual, subjective expectation of privacy, and next, society must be prepared to recognize that expectation as objectively reasonable.

The inquiry whether the owner of a footlocker, suitcase, etc. has a subjective expectation of privacy in the contents located therein typically hinges on whether such container is locked. *Andrus*, 483 F.3d 711 (10th Cir. 2007) (citing *United States v. Block*, 590 F.2d 535 (4th Cir. 2001)). In *Block*, the Fourth Circuit held that although a mother could consent to a search of her son's room in the house that they shared, this consent did not extend to a locked foot-

locker since the lock indicated that the son did in fact hold a subjective expectation of privacy.

Some courts considering the issue of third party apparent authority to search computers have analogized computers to other types of containers, likening them to suitcases or briefcases. *United States v. Andrus*, 483 F.3d 711 (10th Cir.2007); *Trulock v. Freeh*, 275 F.3d 391 (4th Cir. 2001). An analysis of Fourth Amendment issues regarding computers must necessarily be more nuanced than when considering the search of an ordinary box, due to the nature of computers and the locks used to secure their contents.

It is not always readily apparent whether the owner of a computer has indicated a subjective expectation of privacy in his or her computer. The Court in *Andrus* recognized this challenge:

Unlike footlockers or suitcases, where the presence of a locking device is generally apparent by looking at the item, a "lock" on the data within a computer is not apparent from a visual inspection of the outside of a computer, especially when the computer is in the "off" position prior to the search. Data on an entire computer may be protected by a password, with the password functioning as a lock, or there may be multiple users of a computer, each of whom has an individual and personalized password-protected "user profile.

In *Trulock*, 275 F.3d 391 (4th Cir. 2001) the Court was faced with the issue as to whether the search of *Trulock's* password-protected computer files was valid under the Fourth Amendment. *Trulock's* housemate consented to the search of the computer which she shared with *Trulock*, but informed police that each of them maintained separate, password-protected files on the hard drive, and that they did not know each other's passwords and therefore were unable to access each other's files. The Court compared *Trulock's* password-protected

files to a locked footlocker, finding that by using a password he affirmatively intended to exclude his house-mate and others from his personal files. No one but Trulock possessed actual authority to consent to the search of these files because no one else shared joint access or control over these files. The steps Trulock took to insure his files were inaccessible to his housemate (the creation of a password which he did not reveal) evidenced that he did not assume the risk the files could be subjected to a search authorized by another. Thus, Trulock had a reasonable expectation of privacy in the password-protected computer files and his housemate's authority did not extend to them. The Court was not faced with the issue of apparent authority, in that the housemate informed the police that she did not know Trulock's password.

The issue as to the validity of third party consent to search a computer can be further complicated when police conduct the search using forensic software or other technological tools that can bypass the passwords put in place by the subject of the search – passwords which presumably indicate a subjective expectation of privacy in the contents of the computer. What if the police receive consent to search a computer from a third party and that person does not reveal that the computer is password protected? Perhaps the person granting consent does not even realize that passwords are in place. These were the facts in *United States v. Buckner*, 473 F.3d 551 (4th Cir. 2007) in which the Fourth Circuit upheld the validity of consent given by the defendant's wife. She told officers she used the computer only occasionally to play solitaire, but did not mention that her husband put a password in place which was necessary to access his files. After shutting down the computer, officers mirrored the hard drive and conducted a forensic analysis of the copy using software that did not reveal the presence of a password. The court considered the totality of the circumstances available to the officer at the time of the search and concluded it was reasonable for the police to think the wife possessed the requi-

site authority to consent to the search. The court noted that the computer was located in a common area and was turned on even though the husband was not home. In dicta, the Buckner court said that they were not holding that officers can rely on apparent authority to search while using technology to intentionally avoid the discovery of passwords put in place by the user. But what does this really mean? Are there certain facts that must be present in order for a court to decide that officers were utilizing forensic tools or software to avoid the discovery of passwords? This also begs the question as to whether digital locks on computers in the form of passwords are somehow inferior to a physical lock. Are passwords somehow incapable of conveying a subjective expectation of privacy merely because they are not apparent from a visual inspection of the outside of the computer?

In *Andrus*, the Tenth Circuit noted that an officer who is presented with ambiguous facts relating to authority has a duty to investigate further before relying on consent. In *Andrus* the defendant's ninety-one year old father owned the house in which the defendant lived. He also paid the ISP bill. There was one computer in the house which was located in the son's room, but the father said he felt he was free to enter the room if the door was open. Together with the fact that the father did not say or do anything to indicate his lack of control over the computer at the time he was asked to give consent, the court found that the officers could have reasonably believed that the defendant's father had mutual use or control over the computer and therefore possessed the actual authority to consent to the search. As a result, the police were under no duty to ask clarifying questions – even though it would not have been a hardship for them to do so.

In *Andrus*, the forensic examiner used EnCase software to make a mirror image of the hard drive. The software not only bypassed the login password but did not reveal that such a password was in place. In essence, the court treated the lock in the

form of the password as non-existent because the police didn't see it (in that they did not turn on the computer) nor did they ask about its presence. In addressing the practice, the Andrus court did note that the practice "may well be subject to question" if it is shown that there is a "high incidence of password protection" among home computer users.

It is understandable that one doing a forensic examination would not want to turn on a computer that is the target of the search - time and date stamps are altered, and booby traps could initiate a wiping process. These are just a couple of concerns. Assume, though, that police wanted to search the son's room in the house that Andrus, Sr. owned? After obtaining consent from Andrus, Sr. police attempted to enter the room but discovered that the door was locked. At this point, the police would presumably ask Andrus, Sr. if he had a key to his son's room. If the answer was "No," the police could not rely on his consent to conduct a search, since it would be obvious that he lacked the authority to give consent.

Is the use of forensic software that not only bypasses digital locks, but also does not even recognize their existence, analogous to using an x-ray device to look through a door without first attempting to turn the doorknob to see if it is locked - or to scanning a box without first seeing if it is protected by a lock?

In *Kyllo v. United States*, 533 U.S. 27 (2001), the Supreme Court held that the Fourth Amendment doesn't allow the government to ignore the walls of a home simply because the police have new technology that uses thermal imaging to perceive activities behind those walls. Should the Fourth Amendment allow the government to ignore computer locks in the form of passwords because the government has the technology to bypass them?

The validity of relying on third party apparent authority to search a computer seems to turn on what one could reasonably believe at the time con-

sent was granted (even if it means ignoring other facts that could potentially have a bearing on the authority of the consentor.) There are at least a couple of very simple practices that the police could employ that could help mitigate some of the problems arising from consent to search based on apparent third party authority. First, the police could simply ask the person granting consent general questions regarding his use of the computer, including whether he knew if the computer was password protected and if so, did he know the password? Another practice that the police could adopt would be to configure the forensic software to check for the presence of passwords. For example, EnCase, one of the premier tools used by law enforcement and forensic examiners, is highly configurable by users and provides users with the ability to easily check for digital locks manually. Both of these low-tech practices could go a long way to ease the ambiguities in third party consent searches of computers as they could reveal not only the presence of a subjective expectation of privacy but perhaps a lack of authority to consent, as well.

¹Priscilla Adams is Senior Research Counsel at the National Center for Justice and the Rule of Law.

ATTORNEYS GENERAL FIGHTING CYBERCRIME

MULTI-STATE

Forty-three Attorneys General entered into a settlement with Craigslist, which posts ads for everything from apartment rentals to jobs, under which the company agreed to crack down on ads for prostitution on its web sites. According to the agreement, anyone who posts an ad for "erotic services" will be required to provide a working phone number and pay a fee with a valid credit card. If subpoenaed, Craigslist will provide that information to law enforcement. The company also agreed to sue 14

software and Internet companies that help people post erotic service ads to circumvent the site's protections against inappropriate content and illegal activity. Craigslist will also start using new search technology in an effort to help law enforcement find missing children and trafficking victims. Attorneys General from the following states and jurisdictions signed the agreement: Arizona, Arkansas, Colorado, Connecticut, Delaware, District of Columbia, Georgia, Guam, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Mississippi, Montana, Nebraska, Nevada, New Hampshire, New Mexico, New Jersey, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virgin Islands, Virginia, Washington, West Virginia, Wisconsin and Wyoming. The National Center for Missing and Exploited Children also joined the agreement.

.....

ARIZONA

Attorney General Terry Goddard discussed Internet safety with 200 eighth graders and their teachers at a state middle school. Attorney General Goddard talked about precautions children should take when visiting chat rooms, gaming and social networking sites. The presentation included interactive videos on Internet safety developed by Netsmartz and the National Center for Missing and Exploited Children.

.....

FLORIDA

Attorney General Bill McCollum's CyberCrime Unit investigators arrested Michael Weber on charges of possession of child pornography after discovering his large collection of child pornography images during an online investigation. Investigators traced the images back to Weber's computer and took him into custody with assistance from the U.S. Immigration and Customs Enforcement and the Hillsborough County Sheriff's Office. A search warrant was then executed on Weber's home, where a

computer was examined and seized. Weber will also be charged with promoting the sexual performance of a minor.

.....

HAWAII

Attorney General Mark Bennett announced that Craig Whang, a former investigator for the Honolulu Department of the Prosecuting Attorney, was sentenced on two counts each of Theft in the Second Degree and Unauthorized Computer Access in the First Degree. In the computer access cases, Whang used an Internet company locator service, which he charged to the Department, to locate people to serve subpoenas for a private business. Theft in the Second Degree is a class C felony, punishable by up to five years imprisonment and/or a fine of up to \$10,000. Unauthorized Computer Access in the First Degree is a class B felony, punishable by up to 10 years imprisonment and/or a fine of up to \$25,000. Attorney General Bennett's prosecutors recommended to the court that Whang be sentenced to five years probation, with special conditions including one year imprisonment and a \$20,000 fine.

.....

ILLINOIS

Attorney General Lisa Madigan filed a lawsuit against Wholesale Buying Group, an online auto wholesale company, for allegedly failing to deliver the vehicles that consumers purchased through its web site. According to the complaint, the company advertises that if consumers select a vehicle and make an upfront payment, the company will purchase the car at auction and add a \$700 fee to the wholesale price to cover their expenses. However, the company failed to carry out their part of the bargain and deliver the cars. The lawsuit asks the court for a permanent injunction prohibiting the company and its president, Christopher Sweis, from offering, brokering or selling automobiles. It also asks the court to order the company to pay restitution to consumers, a \$50,000 civil penalty, an additional \$50,000 penalty for each violation of the Consumer

Fraud Act and all fees associated with the investigation and prosecution of the case.

.....
KENTUCKY

Attorney General Jack Conway and his Office of Special Prosecutions announced that Kevin Cain pled guilty to use of electronic means to induce a minor to engage in sexual activity and to possession of material portraying a sexual performance by a minor. The victim's father learned of Cain's inappropriate conversations and attempts to meet with his daughter by using a program called Spector to monitor her online activities. The father notified State Police which joined with the Bowling Green Police Department to obtain a warrant and search Cain's residence and computers. The charges are Class D felonies and a sex offense, carrying up to five years in prison, a minimum \$1,000 fine and registry as a sex offender.

.....
LOUISIANA

Attorney General Buddy Caldwell will speak during a video news package on the potential dangers children face when using computers during the holidays. The package will also include sound bites from Col. Mike Edmonson, head of the State Police, and Mike Johnson, head of the High Tech Crime Unit in Attorney General Caldwell's Office. The package will focus on the partnership between law enforcement agencies to address Internet crimes against children. It will be available on an FTP site, DVD or mini DVD.

.....
MASSACHUSETTS

Attorney General Martha Coakley announced that Kenneth Conti of Rhode Island, formerly of Massachusetts, pled guilty to one count of Possession of Child Pornography. Conti was sentenced to one year in the House of Correction with 149 days credit for time served, with the balance suspended for a probation period of three years. During his probation,

Conti must register as a sex offender, cannot have contact with anyone under the age of 16 and cannot use the Internet. He also cannot loiter or remain within 1,000 feet of a school, playground or other location where children congregate. Conti must also wear an electronic bracelet and will be monitored by GPS. Attorney General Coakley's Office began an investigation of Conti after being contacted by his former employer. They found that Conti had images of child pornography on USB drives and in binders at his work cubicle. Conti was arrested at his parents' house in Rhode Island by the Johnston Police Department and transported back to Massachusetts by State Troopers assigned to Attorney General Coakley's Office. The case was prosecuted by Assistant Attorney General Christopher Kelly of Attorney General Coakley's Cyber Crime Division and was investigated by State Police assigned to Attorney General Coakley's Office.

.....
NEBRASKA

Attorney General Jon Bruning joined the Entertainment Software Rating Board (ESRB), which assigns ratings for computer and video games, in announcing a Public Service Announcement (PSA) campaign to educate state parents about the rating system. In the TV and radio spots, Attorney General Bruning urges parents to check the rating symbol when buying or renting a game to ensure its suitability. The PSAs are being delivered to radio and TV stations and local cable TV operators and can also be viewed on ESRB's web site, http://www.esrb.org/about/media_library.jsp. ESRB also prepared a brochure of additional information about the rating system, which can be downloaded from the "Kids and Parents" section on Attorney General Bruning's web site at <http://www.ago.ne.gov>.

.....
NEVADA

Attorney General Catherine Cortez Masto's Office joined the Federal Trade Commission in charging 10 related Internet payday lenders and their

principals, based mainly in the United Kingdom, with violating federal and state law by not disclosing key loan terms to U.S. consumers and using deceptive and abusive collection tactics. The corporate defendants are Cash Today, Ltd.; The Heathmill Village, Ltd.; Leads Global, Inc.; Waterfront Investments, Inc.; ACH Cash, Inc.; HBS Services, Inc.; Lotus Leads, Inc.; First4Leads, Inc.; Rovinge International, Inc.; and The Harris Holdings, Ltd., each also doing business as Cash Today; Route 66 Funding; Global Financial Services International, Ltd.; Interim Cash, Ltd.; and BIG-INT, Ltd. According to the complaint, the defendants, through web sites such as <http://www.cash2today4u.com>, offered consumers loans of up to \$500 within 24 hours without requiring a credit check, proof of income or documentation. Consumers were required to submit an online application with their bank account and Social Security number. Representatives then told them they qualified for a loan, with a fee of up to \$80, to be repaid by the next payday. If not, the loan would be automatically extended for an extra fee to be debited from the consumer's bank account. The payday lenders refused to disclose key loan terms in writing. After repaying the loan, sometimes with fees in excess of the original amount, many consumers terminated access to their bank accounts and received abusive and deceptive collection calls.

.....

NEW HAMPSHIRE

Attorney General Kelly Ayotte joined representatives of Comcast to kick off a year-long Internet safety public education campaign. The campaign includes both Public Service Announcements (PSAs) featuring Attorney General Ayotte and complementary educational videos that are available On Demand for Comcast's digital cable customers. The PSAs are set to run on more than 40 cable TV networks carried by Comcast in the state.

.....

NEW JERSEY

Attorney General Anne Milgram joined Criminal Justice Director Deborah Gramiccioni in announcing that Luis Torres pled guilty and was sentenced to three years in prison for distributing child pornography on the Internet. He is also barred from using any computer with Internet access during his prison term. Torres was among more than three dozen people arrested as part of "Operation Silent Shield," an investigation that targeted offenders who distributed known images and videos of child pornography via the Internet. Torres admitted that he knowingly used Internet file sharing software to make multiple files containing child pornography readily available for any user to download. A search warrant executed by the State Police revealed evidence of child pornography on Torres' computer. The Digital Technology Investigation Unit of the State Police coordinated the investigation, and Deputy Attorney General Lee Schwartz represented Attorney General Milgram's Division of Criminal Justice at the sentencing hearing.

.....

NEW MEXICO

Attorney General Gary King announced that Steven Teague, a repeat offender who pled guilty to two counts each of manufacturing child pornography, possession of child pornography and attempted distribution of child pornography, was sentenced to eight years in prison. A search warrant uncovered Teague's computer and thumb drive containing thousands of sexually explicit images of children that were turned over to the National Center for Missing and Exploited Children. The sentencing culminated a multi-agency Internet Crimes Against Children (ICAC) Task Force effort. Attorney General King's ICAC Unit led the investigation with assistance from ICE, the FBI and State Police.

.....
PENNSYLVANIA

Attorney General Tom Corbett's Child Predator Unit agents arrested Christopher Shugars, who is accused of using an Internet chat room to sexually proposition what he believed was a 13-year-old girl, but was actually an undercover Unit agent using the online profile of a child. The Penn Township Police Department assisted in the arrest. Shugars is charged with one count of unlawful contact with a minor and one count of criminal use of a computer, both third-degree felonies each punishable by up to seven years in prison and \$15,000 fines.

.....
SOUTH CAROLINA

Attorney General Henry McMaster announced that Gregory Ethridge was arrested in an undercover Internet sting conducted by the City of Greenville Police Department, a member of Attorney General McMaster's Internet Crimes Against Children (ICAC) Task Force. Ethridge was charged with two counts of Criminal Solicitation of a Minor, a felony offense punishable by up to 10 years imprisonment on each count and one count of Attempted Criminal Sexual Conduct with a Minor, a felony offense punishable by up to 20 years imprisonment. Arrest warrants allege that Ethridge solicited sex on the Internet from an individual he believed to be a 13-year-old girl, but was actually an undercover police officer. Ethridge was arrested when he arrived at a predetermined meeting place to see the "girl." The Lexington County Sheriff's Office, also a Task Force member, assisted with the execution of a search warrant, resulting in the seizure of two computers and computer-related items.

.....
TEXAS

Attorney General Greg Abbott distributed thousands of special child identification software-enhanced flash drives to families attending the Houston Texans vs, Tennessee Titans game. The flash drives, which were developed by Family

Trusted Child ID and sponsored by the National Center for Missing and Exploited Children (NCMEC), allow parents to digitally store their children's recent photographs and other critical identifying information. That information is critical to law enforcement if a child goes missing. Each flash drive can store identifying information for up to 10 children. Funding for the drives was provided by Dell Inc., McAfee, AT&T and Microsoft Corp. through donations to NCMEC.

.....
VIRGINIA

Attorney General Bob McDonnell filed a petition of certiorari to the U.S. Supreme Court, appealing a ruling by the state Supreme Court that invalidated the state's anti-spam law. The case is Virginia v. Jaynes in which the law was struck down because it could be unconstitutional in hypothetical circumstances involving political or religious speech that were not present in the case. Attorney General McDonnell's petition asserts that the court was wrong to completely invalidate the statute on hypothetical grounds. A decision on the petition is expected in early 2009.

.....
WASHINGTON

Attorney General Rob McKenna announced that Rommel Balingit was found to have violated the state's anti-phishing law by setting up a web site that was a mirror-image version of Russell Investment's web site. Russell, a global financial services company, alerted Attorney General McKenna's Office to the look-alike site. Balingit was ordered to pay a \$10,000 penalty under an agreement which provides for suspension of the penalty if he complies with the agreement's terms. The case was handled by Assistant Attorney General Katherine Tassi of Attorney General McKenna's Consumer Protection High-Tech Unit.

IN THE COURTS

ADMISSIBILITY: EXPERT TESTIMONY ON

ROLE-PLAYING

United States v. Joseph, 2008 WL 4137900 (2nd Cir. September 9, 2008). The 2nd Circuit Court of Appeals reversed a defendant's conviction for unlawful sexual activity based upon an improper jury charge but urged the lower court to revisit its ruling on the admissibility of expert testimony. Dennis Joseph was arrested and charged with soliciting sex over the Internet after arranging a meeting with law enforcement agents posing as 13-year-old girls. At trial in the U.S. District Court for the Southern District of New York, Joseph sought to introduce testimony from Dr. Joseph Herriot, an Associate Professor of Clinical Sexuality at the Institute of Advanced Sexuality, about role-playing in sexually explicit conversations on the Internet, but the court refused to admit the testimony. On appeal, the 2nd Circuit reversed, based on an improper jury charge, but also urged the trial court to reconsider its ruling on Dr. Herriot's testimony. The court found that Dr. Herriot's testimony would assist the jury, noting that many courts had upheld the admission of expert testimony to explain conduct not familiar to the average person. The court was not troubled that Dr. Herriot's testimony would rely on inadmissible hearsay about interviews and chat room conversations because under FRE 703, "...the facts or data need not be admissible for the opinion or inference to be admitted."

CHILD PORNOGRAPHY CHARGES:

DOUBLE JEOPARDY

United States v. Schales, 2008 U.S. App. LEXIS 21872 (9th Cir. October 20, 2008). Walter Schales was caught secretly placing a camera up a young girl's skirt and taking photographs. Pursuant to a warrant, police searched Schales' residence and found thousands of child pornography images on his

computer. A jury convicted him on three counts: Count 1 for receiving or distributing material involving the sexual exploitation of minors, Count 2 for possessing material involving the sexual exploitation of minors and Count 3 for receiving or producing a visual depiction of a minor engaging in sexually explicit conduct that is obscene. Schales appealed, claiming his 5th Amendment protection against double jeopardy had been violated because of his convictions under both Counts 1 and 2. The 9th Circuit Court of Appeals applied the Blockburger test (284 U.S. at 304) as follows: "Where the same act of transaction constitutes a violation of two distinct statutory provisions, the test to be applied to determine whether there are two offenses or only one is whether each provision requires proof of a fact which the other does not." So the court examined whether receipt of material involving sexual exploitation of minors requires proof of an additional fact which possession of material involving sexual exploitation of minors does not, and concluded it did not.

VIRGINIA SPAM STATUTE: FIRST AMENDMENT

Jaynes v. Commonwealth, 2008 WL 4181177 (Va. September 12, 2008). The Virginia Supreme Court reversed the conviction of a notorious spammer and also reversed its earlier decision in which a 4-3 majority had affirmed the spammer's conviction. Jeremy Jaynes was convicted under the state spam statute which criminalized using a computer network with the intent to forge routing information for the transmission of unsolicited bulk e-mail. Jaynes was sentenced to nine years imprisonment. On appeal, Jaynes' conviction was affirmed by the Virginia Court of Appeals and by a bare majority of the Supreme Court. Jaynes sought to argue that the statute was overbroad within the meaning of the First Amendment, but the court found he lacked standing to raise those arguments. On reconsideration, a unanimous court adopted Jaynes' argument that a state court has the discretion to allow more, but not fewer, challenges than would be allowed in federal court. The court then found that the statute was

substantially overbroad because it also punished a substantial amount of protected speech and was therefore unconstitutional.

SPAM BLOCKING: FIRST AMENDMENT RIGHT TO PETITION

Ferrone v. Onorato, 2008 WL 4763257 (3rd Cir. October 31, 2008). The Third Circuit Court of Appeals held that a claim for violation of the First Amendment right to petition requires a showing of actual intent to diminish the right. The Allegheny County (Pennsylvania) office of economic development was receiving a lot of e-mail from press@rock-port.com, and the county executive directed the IT staff to block all messages to his e-mail account from that address. Accidentally, the filter was set to block all messages being sent to any county account. When his messages stopped getting through, Rock Ferrone sued the county, claiming a violation of his First Amendment right to petition the government for a redress of grievances. The county moved for summary judgment, which the U.S. District Court for the Western District of Pennsylvania granted. Ferrone appealed, and the Third Circuit affirmed. Rejecting Ferrone's argument that the mere blocking of e-mails constituted a violation.

FOURTH AMENDMENT: HASH VALUE ANALYSIS

United States v. Crist, 2008 U.S. Dist. LEXIS 84980 (M.D. Pa. October 22, 2008). The U.S. District Court for the Middle District of Pennsylvania determined that running hash value sets without a warrant against seized files constituted a Fourth Amendment search. Robert Crist was in arrears on his rent, so his landlord hired two men to move his belongings to the curb. A friend of one of the movers took home Crist's computer, found videos seeming to depict underage sex and called police. Although Crist reported the computer stolen, the police took it to the Pennsylvania Attorney General's Office, where a special agent made an image of the

hard drive and reviewed its contents using Encase. Instead of directly examining the contents of the hard drive, the agent ran the imaged files through an MDS hash algorithm, producing hash values which he compared to hash values of known child pornography from the database maintained by the National Center for Missing and Exploited Children. He got five hits and 171 videos of suspected child pornography and ultimately found nearly 1,600 such images, all without a warrant. Crist was indicted for possession of child pornography and moved to suppress the evidence found on his computer, arguing that the agent's Encase examination constituted a search under the 4th Amendment. The government argued that it was not a search because the agent only ran hash values and did not "access" the computer. They also claimed that Crist had no 4th Amendment expectation of privacy because the mover's friend had already accessed the computer, viewed in their argument as a single container. The district court rejected the government's argument, finding that the further search of Crist's computer exceeded the scope of the private search by the mover's friend and violated the 4th Amendment.

LEGISLATIVE UPDATE

Copyright Infringement

TENNESSEE. ENACTED. On November 12, Tennessee Governor Phil Bredesen signed Senate Bill 3974 into law, which requires state public and private colleges and universities to take appropriate measures to ensure that computers connected to their network are not being used to illegally download and distribute material through P2P and file-sharing programs. Under the new law, they are required to implement technological support and develop and enforce a computer usage policy to effectively limit illegal downloads. The new law took effect upon signing.

Cyberbullying

TEXAS. INTRODUCED. On November 10, SB 29 was introduced, a bill that would require state public schools to extend their anti-bullying efforts to address students' threatening behavior committed online and on electronic devices. SB 29 would also require schools to institute anti-cyberbullying policies and would permit victims of cyberbullying to transfer to other classes or campuses.

Internet Safety

ENACTED. On December 2, S. 602, a bill requiring the Federal Communications Commission (FCC) to explore technologies that allow parents to censor their children's programming, became Public Law No. 110-452. The bill, sponsored by Senator Mark Pryor (D-AR), requires the FCC to report to Congress on its findings.

NEWS YOU CAN USE

PLAYING VIDEO GAMES LINKED TO VIOLENCE

Children and teenagers who play violent video games show increased aggression for months afterward, according to research published in the November issue of *Pediatrics*, the journal of the American Academy of Pediatrics. The research brings together three longitudinal studies, one from the U.S. and two from Japan, examining the content of games, how often they are played and aggressive behaviors later in the school year. The U.S. study, which focused on 364 children aged nine to 12 in Minnesota, showed an increased likelihood of getting into a fight at school or being identified by a teacher or peer as being physically aggressive five to six months later. The study noted that video games are played in 90 percent of American homes with children aged eight to 16, and the average playing time of four hours per week in the 1980s is now up to 13 hours per week, with boys averaging 16 to 18 hours per week. Researchers in all three studies

accounted for gender and previous aggressiveness. The Academy is revising its recommendations on media violence and now recognizes it as a significant health risk to children and adolescents.

FCC VOTES TO OPEN TV "WHITE SPACES" FOR BROADBAND

The Federal Trade Commission (FTC) voted to open the unused, unlicensed areas of the television airwaves known as "white spaces" for the use of wireless broadband services. The plan will take effect following the upcoming transition from analog to digital television broadcasting in February 2009, which will release additional wireless spectrum. The space could also be used for improved communications networks to connect emergency responders. Supporters claim the vacant spaces, which would be available for free, are well-suited to providing broadband since they can penetrate walls, carry a great deal of data and reach a wide geographic area. The vote is a victory for public interest groups and technology companies, but came over the objections of television broadcasters, which argued that using it could disrupt their over-the-air signals.

NUMBER AND POTENCY OF INTERNET ATTACKS RISING

A survey of 70 of the world's largest Internet operators found that malicious attacks are rising sharply and growing more powerful and sophisticated. According to the *Worldwide Infrastructure Security Report*, produced annually by Arbor Networks, a company providing tools for monitoring network performance. The report shows that the largest attacks have grown to over 40 gigabits in size, from less than one-half megabit, over the last seven years. Since the largest network connections available today carry 10 megabits of data, they can be overwhelmed by powerful attackers, according to the report, network operators say that the largest botnets continue to "outpace containment efforts and infrastructure investment." Despite the drastic increase in the number of attacks, the percentage re-

ported to law enforcement declined, with 58 percent of Internet service providers not referring any instances to law enforcement in the last 12 months. Of those, 29 percent said law enforcement had limited resources, 26 percent said they expected their customers to report illegal activities and 17 percent there was “little or no utility” in reporting them. The full report can be ordered for free at <http://www.arbornetworks.com/report>.

SPAM ECONOMICS: EVEN SMALL

RESPONSE = BIG PROFIT

Only one response for every 12.5 million spam e-mails can mean millions of dollars in profit to big spam operations, according to a study by computer scientists from the University of California, Berkeley and San Diego (UCSD). The team, led by Assistant Professor Stefan Savage of UCSD, infiltrated the Storm network that uses hijacked home computers as relays for junk mail and created several “proxy bots.” The team used these machines to control 75,869 hijacked machines and routed through them a fake spam campaign that lured users to buy an herbal remedy at a fake site. The researchers sent out 469 million junk e-mails, but only made 28 sales, so the response rate was less than .00001 percent. However, scaling this up to the full Storm network, the researchers estimated that the system is netting about \$7,000/day or more than \$2 million/year.

U.S. MILITARY LAUNCHES YOUTUBE SUBSTITUTE

Eighteen months after restricting access to YouTube and other video sites, the U.S. military launched a video-sharing web site for troops and their families. The site, TroopTube, allows people to register as members of an armed forces branch, family, Defense Department employee or supporter. Members can upload personal videos from anywhere with an Internet connection, although each is screened for taste, copyright violations and national security issues. The military was assisted by Seat-

le-based Delve Networks, which was responsible for building tools for approving and sorting incoming videos, “crunching” video files into different sizes and automatically playing the one best suited to the viewer’s Internet connection and ensuring that site searches produce the best video results.

COLLEGES MUST BE HIGH TECH TO COMPETE

Technology is a key factor influencing students in their college selection, according to a report by CDW Government, Inc., a seller of technology products, entitled “The 21st Century Campus: Are We There Yet?” The report findings were based on survey responses from more than 1,000 college students, faculty and IT staff. However, only one-third of faculty reported that technology was completely integrated at their schools. The report also found that while more than 80 percent of faculty teach some of their courses in “smart classrooms,” only 42 percent use technology during each class session. The number one item on students’ technology wish list is the ability to communicate online with their teachers, but only 23 percent of campuses offer this feature. The full report can be accessed at <http://newsroom.cdwg.com/features/feature-10-13-08.html>.

PATENT PROCESSING UP IN 2008

The U.S. Patent and Trademark Office (PTO) reported that patent processing increased by 14 percent in fiscal year 2008 compared with 2007’s increase of only 5.7 percent over the previous year. The PTO’s Performance and Accountability Report for fiscal year 2008, which ended on September 30, concluded that patent filing and processing trends continue an upward trend. Patent processing has jumped by 38.6 percent over the last four years, compared to a 21.3 percent increase in patent application filings during the same time period. There were 448,003 patent filings in 2008, with action taken on a patent application at an average of 25.6 months after filing. Patents were issued an average

of 32.3 months after filing. The full report can be accessed at <http://www.uspto.gov/web/offices/com/annual/2008/2008annualreport.pdf>.

ARMY REPORT FINDS TWITTER COULD BE TERRORIST TOOL

The U.S. Army released a draft intelligence paper on possible scenarios where terrorists could use new technology. Some of the technology cited was the use of GPS devices on phones for travel plans, surveillance and targeting; the use of mobile phone cameras as surveillance devices; and the use of voice changing technology to make phone calls. The paper said that Twitter, a popular real-time social messaging utility, could also be used as a terrorist tool, and the report imagines a "Red Team" scenario where terrorists send other terrorists Twitter messages as real time updates of an attack. The report warns that this scenario could allow terrorists to select the precise moment to set off a bomb based on the Twitter messages received. Further research is required to test whether the scenarios could play out. The report can be accessed at <http://www.fas.org/irp/eprint/mobile.pdf>.

DATABASE OF IP CASES YIELDS SURPRISES

Stanford Law School unveiled its Intellectual Property Litigation Clearinghouse, a searchable online database that tracks all patent cases since 2000. Offering such diverse statistics as trends, the number of suits filed and the decisions for plaintiffs before a particular judge, the database has also revealed some surprising facts. The database revealed that despite rumors of growing numbers of patent infringement suits, the actual number of suits has held steady to between 2,300 and 2,800 a year. It also showed that defendants in patent infringement cases win more in the courtroom than plaintiffs, 57 percent to 43 percent. The database is designed for non-commercial use, and registration can be accessed at <http://exmachina.stanford.edu/register/>.

CYBER SECURITY EDUCATION STUDY RELEASED

The National Cyber Security Alliance released the "2008 National Cyberethics, Cybersafety, Cybersecurity Baseline Study," which looks at the state of cyber security education in the K-12 range. Data was collected from 1,569 U.S. K-12 public and private educators and 94 technology coordinators in an online survey. In addition, 219 educators, local and state technology coordinators and state technology directors participated in focus groups. A key finding was that only eight percent of educators said their school included cyber security, safety and ethics as part of their curriculum or one-day assemblies. It also found that less than five percent of educators said that protecting, identifying and responding to identity theft, predators, bullying and other crimes is included in their curriculum. Also notable is that only 22 percent of teachers are comfortable teaching about these cyber crimes, and only 23 percent feel prepared to teach students how to protect their personal information online. The full study can be accessed at <http://staysafeonline.mediaroom.com/file.php/98/NationalC3BaselineSurvey111408Finalwforward+%283%29.pdf>.