



## Issue 123 August 2007

The URLs referenced in Bytes frequently link to newspapers and other current news sources. Be aware that these links may fail over time.

### FTC RECOMMENDS HANDS-OFF APPROACH TO NET NEUTRALITY

In a report issued on June 27, 2007, the Federal Trade Commission's (FTC) Internet Access Task Force cautioned policy makers about attempting to regulate the evolving, dynamic industry of broadband Internet access. The FTC warns that imposing one-size-fits-all restraints on a market as large and diverse as the Internet could have unpredictable, adverse effects on consumers. The FTC also suggests that current consumer protection laws are sufficient to combat deceptive marketing practices by Internet service providers and other online schemes threatening consumers. In addition to proposing policy recommendations, the 169 page report includes background information on the technical functioning of the Internet and the legal and regulatory developments that have led to the current debate over network neutrality regulation; provides an overview of the arguments for and against such regulation; analyzes the consumer welfare effects of certain potential conduct by broadband providers, including data discrimination and prioritization; explores the application of the antitrust and consumer protection laws to such conduct; and identifies various proposals for broadband Internet access that have been put forth to date. The full report may be found at <http://www.ftc.gov/reports/broadband/v070000report.pdf>

### CYBERBULLYING AFFECTS ONE-THIRD OF TEENS

According to a report issued June 27, 2007 by the Pew Internet & American Life Project, about one-third (32%) of teenagers who use the Internet say that they have been victims of so-called cyberbullying. The most common forms of bullying involved another person publicizing a private e-mail, instant message or text message. Other types of harassment included spreading rumors or posting an embarrassing photo on the web, as well as sending a threatening or aggressive e-mail, IM, or text message. Girls are more likely to be the targets of bullying than boys, with 38% of girls reporting that they have been harassed compared with 26% of boys. In addition, teens that frequently use social sites like MySpace and Facebook are 17% more likely to experience some form of cyberbullying. The report may be found at <http://www.pewinternet.org/pdfs/PIP%20Cyberbullying%20Memo.pdf>

### COURT OF APPEALS RELUCTANTLY OVERTURNS CHILD PORN CONVICTION

In a decision released on June 21, 2007, the Georgia Court of Appeals reluctantly reversed the conviction of a man for 106 counts of sexual exploitation of children because the prosecution did not prove that the defendant knew he had pornographic images stored on his computer's hard drive. Edward Ray Barton was charged with child molestation and possession of child pornography after his wife turned over his laptop to authorities during divorce proceedings. Barton was acquitted of the molestation charges but received a 20-year sentence for possession of the child pornography. At Barton's jury trial, the prosecution's computer forensic expert testified that all the images of child pornography on Barton's computer were stored in temporary Internet folders. Since the images were only stored in temporary files, the expert testified that Barton had viewed the files but did not save them to the hard drive and could not access the images without special software. Although the expert stated that images such as "pop-ups" are stored in temporary Internet files, he did not specify whether the images on Barton's computer constituted "pop-ups." Barton appealed, arguing that the state hadn't shown he knowingly possessed the images because he hadn't taken any affirmative action to store the photos on his computer, was unaware the computer had automatically saved the images, and had no ability to access the saved images. The court "reluctantly" agreed, concluding that merely proving a defendant has pornographic images stored in temporary files does not satisfy

the "knowingly possess" requirement of Georgia's sexual exploitation statute. The court ruled that, in addition to proving that Barton possessed pornographic images, the state must also show that Barton either took affirmative steps to save or download those images or had knowledge that the computer automatically saved the files. Further information is available at <http://www.law.com/jsp/article.jsp?id=1182848790153>

## **TORRENTSPY, RAM AND E-DISCOVERY DECISION**

On May 29, 2007, a ruling by a magistrate judge in the U.S. District Court for the Central District of California, holding that data residing temporarily in a computer's random access memory (RAM) is eligible for e-discovery, has sparked a huge debate over whether or not data that only exists temporarily in RAM should be considered "electronically stored information" under the amended Federal Rules of Civil Procedure. This extremely technical and complicated case began when the Motion Picture Association of America (MPAA) on behalf of Columbia Pictures brought a suit against Justin Bunnell, the founder of TorrentSpy, for copyright infringement. TorrentSpy is a search engine similar to YouTube that indexes and makes videos available for public download using the BitTorrent file-sharing protocol. Although TorrentSpy provides a search engine for downloading videos, the BitTorrent application assembles whole files from a variety of sources including all users of BitTorrent software and not directly from the TorrentSpy website. This means that MPAA cannot sue TorrentSpy directly because the allegedly infringed material is actually coming from individual consumers of BitTorrent and TorrentSpy, so instead the MPAA has accused TorrentSpy of contributory infringement. In order to prove its contributory claims against TorrentSpy, the MPAA would need evidence that users of TorrentSpy downloaded and shared copyrighted material. In an attempt to acquire this information, the MPAA served discovery requests on TorrentSpy asking the company to produce server log data such as the IP addresses of users who downloaded files, records of the requests for the files, as well as the dates and times of the requests. TorrentSpy, however, claimed that it did not log customers IP addresses and requests because it was contrary to its privacy policy. The information requested by the MPAA was only stored in the server's RAM which in the normal course of business is overwritten after approximately six hours.

This is where the debate over whether or not data temporarily stored in RAM is discoverable under the Federal Rules of Civil Procedure begins. Rule 34 provides that a party may request "electronically stored information . . . stored in any medium from which information can be obtained . . . and which are in possession, custody or control of the party" served. Since data is only temporarily retained in RAM, TorrentSpy claimed that it did not constitute electronically stored information as defined by the federal rules. Magistrate Judge Jacqueline Chooljian, who issued the opinion, disagreed with TorrentSpy's analysis, concluded that the company could have created a log of the requested information, and required TorrentSpy to preserve and produce the server logs. The magistrate's opinion emphasized that the ruling should not be read to require all litigants to preserve and produce data stored in RAM because this was a special case in which the relevant evidence could only be obtained from RAM. In addition, the magistrate ordered TorrentSpy to mask the IP addresses of its consumers to prevent the MPAA from bringing suits against individuals. In spite of Magistrate Chooljian's efforts to quell fears that her ruling would open the floodgates for discovery requests to produce data stored in RAM, groups such as the Electronic Frontier Foundation (EFF) and the Center for Democracy and Technology have joined the fight. These groups warn that the court's ruling could require Internet companies as well as other digital service providers such as digital telephone services to record and preserve massive amounts of consumer information. On June 8, 2007, in light of the controversy, Chooljian set aside her ruling to allow TorrentSpy to present its appeal. The appeal is scheduled to be heard on August 16, 2007 by Judge Florence-Marie Cooper. The EFF has filed an amicus curiae brief on behalf of TorrentSpy which may be found at [http://www.eff.org/legal/cases/torrentspy/EFF\\_CDT\\_amicus.pdf](http://www.eff.org/legal/cases/torrentspy/EFF_CDT_amicus.pdf)

## **FORMER DEFENDANT RETALIATES AGAINST RIAA'S LEGAL TACTICS**

On June 25, 2007, Tanya Andersen, who had been defending herself against an RIAA lawsuit for about two years, filed a complaint in U.S. District Court against the RIAA as well as several other defendants, including Atlantic Recording Corporation, Priority Records, Capitol Records, UMG Recordings, and BMG Music, MediaSentry, and Settlement Support Center. In her complaint, Andersen alleges that the RIAA conspired with the other defendants to pursue tens of thousands of

vicious and illegal lawsuits against private citizens, in many cases forcing defendants to settle claims rather than face years of litigation and considerable legal expenses. Andersen's suit focuses on the techniques used by the RIAA and MediaSentry to identify potential defendants. According to the complaint, MediaSentry poses as a peer user and then accesses individuals' computers gathering information about them including their IP addresses. MediaSentry then allegedly sells this information to the RIAA which it uses as the sole basis for filing lawsuits. A copy of Andersen's complaint may be found at [http://www.ilrweb.com/viewILRPDF.asp?filename=andersen\\_riaa\\_070622complaint](http://www.ilrweb.com/viewILRPDF.asp?filename=andersen_riaa_070622complaint)

## **FBI REPORTS THAT OVER 1 MILLION PEOPLE ARE VICTIMS OF BOTNETS**

On June 13, 2007, the FBI and the Department of Justice announced that over one million people might be victims of botnet cyber crime. A botnet is a collection of computers under the remote control of a bot-herder who uses his victims' computers to commit other crimes such as identity theft, denial of service attacks, phishing, click fraud, and the mass distribution of spam and spyware. Typically, owners of compromised computers have unintentionally allowed access to their computers and are usually unaware that they are victims of botnets. In order to combat botnet crime as well as spread public awareness about the threat posed by botnets, the FBI and the DOJ have teamed up with companies such as Microsoft and launched a cyber crime initiative called Operation Bot Roast. According to the FBI's press release, botnets are a growing threat to national security and the national infrastructure because of their wide variety of capabilities. In order to protect one's computer, the FBI suggests updating anti-virus software, installing a firewall, using strong passwords, and practicing good e-mail and web security habits. More cyber security tips may be found on the FBI's website at <http://www.fbi.gov> and the FBI's press release regarding botnet activity may be found at <http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm>

## **BEST BUY ATTORNEY ADMITS TO ALTERING DISCOVERY DOCUMENTS**

On June 4, 2007, law.com reported that a strange twist had occurred in a consumer class action suit against Best Buy involving its outside counsel. On May 24, 2007, Robins, Kaplan, Miller & Cerisi filed a motion to withdraw as Best Buy's counsel stating that one of the firm's partners, Timothy Block, had been placed on indefinite medical leave. The motion also explained that Block admitted to redacting and altering documents which he had produced to the plaintiffs for discovery. Furthermore, the motion stated that Block self-reported his actions to the Minnesota Board of Professional Responsibility. According to the report from law.com, the judge in the matter granted Best Buy a stay in order to resolve the issue. However, the plaintiffs' attorneys suspect that corporate officials are to blame for discovery problems as opposed to an isolated problem with one outside counsel. The class action suit, which was certified in December of 2005, claims that Best Buy and Microsoft collaborated in a deal in which both companies would promote the other's goods and services. As a part of this deal, Best Buy customers were given six month free trial CDs for MSN Internet services; however, when the six months expired, customers claim they were billed for the service without their consent. Further information may be found at <http://www.law.com/jsp/article.jsp?id=1180688739517>

## **NEW LAWYER RATING SITE HAS CRITICS**

On June 5, 2007, Avvo, Inc. launched its new website, [www.avvo.com](http://www.avvo.com), which purports to rate and profile every attorney in the United States so that consumers can choose the right lawyer. Avvo's website provides information on an attorney such as the attorney's Avvo Rating, disciplinary sanctions, and client ratings. According to the company's CEO, Mark Britton, the most critical piece of guidance the site provides is the Avvo Rating which is Avvo's assessment of how well a lawyer could represent a client. The rating is based on a proprietary mathematical model applied equally to each lawyer to analyze information Avvo has about them, including their experience, disciplinary sanctions and professional achievements. Britton claims that the Avvo Rating was developed with input from legal experts, hundreds of lawyers and thousands of consumers, and the information used to give each attorney their rating was found through state bar associations, court websites, and lawyer's websites. In addition, lawyers can go online and update their profile, and both lawyers and clients can comment and rate other lawyers. Although the company's goal is to rate every lawyer in the United States, currently the website only includes ratings and profiles on every

licensed attorney in Arizona, California, District of Columbia, Georgia, Illinois, New York, Ohio, Pennsylvania, Texas and Washington. More states are added on a regular basis. Critics have pointed out that Avvo's website is riddled with bizarre errors, profiles of attorneys who have been dead for more than a century such as Abraham Lincoln and Clarence Darrow, as well as inexplicable scores in which some felons received better ratings than law school deans and internationally renowned litigators. On June 14, 2007, only nine days after the launch of the rating site, two Seattle lawyers filed a class action suit against Avvo. The complaint claims the Avvo's rating are misleading and unreliable; however, Avvo defends its right to free speech and reiterates that its ratings are merely the opinions of Avvo and its consumers. More information about Avvo's site may be found at <http://www.avvo.com>

### **GLOBAL ONLINE PEDOPHILE RING BUSTED**

On June 18, 2007, London police announced that they had infiltrated and dismantled a global Internet pedophile ring, rescuing 31 children and rounding up more than 700 suspects worldwide. According to the Child Exploitation and Online Protection (CEOP) Centre, the 10 month long investigation involved authorities from over 35 countries. The ring was traced to an Internet chat room called "Kids the Light of Our Lives" that featured images of children being subjected to horrific sexual abuse. The host of the website, Timothy David Martyn Cox, 27, of Buxhall, who used the online identity "Son of God," admitted to nine counts of possessing and distributing indecent images. After his arrest in September, authorities were able to infiltrate the chat room and collect evidence on the other members. More information regarding the investigation may be found at [http://www.ceop.gov.uk/news\\_items/article\\_20070618\\_ceop.htm](http://www.ceop.gov.uk/news_items/article_20070618_ceop.htm)

### **NEW STUDY RANKS INTERNET COMPANIES' PRIVACY AWARENESS**

On June 9, 2007, Privacy International, a watchdog group concerned with how online search engines handle users' personal information, released a report ranking major online companies' privacy practices. The study focused on 23 companies including Google, Yahoo, Facebook, Amazon, and BBC. The report was compiled using data derived from public sources (newspaper articles, blog entries, submissions to government inquiries, privacy policies, etc), information provided by present and former company staff, technical analysis and interviews with company representatives. Using this information, Privacy International analyzed specific areas of the companies' privacy practices such as data collection and processing, data retention, transparency, responsiveness, and ethical compass. After gauging all the categories, a company was then given one out of six possible rankings from highest to lowest: privacy-friendly and privacy enhancing, generally privacy aware but in need of improvement, generally aware of privacy rights but demonstrates noticeable lapses, serious lapses in privacy practices, substantial and comprehensive privacy threats, and comprehensive consumer surveillance and entrenched hostility to privacy. One of the study's more interesting and controversial findings was its ranking of Google at the lowest possible level of comprehensive consumer surveillance and entrenched hostility to privacy. In defending its finding, Privacy International stated that an independent European panel recently opened an inquiry into whether Google's policies abide by Europe's privacy rules and that U.S. groups such as the Electronic Privacy Information Center have filed complaints with the Federal Trade Commission over the possible Google/DoubleClick merger. Google says it stockpiles data to help its search engine better understand its users so it can deliver more relevant results and advertisements. Privacy International is particularly troubled by Google's ability to match data gathered by its search engine with information collected from other services such as e-mail, instant messaging and maps. Privacy International said it reached its initial findings after spending the last six months reviewing Internet privacy practices with the help of about 30 professors, mostly in the U.S. and Britain. An updated report will be released in September. Seven of the Internet companies and websites included in the report received the second-lowest grade of substantial and comprehensive privacy threats including Time Warner Inc.'s AOL, Apple Inc., Facebook.com, Hi5.com, Reunion.com, Microsoft's Windows Live Space and Yahoo. No company or site received Privacy International's top grade, but five rated as generally privacy-aware. They were BBC, EBay Inc., Last.fm, LiveJournal.com and Wikipedia.com. Privacy International's report may be found at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-553961](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-553961)

### **MICROSOFT RESEARCH DEAL OVER NEW VISTA OPERATING SYSTEM**

On June 19, 2007, the Department of Justice (DOJ) announced that Microsoft had agreed to revise its operating system. Microsoft's concession came after Google filed a complaint alleging that it and other competitors were unfairly disadvantaged by how Microsoft designed the feature for conducting computer-desktop searches. In particular, Google said that it was difficult to turn off the Microsoft desktop search and that Google's desktop search ran too slowly when users chose it as an alternate. Though Microsoft executives denied those accusations, the company said it would make several changes in its desktop search. The feature, which is separate from Internet search, allows users to scan information on computer hard drives. These revisions are to be included in a forthcoming service pack provided to users so they can update their operating system. The service pack should be distributed in late 2007, but Microsoft could not yet say when it would become available to the public. The DOJ's press release may be found at [http://www.usdoj.gov/opa/pr/2007/June/07\\_at\\_437.html](http://www.usdoj.gov/opa/pr/2007/June/07_at_437.html)

### **COURT DISMISSES WIRETAPPING SUIT AGAINST THE NSA**

On July 6, 2007, a U.S. appeals court ordered that a lawsuit against the National Security Agency (NSA) for a wiretapping program be dismissed because the plaintiffs had not been hurt by the agency's actions. A divided three-judge panel for the U.S. Court of Appeals for the Sixth Circuit ruled that the lawsuit, brought by the American Civil Liberties Union (ACLU) and a group of journalists, lawyers, and academics, be sent back to a district court judge to be dismissed. In August 2006, Judge Anna Diggs Taylor of the U.S. District Court for the Eastern District of Michigan ruled the NSA program, which monitored telephone and Internet communications without court-ordered warrants, was illegal. The appeals court ruled that the plaintiffs did not prove that they had been affected by the NSA's Terrorist Surveillance Program, authorized by President George Bush in 2002. The program allowed the NSA to monitor communications between U.S. residents and people in other countries with suspected ties to the terrorist group al Qaeda. The plaintiffs argued, among other things, that the program violated the U.S. Constitution's Fourth Amendment, protecting U.S. citizens against unreasonable search and seizure. The court felt, however, that none of the plaintiffs could prove their Fourth Amendment rights had been violated. In a dissenting opinion, Judge Ronald Lee Gilman concluded that the plaintiffs were entitled to sue because they felt a need to alter their communications after the program was disclosed. Although the Sixth Circuit's decision has thwarted the ACLU's attack on the NSA program, two other lawsuits challenging the NSA's practices are pending before the Ninth Circuit. The suits include Al-Haramain Islamic Foundation, Inc. v. Bush, in which the plaintiffs, an Oregon branch of a Saudi charity that has been investigated for alleged terrorist ties and others, contend that they have a document proving they were a direct target of NSA surveillance. The other case, Hepting v. AT&T Corp., has been brought on behalf of a group of AT&T customers who allege that the company intercepted their phone calls and e-mails and disclosed them to the NSA. The Sixth Circuit full opinion may be found at <http://www.ca6.uscourts.gov/opinions.pdf/07a0253p-06.pdf>

### **COURT RULING PROTECTS CONSUMER WEBSITE FROM LAWSUIT**

On June 26, 2007, the Second Circuit Court of Appeals issued an opinion preventing a New York-based moving company from suing an Iowa resident for operating a website that posted critical reviews of the companies' performance. The court concluded that under New York's long-arm statute, the court did not have personal jurisdiction over the defendant because he had not "transacted business" in New York. Defendant Timothy Walker operates MovingScam.com, a website that provides consumer-related feedback regarding moving companies. In August of 2003, Walker posted comments asserting that the plaintiff, Best Van Lines, was operating without legal authorization and insurance. The company sued in the Southern District of New York asking the court to enjoin Walker from posting any further defamatory statements and to order him to pay compensatory and punitive damages totaling \$1.5 million. When the trial court dismissed the case for lack of personal jurisdiction, the plaintiff appealed. While the appeals court explained that this was the first time a New York appellate court had addressed a case of website defamation under the "transacting business" clause of New York's long-arm statute, the court deferred to the federal district courts which had tackled the issue. According to the opinion, the lower courts have concluded that the posting of defamatory material on a website accessible in New York does not, without more, constitute "transacting business" in such a way that would allow a New York plaintiff to sue an out-of-state defendant in a New York federal court. The court noted that Walker's

comments were directed at a national audience and not specifically at New York residents, further supporting their decision that New York could not exercise jurisdiction. The court's full opinion may be found at [http://www.ca2.uscourts.gov:8080/isyssnative/RDpcT3BpbnNcT1BOXDA0LTM5MjQtY3Zfb3BuLnBkZg==/04-3924-cv\\_opn.pdf](http://www.ca2.uscourts.gov:8080/isyssnative/RDpcT3BpbnNcT1BOXDA0LTM5MjQtY3Zfb3BuLnBkZg==/04-3924-cv_opn.pdf)

## **SEDONA CONFERENCE PUBLISHES ITS SECOND EDITION ADDRESSING ELECTRONIC DISCOVERY**

On July 7, 2007, The Sedona Conference, a nonpartisan law and policy think tank, announced publication of "The Sedona Principles, Second Edition, Best Practices Recommendations and Principles for Addressing Electronic Document Production." The Sedona Conference's first edition was extremely successful and widely influential with the courts. The Sedona Principles have been cited in many precedential cases involving electronic discovery issues. The second edition has been released to coincide and provide helpful and timely guidance for issues that have emerged since the implementation of the 2006 amended Federal Rules of Civil Procedure. While the 14 fundamental principles remain relatively unchanged, the language has been updated to accommodate the language of the 2006 amendments and the comments under each of the principles have been significantly updated to reflect the new rules, a wave of recent court decisions, advances in electronic discovery technology, and a deeper appreciation among judges and lawyers for the unique qualities of electronically stored information. The Sedona Principles, Second Edition is free for download and may be found at [http://www.thesedonaconference.org/content/miscFiles/TSC\\_PRINCP\\_2nd\\_ed\\_607.pdf](http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ed_607.pdf)

## **NEW ELECTRONIC EVIDENCE PRACTICE GUIDE DIRECTED AT POLICE**

On July 6, 2007, the Association of Chief Police Officers (ACPO) of England, Wales and Northern Ireland released a new guide for collecting electronic evidence. The ACPO teamed up with 7Safe, a private information security-consulting firm, to create a guide that reflects the latest developments in computer forensic investigation techniques. The "Good Practice Guide for Computer-Based Electronic Evidence" was launched at the ACPO e-crime conference, which explored the rapidly changing nature of policing cyber-crime as well as ways that government, industry and law enforcement can work together better to combat the use of the Internet to commit or facilitate crime. While the guide is targeted at law enforcement in the United Kingdom, the guide may still provide background information useful to any professionals dealing with computer forensics. The guide is free and may be found at [http://www.7safe.com/electronic%5Fevidence/ACPO\\_guidelines\\_computer\\_evidence.pdf](http://www.7safe.com/electronic%5Fevidence/ACPO_guidelines_computer_evidence.pdf)

## **VISTA'S DATA RETENTION CAPABILITIES HIGHLIGHTED**

In an article published in the July 2007 issue of the American Bar Association Journal, author Jason Krause cautions that Microsoft's new operating system Vista might retain more discoverable data than lawyers and their clients realize. Since Vista has new features and tools to prevent data loss and allow users easy access to stored information, the system keeps much more detailed user records that may prove useful as evidence in litigation. For technical expertise on this issue, Krause interviewed Sensei Enterprise's Vice President, John Simek. Simek explained that Vista not only creates a shadow copy of a user's work making it easier for a computer forensic experts to retrieve deleted files, but it also creates an index of practically everything a user has worked on providing an already indexed database of evidence for an opposing party to discover. For the first time, computer forensic technologists may be able to determine not only the date on which a file was last accessed, but ALL the dates on which it was accessed. Simek also pointed out that Vista offers an interesting new feature for high-end versions: bitlocker encryption. Bitlocker allows users to lock data so that only those with a decryption key can unlock and access the data. The full ABA article may be found at [http://www.abajournal.com/magazine/a\\_lot\\_of\\_room\\_in\\_its\\_view/](http://www.abajournal.com/magazine/a_lot_of_room_in_its_view/)

## **NO PROGRESS IN NET RADIO'S FIGHT AGAINST ROYALTY HIKES**

On July 11, 2007, a federal appeals court denied a petition by webcasters to delay the onset of new royalty fees that they argue could cripple their ability to offer their services to consumers. In a one-

page order, the U.S. Court of Appeals for the District of Columbia said the opponents of the fees had not satisfied the stringent standards required for a stay pending court review and rejected their request for an emergency stay. On July 13, 2007 SoundExchange, the nonprofit entity that collects the fees, announced in a press release that it offered to cap the \$500 per channel minimum fee at \$50,000 per year. However, this glimmer of reconciliation between the webcasters and the music industry was short lived. On July 18, 2007, the Digital Music Association (DiMA), the group that represents larger webcasters such as Live365 and Pandora, announced that it and SoundExchange were at an impasse regarding the proposed terms of the cap. While the debate over fees continues with no real progress, July 15th, the day webcasters claimed would be the Armageddon of Internet radio, has come and passed with most net radio streams still streaming. Press releases from SoundExchange and the DiMA may be found respectively at <http://www.soundexchange.com> and <http://www.digmedia.org/content/mediacenter.cfm?content=pr>

## **NEW SITE TO PUBLICLY AUCTION SOFTWARE VULNERABILITIES**

On July 9, 2007, a Swiss Internet company launched WabiSabiLabi.com which is an online auction house where software vulnerabilities are sold to the highest bidder. Several established vulnerability management companies already purchase information about software flaws from researchers, but the terms of those deals are private and generally set by the companies. Executives at WabiSabiLabi claim that their approach to auctioning vulnerabilities ensures that researchers receive the fair market value for the work they put into finding the flaws. However, security experts warn that the site could allow cyber criminals to pose as legitimate companies and purchase these vulnerabilities. Vulnerabilities that could be sold on the site range from those present in hardware that supports critical information infrastructure -- such as Internet routers -- to flaws in common desktop applications, such as Web browsers, instant messenger and e-mail programs. In many cases, criminals could exploit the flaws, gain control over home computers or business networks, and gain access to sensitive information. The company, though, claims to thoroughly screen all potential sellers and buyers, requiring proof of identification, articles of incorporation, and even bank account information from all parties involved. The company's press release announcing the launch of its service may be found at <http://www.wslabi.com/wabisabilabi/news.do?>

## **BURGLARS USE GOOGLE TO CRACK A SAFE**

On July 11, 2007, Colorado Springs news station KKTV reported that two burglars had used Google to look up how to open a safe while in the process of committing a burglary. In a bizarre crime that actually occurred on June 11, 2007, the two burglars, who have yet to be caught, broke into a large amusement center and stole cash, a laptop, and a PlayStation 3 game console worth a total of \$12,000. Even though they had the pass code needed to get into the company's main office and the combination to the safe, the two men still couldn't open it up. Not to be dissuaded, the men found a computer that had been left on and simply Googled for information on how to break into the safe. Believing that the burglary was an inside job, police withheld video surveillance that has now been released to KKTV in hopes of finding a new lead in the case. Although the circumstances of this crime may seem uncommon, businesses should still be aware of how leaving their computers on or unlocked could create an opportunity that even a novice criminal could exploit. The news story and clips of the video surveillance may be found at <http://www.kktv.com/crimestoppers/headlines/8381222.html>

## **DEA USES KEY LOGGER SOFTWARE TO GATHER EVIDENCE**

On July 6, 2007, the Ninth Circuit Court of Appeals issued an opinion that primarily dealt with Internet surveillance but hinted at more pervasive surveillance techniques used by the Drug Enforcement Agency (DEA). The DEA began investigating defendants Mark Forrester and Dennis Alba for manufacturing MDMA or Ecstasy. In May 2001, the DEA began its electronic surveillance of the defendants' e-mail and Internet activity after obtaining court permission to install a pen register analogue or wiretap on Alba's computer. The initial pen register only recorded IP addresses of visited websites and the To/From addresses of e-mail messages. However, the defendants were using encrypted e-mail services such as Hushmail.com that prevented the DEA from obtaining the desired information. The DEA then persuaded a judge to allow an agent to enter the defendants' office and install keystroke-logging software, allowing the DEA to monitor all activity on the

defendants' computers. Surprisingly, the defendants did not move to suppress any evidence obtained as a result of the key logger at trial and instead focused on the validity of the initial pen register. The court determined that the pen register used to monitor the defendants' Internet and e-mail activity did not violate the Fourth Amendment because the defendants had no reasonable expectation that the IP addresses and the To/From lines of e-mails would remain private since such activity is transmitted through a third party. Both Forrester and Alba were sentenced to 30 years in prison on charges including conspiracy to manufacture and distribute Ecstasy. The court's full opinion may be found at

[http://www.ca9.uscourts.gov/ca9/newopinions.nsf/F0E09BB37A97D51A88257310004D1DAC/\\$file/0550410.pdf?openelement](http://www.ca9.uscourts.gov/ca9/newopinions.nsf/F0E09BB37A97D51A88257310004D1DAC/$file/0550410.pdf?openelement)

## **1ST AMENDMENT DOES NOT PROTECT VIOLENT INSTANT MESSAGES**

On July 5, 2007, the Second Circuit Court of Appeals held that a student's First Amendment right to free speech was not violated when he was suspended for sending an instant message containing a violent image and calling for his teacher's death. In April of 2001, Aaron Wisniewski, an eighth-grader, used his parents' computer to send 15 friends an icon containing a small drawing of a pistol firing a bullet at a person's head and blood splattering. Beneath the icon were the words "Kill Mr. VanderMolen," a reference to Aaron's English teacher, Philip VanderMolen. Although the exchange took place off-campus, a classmate of Aaron's told VanderMolen about it, and Aaron was suspended for five days. Even though Aaron expressed regret and said it was meant as a joke, the School Board later decided to suspend Aaron for one semester and granted the teacher's request that he no longer teach Aaron. Because of the controversy, Aaron and his family eventually moved out of town. His parents decided to file suit in the Northern District of New York under 42 U.S.C. §1983, claiming the icon was protected speech because it was not a true threat. They said the board retaliated against their son for exercising his First Amendment rights. They also charged a failure by the board and school superintendent to train school staff in threat assessment and alleged violations of New York State Education Law. The trial court and the court of appeals, however, disagreed and dismissed the Wisniewski's suit. The court concluded that the school could suppress speech that would materially and substantially disrupt the work and discipline of the school; in addition, the court noted that off-campus conduct could create a foreseeable disruption on-campus allowing the school to discipline off-campus speech as well. The court's ruling not only gives school officials broader authority to sanction student speech, but it also clarifies that there does not have to be a true threat for schools to impose discipline. The court's full opinion may be found at

[http://www.ca2.uscourts.gov:8080/isysnative/RDpcT3BpbnNcT1BOXDA2LTMzOTQtY3Zfb3BuLnBkZg==/06-3394-cv\\_opn.pdf](http://www.ca2.uscourts.gov:8080/isysnative/RDpcT3BpbnNcT1BOXDA2LTMzOTQtY3Zfb3BuLnBkZg==/06-3394-cv_opn.pdf)

## **COURT IMPOSES SPOILIATION SANCTIONS ON GOVERNMENT**

On June 27, 2007, the U.S. Court of Federal Claims imposed sanctions against the United States for, what it called, the government's "reckless disregard" of its duty to preserve relevant evidence. The case involved a breach of contract claim by United Medical Supply Co., Inc. United Medical claimed that the United States government ordered medical supplies from other suppliers after entering into a requirements contract with United Medical. During the course of discovery, the government failed to properly inform the medical treatment facilities, which should have ordered supplies from United Medical under the contract, to retain records that would be relevant to the litigation. Due to this failure, many of the medical treatment facilities destroyed records that should have been retained. In addition, the government assured the court that it was doing everything in its power to make sure that the records were being located and produced. The court determined that the government's actions required the imposition of sanctions. The court said that the defendant would be prohibited from cross-examining the plaintiff's expert to the extent that the expert construes, to plaintiffs' favor, the gaps in the record created by defendant's spoliation and from adducing its own expert testimony construing the same gaps. Furthermore, the court ruled that defendant must reimburse plaintiff for any additional discovery-related costs, including attorney's fees, that were incurred because of defendant's malfeasance and misrepresentations, as well as all the costs, including attorney's fees, that were incurred in specifically pursuing the spoliation matter. The courts full opinion may be found at

[http://www.klgates.com/files/upload/eDAT\\_Westlaw\\_Document\\_United\\_Med\\_Supply.doc](http://www.klgates.com/files/upload/eDAT_Westlaw_Document_United_Med_Supply.doc)

## **REPORT: 90 PERCENT OF COMPANIES FAIL TO COMPLY WITH DATA HANDLING REGULATIONS**

On July 18, 2007, the IT Policy Compliance Group published a report concluding that 90 percent of all businesses still do not have sufficient policies in place to meet government regulations and adequately protect against a data breach. In the survey of 475 companies, the study found that an overwhelming majority of the firms expect to deal with at least six business disruptions a year related to major data incidents along with five or more instances of information loss or theft. In addition to gauging what percentage of companies remain at risk for a data breach, the survey also attempted to measure the impact of such an event on the average company. Based on its respondents' replies, businesses that are forced to report major incidents publicly can expect to experience an eight percent loss of their stock price and an equal eight percent of their customers. Companies can also expect to report an eight percent falloff in their quarterly revenue along with additional costs for litigation, customer notification, and subsequent settlements averaging \$100 per each record they lose. The report concludes that larger companies are more likely to have incidents, based on its research. Organizations with less than 1,000 workers average roughly eight percent in revenue and customer losses per event, whereas companies with more than 100,000 employees can expect to lose 12 percent of their sales and clientele. Unsurprisingly, the report also finds that companies that allocate the highest budgets for compliance automation technologies are faring better in their efforts than those who spend less on the issue. The full report may be found at [http://www.itpolicycompliance.com/images/uploaded/why\\_compliance\\_pays.pdf](http://www.itpolicycompliance.com/images/uploaded/why_compliance_pays.pdf)

## **ORGANIZED CRIME RECRUITS IT WORKERS**

On July 23, 2007, a new report was published by Actimize, an antifraud software maker, claiming that IT workers are being trained and recruited by organized crime to steal the information they are employed to protect. The report was based on interviews with 40 large financial services companies in the United States and the United Kingdom. According to the report, about 50 percent of those surveyed indicated they believed that they have employed workers who have either been trained or recruited by outsiders to carry out fraud. Eighty-five percent of the respondents also said they had been affected by employee fraud. More than 50 percent of participating companies admitted that only half, or less, of all employee fraud was currently being caught. Among the factors contributing to the criminal trend are increased access to technology by rank-and-file employees as well as poor hiring and screening processes within firms. Data availability and a lack of dedicated resources for fraud detection technologies were other issues identified by respondents as fueling internal attacks. More than 75 percent of companies surveyed said that they expect insider fraud schemes to grow even more sophisticated. In addition, about half of the companies involved in the research said that they have experienced a data theft within the last 12 months. The types of scams reported by participants included self-dealing, skimming, data-theft, embezzlement and collusion. While data-handling regulations such as the Sarbanes-Oxley Act and the Payment Card Industry (PCI) compliance requirement were designed to help combat insider fraud, those surveyed said that is not necessarily the case. An overwhelming 70 percent of respondents said that government regulation or standards regarding employee access to customer accounts and data would actually hinder their company's ability to detect or prevent employee fraud. As with many other types of IT issues, the shortfall in more comprehensive insider fraud protection can be tied largely to a lack of sufficient budgeting for tools to prevent fraud. Actimize's summary of the survey may found at <http://www.actimize.com/index.aspx?page=news80>

---

"*Bytes in Brief*"<sup>®</sup> is a FREE monthly digest of Internet law and technology news delivered to you by e-mail. For members of the legal and business community interested in Internet law and technology developments, "*Bytes in Brief*" provides a synopsis of related news and links to sources with more expanded coverage. In the time it takes to drink a cup of coffee, "*Bytes in Brief*" is designed to make sure you are tracking major developments in this fast moving area.

If staying current in this field is important to you and you find yourself buried under unread magazines, newspapers and journals, "*Bytes in Brief*" can help you stay in touch without a major

outlay of time or expense.

To subscribe, [click here](#) and enter your real name, company name, and e-mail address.

---

Copyright © 2008 Sensei Enterprises, Inc. All rights reserved.