

{bytes in brief}

LAW AND TECHNOLOGY NEWS MONTHLY

EDITORS: Sharon D. Nelson, Esq. and John W. Simek
ASSOCIATE EDITOR: Nicole Kolinski EDITOR EMERITUS: G. V. Nelson



© 2009 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

Issue 142 - March 2009

PLEASE NOTE: The URLs referenced in Bytes frequently link to newspapers and other current news sources. These links may fail over time.

COURT HOLDS THAT ACCESSING FORMER EMPLOYER'S E-MAIL MAY VIOLATE STORED COMMUNICATIONS ACT

On October 10th, 2008, U.S. District Court for the Middle District of Tennessee granted partial summary judgment on a claim arising under the Stored Communications Act (SCA). The case involved a nuclear pharmacy that sued two former employees for allegedly accessing their work e-mails after they were no longer employed. One employee obtained his replacement's e-mail logon information, logged into the account and forwarded the e-mails to the other employee. The court found that the accessing employee had violated the SCA by accessing the employers' e-mail knowingly and willfully, although the computer evidence showing his access was destroyed. The SCA provides a private right of action against a person who "intentionally accesses without authorization a facility through which an electronic communication service is provided." Under this language, the court held that the employee violated the SCA as a matter of law. A post on the decision in *Cardinal Health 414 v. Daniel Adams et al.*, may be found at http://www.ibls.com/internet_law_news_portal_view.aspx?s=articles&id=DDCF8FF7-35AD-4D5F-A09C-134D85F0CAFB (free subscription required)

CONGRESS DELAYS DIGITAL TV TRANSITION UNTIL JUNE, STRUGGLES REMAIN

On February 4th, the U.S. House of Representatives approved a bill to delay the digital TV transition until June 12th. The Senate approved the bill the week before, but the House initially voted it down. Concern that many TV viewers would be left in the dark caused the House to reconsider - as many as 6.5 million U.S. households were expected to be unprepared for the transition. The digital TV transition requires television broadcasters to turn off analog signals and only broadcast digital signals. Households with analog televisions and antennas have two options: upgrade to a digital TV, or install a converter box. On February 5th, the Federal Communications Commission held an open meeting on how the delayed transition would work. Chairman Michael Copps said that the agency would carefully evaluate which stations could turn off their analog signals before the June 12th deadline. The major broadcast networks including ABC, CBS, Fox, and NBC/Telemundo agreed that their owned and operated stations would remain in an analog signal until the deadline. 421 smaller stations made the transition early on February 17th, causing more than 28,000 phone calls to the FCC transition hotline. The FCC approved most of the applications to make the switch early, but denied about 43 applications to ensure that at least one analog station remained for news and public safety information. Many stations that made the switch early will continue to air an analog signal with instructions on how to make the transition. A story on the Congressional action may be found at

http://www.informationweek.com/news/personal_tech/TV_theater/showArticle.jhtml?articleID=213001981&subSection=News

The FCC information on the open meeting may be found at <http://www.fcc.gov/realaudio/presentations/2009/020509/Welcome.html>

A news story on the stations that transitioned early may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2009/02/18/AR2009021803131.html>

AMOUNT OF SPAM RISES 150% IN TWO MONTHS

On January 27th, the Times in London reported that spam was on the rise since the November shutdown of McColo, one of the largest spam server farms in history. Unfortunately, spammers have regrouped and almost reached the spam levels that existed before the McColo shutdown. In 2008, the average user not protected by anti-virus software would have received 45,000 spam messages, up from 36,000 in years past. On the highest spam e-mail day last year, users received an average of 100 spam e-mails per minute. The problem perpetuates because spam servers are difficult to shut down. According to Google's data, the amount of spam is supposed to increase drastically this year, especially as spammers discover new resources and new ways to dupe computer users. The story may be found at http://technology.timesonline.co.uk/tol/news/tech_and_web/article5598661.ece

REPORT SAYS CLICK FRAUD HIT RECORD HIGH

On January 28th, Click Forensics, a firm that specializes in monitoring Internet crime, released a report stating that 17 percent of all clickthroughs on Web advertising are a result of click fraud, the highest rate the company has seen since 2006. "Click fraud" is the act of clicking on an Internet ad to artificially increase its clickthrough rate. Examples of malicious click fraud are competitors clicking on rivals' ads to increase the rivals' advertising costs, or a website clicking on its own advertisements to increase its ad revenue. Click fraud also includes non-malicious activity that leads to a click of no value to the advertiser, for example when someone clicks an ad twice by mistake. The report further found that 31.4 percent of click fraud is coming from automated bots and botnets, a 14 percent increase from last quarter and the highest recorded rate. Click Forensics stated that the increase may be due to the poor economy, which has spurred a rise in other cybercrime. Google is highly affected by click fraud, as it generates most of its revenue from pay per click advertisements. Google was quick to dismiss the report, stating that Click Forensics's estimates of click fraud never matched its own. Google maintained that its click fraud rate is less than 10 percent. The Click Forensics press release may be found at <http://clickforensics.com/newsroom/press-releases/120-click-fraud-index.html>

A news story on Google's reaction may be found at http://www.pcworld.com/article/158570/google_dismisses_click_fraud_report.html?tk=rss_news

GOOGLE TO HELP DISCOVER INTERNET BLOCKERS

On January 28th, Google introduced Measurement Lab, a new tool to help researchers determine whether ISPs are inappropriately blocking or slowing Internet traffic. Through Measurement Lab, Google will provide researchers with 36 servers in 12 locations in the United States and Europe to analyze data. The purpose of the project is to alleviate some of the problems researchers were having in uncovering blocking, to keep users informed, and to promote net neutrality. The development is timely considering a recent FCC decision to uphold a complaint against Comcast for slowing traffic in violation of the FCC's open source policy. The Google blog post may be found at <http://googleblog.blogspot.com/2009/01/introducing-measurement-lab.html>

HEARTLAND SUED OVER DATA BREACH, 3 ARRESTS MADE

On January 27th, a lawsuit was filed against Heartland Payment Systems in U.S. District Court for the District of New Jersey, in regards to a data breach announced by the company on Inauguration Day. The suit seeks class action status, but was filed on behalf of Alicia Cooper, who was notified by her credit union that one of her credit cards was included in the breach. In the complaint, Heartland is accused of failing to adequately safeguard data, not notifying consumers of the breach in a timely manner, and not offering to compensate consumers for losses stemming from the breach. It also alleges that Heartland was negligent in taking more than two months to determine the existence and scope of the breach and for failing to identify affected merchants. On February 10th, police in Florida arrested three suspects allegedly using credit card numbers stolen from Heartland. The police said

that the three men who were arrested had been using the stolen numbers on Visa gift cards to purchase goods at Wal-Mart, and then sold the goods for cash. It was unclear whether the three men played a role in breaking into Heartland's system. The complaint may be found at <http://chimicles.com/assets/1--Heartland%20Complaint%20-%201.27.09%20-%20final%20for%20filing.pdf>

The police announcement of the arrests may be found at <http://lcs.leonfl.org/news/021109CreditCardArrest.pdf>

STUDY FINDS CYBERCRIME MORE COSTLY THAN EVER

On January 29th, McAfee released a new report entitled "Unsecured Economies: Protecting Vital Information," which estimated the cost of cybercrime to be \$1 trillion globally. The report made the prediction based on responses to a survey of more than 800 chief information officers in the U.S., United Kingdom, Germany, Japan, China, India, Brazil and Dubai. The responses indicated that they lost data worth \$4.6 billion and spent \$600 million cleaning up after the breaches. Respondents also indicated that the recession increases the security risk, with 42 percent stating that displaced workers were the biggest threat to sensitive information. The report indicated a global divide, as 25 percent of respondents said they would not store data in China, but 47 percent of respondents in China said they believed the U.S. posed the biggest security threat. The report (registration required) may be found at <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>

VETERANS AFFAIRS TO PAY \$20 MILLION FOR DATA BREACH

On January 27th, the U.S. Department for Veterans Affairs ended nearly three years of litigation over a potential data breach by agreeing to pay \$20 million to veterans. The data breach occurred in 2006 when a VA data analyst lost a laptop containing the names, birthdays, and social security numbers of up to 26.5 million veterans and active duty troops. The laptop was recovered and no data was compromised, but the VA inspector general stated that veterans were exposed to unreasonable risk. The employee promptly notified his supervisors but veterans were not told of the breach for three weeks. The proposed settlement will allow veterans who show harm from the data theft to recover between \$75 and \$1,500. If any money is left after making the payments, it will be donated to veterans' charities. On February 10th, U.S. District Judge James Robertson approved the settlement, making it final. The story may be found at <http://www.nytimes.com/2009/01/28/washington/28vets.html>

GOOGLE SEARCHES LEAD TO MURDER CONVICTION

On January 23rd, a Florida Appeals Court affirmed the conviction of a man for the murder of his wife - the evidence included his Google searches before the murder. On August 17, 2002, April Barber was murdered while walking along a deserted beach with her husband, Justin. Justin was shot four times - in his left hand, left shoulder, base of his neck, and his chest - but did not die. April's family was convinced that Justin murdered her and shot himself to cover up the crime, as a \$2 million life insurance policy had been taken out on both parties, Justin was in debt of over \$50,000, and he was having affairs. Justin was prosecuted for the murder, and the police introduced evidence of his Google searches, which included "trauma, cases, gunshot, right chest" and "Florida & divorce." Justin was convicted by a jury and was sentenced to life in prison. He appealed his conviction claiming it was based on circumstantial evidence. An appeals court affirmed, finding sufficient evidence. Justin's case is one in a line of cases where Google searches have linked to the crime. The story may be found at http://news.cnet.com/8301-13578_3-10150669-38.html

USER DATA STOLEN FROM MONSTER.COM

On January 23rd, Monster.com announced that its database that stores user information including usernames, passwords, e-mail addresses, names, phone numbers, and some demographic data was illegally accessed. The accessed information did not include sensitive information such as social security numbers, financial data, or

resumes. But the information that was stolen could be used to contact Monster users and trick them into giving up sensitive information. Monster recommended that users visit its website and change their password, and reminded users that it does not send unsolicited e-mails asking users to confirm a username and password. The website also offers other security tips. The Monster announcement may be found at <http://help.monster.com/besafe/jobseeker/index.asp>

MAN BUYS MP3 PLAYER WITH U.S. TROOP DATA

On January 26th, news site TVNZ reported that a New Zealand man who bought a used MP3 player from an Oklahoma thrift store found troop data on the device. There were over 60 files on the device which included names, cell phone numbers, and Social Security numbers of U.S. troops, lists of soldiers based in Afghanistan, personnel who fought in Iraq, equipment deployments, and private information such as which soldiers were pregnant. The files were marked with a warning saying access was prohibited by federal law. Most of the files were dated 2005 and were unlikely to compromise any national security information, but could put individual soldiers at risk. The story may be found at <http://tvnz.co.nz/view/page/413551/2453415>

FBI BACKLOGGED IN CHILD PORN CASES

On January 23rd, the *Associated Press* reported that the Federal Bureau of Investigation was encountering a backlog in its computer labs due to an increase in child pornography cases. The information came from a Justice Department Inspector General audit of the FBI's efforts to combat child exploitation. The number of child pornography cases increased twenty-fold between 1996 and 2007. The increase caused an average backlog of about two months to process evidence from such crimes, and could take as long as nine months. The FBI built a new computer lab in Maryland to deal with the increased demand, and may need to hire more staff to help process electronic evidence in child pornography cases and other computer crime cases. The story may be found at <http://www.iht.com/articles/ap/2009/01/23/america/FBI-Child-Porn.php>

The Inspector General report may be found at <http://www.usdoj.gov/oig/reports/FBI/a0908/final.pdf>

CA COURT AFFIRMS PROTECTIVE ORDER PROHIBITING PEDOPHILE FROM PHOTOGRAPHING CHILDREN

On January 15th, the California Court of Appeals for the Second District upheld a restraining order and permanent injunction against Scott McClellan, who operated a website that posted pictures of young girls taken in public places. The website also ranked public places based on the number of three to eleven year old girls present there, in what was called the "girl love" ranking. Parents of children posted on the website filed suit, asking for a permanent injunction preventing McClellan from posting pictures of any young children on his website. The trial judge granted the injunction, which said McClellan must stay more than 10 yards away from areas where children congregate, and that McClellan cannot record or publish any image of a young child without the parents' consent. McClellan represented himself in the action, and claimed that the injunction violated his free speech rights under the California Constitution. The court of appeals disagreed and upheld the injunction, saying that McClellan was presenting the children in a light that would indicate they are available to pedophiles. Not surprisingly, the court determined that this did not interfere with his free speech rights. The story may be found at http://news.cnet.com/8301-13578_3-10149724-38.html

GOOGLE LATITUDE LETS YOU KNOW WHERE FRIENDS ARE – AT ALL TIMES

On February 4th, Google unveiled its new feature for Google Maps called Google Latitude, which allows you to see where your friends are at all times. The feature is available on a mobile phone, and on the computer through iGoogle. Once users opt in, they can share their location with whomever they want, and see the location of friends

who decided to share with them. In addition to seeing the friend's location, users can also communicate through SMS, Google Talk, or Gmail. Google stated in its blog that it recognized the sensitivity of location information, and enacted safeguards to deal with the privacy issues. The safeguard is that everything about Latitude is opt-in, as you control who sees your data and what they see. But watchdog group Privacy International claimed to identify a flaw in the security the day after Latitude's release. As an example, a second user could enable Latitude on a phone without the primary user's knowledge, and see the location of that person's friends. The Google blog post may be found at <http://googleblog.blogspot.com/2009/02/see-where-your-friends-are-with-google.html>

The Privacy International story may be found at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-563567](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-563567)

CLONED DEBIT CARDS USED TO WITHDRAW MONEY FROM ATMS

On February 4th, the *Chicago Tribune* reported that the Federal Bureau of Investigation was looking for two suspects who used cloned debit cards in a complicated international scheme. The cards were created by hacking into the computers of RBS World Pay, a firm that processes financial transactions. RBS World Pay announced a data breach before Christmas that compromised 1.5 million cardholders' information and 1.1 million Social Security Numbers. The hackers used the information to clone debit cards and somehow distributed the cards to people all over the world. The FBI stated that people made thousands of withdrawals over ten hours starting November 8th. The FBI stated that the two suspects were likely low-level participants, but hopefully could lead to the heads of the hacker crime ring. The story may be found at <http://www.chicagotribune.com/news/local/chi-atm-fraudfeb04,0,7303260.story>

LAWYERS WARNED ABOUT E-MAIL SCAMS

On January 26th, *Texas Lawyer* reported the story of a Houston lawyer who was scammed out of \$182,500 by a client who contacted him through e-mail. The lawyer, Richard T. Howell, Jr., is speaking out about the incident to prevent other lawyers from falling into the same trap. Howell apparently was a victim of a complicated check fraud scheme, which stemmed from collections work Howell did for a client, allegedly from Japan. Howell's law firm sued Citibank after the scam was revealed for clearing a bogus check from the client in the amount of \$367,000. The firm then sent \$182,500 to a supplier of the Japanese company in Hong Kong, which could not be rescinded when Sterling Bank notified the firm that the \$367,000 check was a fraud. Howell tried to e-mail the client but was unsuccessful. Experts say that Howell has little hope in getting his money back, which he paid to the firm himself for his mistake. The story may be found at <http://www.law.com/jsp/article.jsp?id=1202427717175>

SECURITY RESEARCHER CLONES DHS PASSPORTS & DRIVERS LICENSES

On February 2nd, news sources reported that security researcher Chris Paget cloned Department of Homeland Security issued passports using a \$250 RFID scanner purchased on eBay and an antenna hidden in his car. The security weaknesses of the EPC Gen 2 RFID tags include the lack of encryption and true authentication. These tags are being used in new passport cards offered by the DHS as part of its Western Hemisphere Travel Initiative and enhanced drivers' licenses (EDLs). The cards are supposed to encourage travel to and from Western Hemisphere countries by offering a way to speed up and simplify the border-crossing process. Paget's hack took place from twenty feet away as he was driving his car at 30 miles per hour – unlike previous RFID hacks that took place within inches of the card. Paget planned to present his research at a conference in Washington, D.C. in the beginning of February. The story may be found at http://www.theregister.co.uk/2009/02/02/low_cost_rfid_cloner/

911 FRAUD CAUSES SWAT TEAMS TO BE DEPLOYED

On February 2nd, the *Associated Press* reported a new type of telephone fraud that exploits a weakness in the 911

call system. The story described the plight of a couple in Southern California who was ordered out of their home at 10pm by an armed SWAT team of police officers. The source of the call was eighteen-year-old Randal Ellis in Mukilteo, Washington. Ellis was on the phone for 27 minutes telling the police that he was high on drugs and shot his sister. Ellis was able to make it seem like he was inside the Bateses' home by entering bogus information about his location. Similar cases have occurred throughout the country. Some cases have been successfully prosecuted and some have not. Prosecutors were hoping that long prison terms would deter such "swatters," as they are a strain on already tight emergency dispatch resources. The story may be found at http://tech.yahoo.com/news/ap/20090202/ap_on_hi_te/tec911_swatting

MICROSOFT SUES FORMER EMPLOYEE FOR SPYING

On January 22nd, Microsoft sued former employee Miki Mullor for applying for a job under false pretenses and using his job at Microsoft to access confidential information for use in a patent litigation. Mullor allegedly downloaded confidential files onto his company issued laptop, which had to do with the patent litigation, but nothing to do with Mullor's job. Microsoft hired Mullor in November 2005, and fired him in September 2008. On his application, Mullor stated that he worked for Ancora Technologies, but that the company went out of business. Microsoft alleges that this was false, as Ancora was still in business and Mullor was its chief executive officer. Mullor stated that the lawsuit was in retaliation for Ancora's patent suit and nothing more. The story may be found at http://seattlepi.nwsource.com/business/398089_msftsuit30.html

CHILD PORN INDICTMENT REINSTATED DESPITE EVIDENCE ISSUES

On February 12th, the Tennessee Court of Criminal Appeals reinstated the indictment in a child pornography case, despite finding that the county prosecutor was wrong for refusing to turn over evidence. In the case against Re'Licka Dajuan Allen, the prosecutor failed to turn over the mirror image of the hard drive at issue, though the Tennessee Court of Criminal Appeals had held in another case that defense counsel was entitled to the evidence. The trial court dismissed the case after the prosecutor refused to turn over the evidence, but the appeals court held that was not the proper punishment for the prosecution. One judge dissented, finding that the state's refusal to turn over the evidence created the problem that led to the trial judge withholding the evidence. The majority opinion may be found at <http://web.knoxnews.com/pdf/021709porn-allenmajority.pdf>

The dissenting opinion may be found at <http://web.knoxnews.com/pdf/021709porn-allendissent.pdf>

COURT ORDERS MULTIPLE SANCTIONS FOR BAD FAITH DESTRUCTION OF EVIDENCE

On January 26th, the U.S. District Court for the Southern District of New York imposed severe sanctions in the case of *Arista Records v. Usenet.com*, for Defendants' bad faith destruction of evidence. In this case, Plaintiffs alleged that Defendants provided subscribers access to music piracy "newsgroups," which contained Plaintiffs copyrighted files. Plaintiffs issued multiple discovery requests, including requests for usage data and digital music files. Plaintiffs claimed that Defendants deliberately spoliated evidence by failing to preserve the usage data and manipulated their server to prevent the storage of digital music files. Defendants later produced some information from re-enabled music groups after the server was shut down. Defendants claimed that the lost data was due to the automatic operation of their system. The court found that Defendants' duty to preserve arose no later than when Plaintiffs issued their discovery requests. The court also found that Defendants' failure to preserve was in bad faith, as Defendants claimed they could not produce the information due to the nature of their server but later produced some of the same information. Since the data was extremely relevant to Plaintiffs' claims, sanctions were warranted. The court ordered that an adverse inference instruction be imposed against Defendants at trial, precluded Defendants from challenging Plaintiffs' statistical evidence and awarded Plaintiffs' attorneys' fees and costs. The decision may be found at http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_Arista.doc

APPLE: JAILBREAKING IPHONE = COPYRIGHT VIOLATION

On December 2nd, the Electronic Frontier Foundation (EFF) filed a request with the U.S. Copyright office requesting a Digital Millennium Copyright Act (DMCA) exception for those who have chosen to bypass the restriction Apple places on the iPhone, which only allows installation of applications from the Apple App Store. The EFF claims that this action, termed "jailbreaking," is protected under fair-use doctrines and that tinkering with technology is an important part of our innovation economy. Apple's response filed with the Copyright Office stated that the act of jailbreaking the iPhone itself results in copyright infringement, as they use unauthorized modifications to the copyrighted operating system. Apple also argued that jailbreaking is not innovative at all, as most users do not jailbreak their iPhones themselves, but use software created by other parties. The EFF exemption request may be found at http://www.eff.org/files/filenode/dmca_2009/RM2008-08.phoneunlocking.exhibits.pdf

Apple's response may be found at <http://www.copyright.gov/1201/2008/responses/apple-inc-31.pdf>

FTC ANNOUNCES NEW WEB-AD POLICY, PRIVACY GROUPS CHALLENGE IT

On February 12th, the Federal Trade Commission (FTC) announced its revised principles for online behavioral advertising. The principles push for better self-regulation for behavioral ads. The four principles are that websites should: 1) give consumers an accessible way to opt out, 2) maintain reasonable security and retention practices for collected data, 3) inform consumers of material changes, and 4) receive express consent before collecting sensitive data. Privacy advocates immediately attacked the principles, saying that they were unlikely to result in significant changes in online data tracking. The privacy groups said that the FTC punted on the issue of sensitive data, and also criticized the failure to mention children who are vulnerable to online predatory practices. The FTC press release may be found at <http://www.ftc.gov/opa/2009/02/behavad.shtm>

A news story on privacy group reactions may be found at http://news.cnet.com/8301-13578_3-10163062-38.html

GOOGLE WINS STREET VIEW PRIVACY SUIT

On February 17th, the U.S. District Court for the Western District of Pennsylvania dismissed a lawsuit against Google by a couple claiming that Street View on Google Maps is a reckless invasion of their privacy. The couple claimed in their lawsuit that Street View images of their home taken from their private road significantly disregarded their privacy interests. The court disagreed, and found that the couple failed to state a claim on any of its five counts against Google. Ironically, the couple exposed itself to the public more by filing the lawsuit than the Google Street View had, as the lawsuit included their home address, and investigations revealed that pictures of their home were previously posted on a Pennsylvania County website. A copy of the dismissal may be found at http://i.i.com.com/cnwk.1d/i/ne/pg/fd_2009/boringvgoogledismissal.pdf

FACEBOOK FACES SCANDAL OVER TERMS OF SERVICE

In early February, Facebook updated its terms of service, causing many users to be concerned about their privacy and their control over the data they posted to the website. Facebook removed language that said if you remove anything you have posted to Facebook, the company relinquished any rights to it with the exception of keeping an archival copy. Consumer groups interpreted this change to mean that Facebook could do whatever it wanted with any users' information. On February 16th, Facebook CEO Mark Zuckerberg posted on the Facebook blog that users still control and own everything that they post to the website, and that before any information is used, the user must grant Facebook the right to use it. Zuckerberg acknowledged that the site had made missteps in sorting out these issues, and vowed to continue to work on the language in the terms of use to clarify the various problems pointed out by critics. The blog post may be found at <http://blog.facebook.com/blog.php?post=54434097130>

FAKE PARKING TICKETS USED TO SPREAD COMPUTER VIRUS

On February 3rd, SANS ant-virus analyst Larry Zeltser reported a new scam where hackers left fake parking tickets on cars and directed the cars to a website that supposedly contained photographic evidence of the violation. The website encouraged users to download a special toolbar, which installs the Vundo Trojan, thereby installing a fake virus scanner onto the computer. The targets of the scam were vehicles in Grand Forks, North Dakota. This is one of the many examples of hacker's creativity in coming up with new scams, but it may be the first time the hackers used a real world and web combination to attack potential victims. The blog post may be found at <http://isc.sans.org/diary.html?storyid=5797>

TEEN ACCUSED OF FACEBOOK BLACKMAILING FOR SEX

On February 5th, the *Associated Press* reported that eighteen year old Anthony Stancl of New Berlin, Wisconsin was arrested for posing as a girl on Facebook, enticing teenage males to send nude photos of themselves, and then threatening to post the nude photos on the Internet if the males did not perform sex acts with him. The charges included five counts of child enticement, two counts of second-degree sexual assault of a child, two counts of third-degree sexual assault, possession of child pornography, repeated sexual assault of the same child, and making a bomb threat. Police uncovered the scandal when they were investigating Stancl for a bomb threat that shut down New Berlin Eisenhower Middle and High Schools. Stancl's attorney said that he was looking into a plea bargain for his client. If Stancl were convicted of all charges he would be facing up to 300 years in prison. The story may be found at <http://www.msnbc.msn.com/id/29032437>

TORRENTSPY APPEALS DECISION IN FAVOR OF MPAA

On February 3rd, file sharing site TorrentSpy filed an appeal of a decision in favor of the Motion Picture Association of America forcing TorrentSpy to pay \$111 million in damages for copyright infringement. TorrentSpy allowed users to upload bootlegged films, but the website was shut down after the lawsuit. The court terminated the lawsuit before trial because TorrentSpy did not abide by discovery orders, and had been previously warned that the case would be terminated if it did not comply. The appeal is claiming that the court erred in terminating the case before trial and that the court wrongly forced TorrentSpy to violate its own privacy policy. The MPAA claimed that the purpose of TorrentSpy was to facilitate the illegal copying of films, and that the court correctly decided that TorrentSpy engaged in copyright infringement. The story may be found at http://news.cnet.com/8301-1023_3-10156637-93.html

Bytes in Brief[®] 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, enter your e-mail address into the sign-up box below. It will take you offsite to the *Constant Contact* website, where our opt-in only list is maintained and updated. After you confirm your e-mail address, you will receive an e-mail asking for confirmation that you do wish to become a *Bytes In Brief* subscriber. Once you reply to that e-mail, you will be added to the subscription list.

Subscribe to *Bytes in Brief*

Email:

Privacy by  SafeSubscribeSM
For Email Marketing you can trust

Copyright © 2009 Sensei Enterprises, Inc. All rights reserved.