

# {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 144 - May 2009

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

---

### COURT ENCOURAGES SEARCH TERM COLLABORATION

On March 19th, Magistrate Judge Andrew J. Peck of the U.S. District Court for the Southern District of New York encouraged collaboration between parties in forming search terms for electronic documents. The case involved disputes over alleged defects and delay in construction of the Bronx County Hall of Justice. The Dormitory Authority of the State of New York (DASNY) “owned” the project but non-party Hill International was the current construction manager for the hall. At issue were Hill’s e-mails and how to formulate search terms to separate e-mails concerning only construction of the hall. DASNY selected some search terms, but Hill did not contribute to the discussion. The court explained that it was left in the “uncomfortable position” of selecting search terms without adequate information from the parties. The court ordered production under DASNY’s proposed search terms, in addition to the names of the personnel involved in the hall construction. The court then explained the need for care and collaboration in selecting search terms, since the message did not get through in this case. The court quoted decisions by Magistrate Judges Grimm and Facciola, explaining the proper selection of search terms. These opinions stressed that proper implementation requires a specialized knowledge, and that implementation requires careful advance planning. The court advocated that parties should be more cooperative in the future, consistent with the Sedona Conference Co-operation Proclamation. The decision may be found at [http://www.ediscoverylaw.com/uploads/file/Westlaw\\_Document\\_William%20A%20Gross.doc](http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_William%20A%20Gross.doc)

---

### FAKE FACEBOOK GROUP DEMONSTRATES SECURITY ISSUES

On March 26th, ZD Net reported that a fake Facebook group could potentially expose millions to malware, as over one million people joined a fake (but non-malicious) group purporting to be from “Facebook Messenger.” Facebook users received a group invitation that stated they had to join this group and download a toolbar before the messenger system would work. The reporter went to the download website, and had friends validate it to assure that it was not malicious. Though the download website was not malicious in this case, it easily could have been, indicating the need for people to pay attention to the groups they join and applications they download. It was unclear what the site was set up for since it was not malicious, though it could have been used for click fraud. The reporter reported the group to Facebook, who removed it after one million users had already joined. Facebook indicated that it removes fake groups as soon as they are reported, but it remains to be seen what would happen if the group was not reported. The moral of the story is: be careful what groups you join, links you click on, and applications you download. The story may be found at <http://blogs.zdnet.com/feeds/?p=809>

---

### CANADIAN JUDGE ORDERS WEBSITE TO REVEAL ANONYMOUS POSTERS

On March 25th, Ontario Superior Court Judge Stanley Kershman ordered the owners of the website Free Dominion to turn over the identifying information of about eight people accused of defamation over anonymous comments. The commenters were accused of defaming human rights lawyer Richard Warman by posting on the site that he had made hateful and racist comments. Warman requested documents that would help identify the posters, including their e-mail addresses, IP addresses, and other personal information. The court found that privacy concerns do not always protect people from civil or criminal liability. Further, the types of information requested were not those that were expected to be kept from the state. The website operators did not have the funds to

appeal, and therefore would likely have to comply with the decision. The story may be found at <http://www.cbc.ca/canada/ottawa/story/2009/03/25/tech-090325-anonymous-posters.html>

---

## **ACLU SUES PROSECUTOR FOR CHILD PORN PROSECUTION OF TEENS**

On March 25th, the American Civil Liberties Union filed suit against a Wyoming County, Pennsylvania prosecutor for threatening teenage girls with child pornography charges. The charges stemmed out of a phenomenon known as "sexting," a play on the term texting, in which nude or semi-nude photos are sent on cell phones or posted on the Internet. School officials discovered the photos, which depicted two of the girls in white bras, and one in a towel that covered her only from the waist down, on students' cell phones. The prosecutor claimed that the girls were accomplices to the production of child pornography because they allowed themselves to be photographed. To avoid the charges, the prosecutor stated that the girls would be placed on probation, have to complete a five-week re-education program, and be subject to random drug testing. The ACLU lawsuit alleged that the prosecutor abused his power in threatening children with baseless charges, and asked that the court issue an order preventing criminal charges from being filed. The ACLU press release with a link to the complaint may be found at <http://www.aclupa.org/pressroom/aclusueswyomingcountyafor.htm>

A more comprehensive story on sexting may be found at <http://www.cnn.com/2009/CRIME/04/07/sexting.busts/index.html>

---

## **CHILD PREDATORS INCREASE WITH INCREASE IN PROSECUTIONS**

On March 23rd, the Associated Press reported that although prosecutions of child predators have increased, so have the number of child predators. The increase in child predators is partially due to increased access to the Internet. There are over 60 specialty units nationwide that deal with the exploitation of children, and these units are becoming overworked as the number of arrests increases. The officers pose as children online, and set up meetings with predators. In Wisconsin, an officer lured a predator to a parking lot and was met with the youth pastor at the officer's church. As the caseload increases, the departments request more officers and resources, which limited state budgets cannot always give. Further information may be found at <http://www.newswise.com/articles/view/550579/>

---

## **RESEARCH DISCOVERS CYBER-ESPIONAGE THAT COVERED 103 COUNTRIES**

On March 29th, a report revealed that an astonishing number of computers have been spied on across the world. The culprit for the spying is a network named GhostNet, which uses a malicious software program called gh0st RAT (Remote Access Tool) to steal sensitive documents, control webcams and control infected computers. Most of the infected computers belonged to international institutions that had no idea they were being tracked. The report did not know whether the information was valuable to the hackers or whether it was being sold or passed on as intelligence. There was some indication that servers in China were collecting the data, but the researchers did not want to point the finger at China too quickly. The researchers first discovered the scheme through servers in Tibet, and conducted ten months of research to discover other targets. Some of the research involved simply typing code from infected computers into Google. The report shocked governments across the globe, and showed a need to reassess their infrastructures to prevent such cyberspying. The report may be found at <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>

---

## **CYBERSECURITY BILL INTRODUCED IN SENATE**

On April 1st, Senators Olympia Snowe and John D. Rockefeller IV introduced sweeping cybersecurity legislation that would revise cybersecurity processes and oversight in government, facilitate public-private partnerships to keep computer systems safe, and fund cybersecurity research. To facilitate cooperation between the public and private sectors, the legislation would create a public-private clearinghouse to share vulnerabilities in computer systems, create a licensing requirement for those who work in cybersecurity, and create a program to help smaller businesses comply with cybersecurity requirements. To fund research, the legislation would increase a current

program that gives scholarships to students who promise to work in government after studying information technology in college. The bill would create a national cybersecurity advisor who would answer to the President and would be the top official on cybersecurity issues. The advisor would also coordinate efforts within the intelligence community and other agencies. The legislation also requires the advisor to conduct a comprehensive cybersecurity review every four years to assess cybersecurity strategy and progress. Senator Snowe's press release may be found at

[http://snowe.senate.gov/public/index.cfm?FuseAction=PressRoom.PressReleases&ContentRecord\\_id=6306ecb2-802a-23ad-4a08-163f03f287da&Region\\_id=&Issue\\_id=](http://snowe.senate.gov/public/index.cfm?FuseAction=PressRoom.PressReleases&ContentRecord_id=6306ecb2-802a-23ad-4a08-163f03f287da&Region_id=&Issue_id=)

---

## **U.S. SUPREME COURT REFUSES TO HEAR VA. SPAM CASE**

On March 30th, the U.S. Supreme Court refused to reinstate Virginia's Anti-Spam law after the Supreme Court of Virginia struck down the law as a violation of First Amendment rights. The case also overturned the conviction of Jeremy Jaynes, one of the world's most prolific spammers, and the first individual convicted of a felony for sending spam. Virginia Attorney General Bill Mims said he was disappointed with the decision and indicated his desire to draft new legislation to replace the overturned law. The new legislation would address the Supreme Court of Virginia's concerns with the overturned law. The story may be found at

<http://www.cnn.com/2009/TECH/03/30/scotus.anti.spam/>

---

## **REPORT INDICATES THAT INTERNET CRIME INCREASED WITH RECESSION**

On March 31st, the Internet Crime Complaint Center (IC3), run by the FBI and the National White Collar Crime Center, released its annual report on the number of received Internet crime complaints. Complaints hit a record high in 2008 with 275,284 complaints, compared to 206,884 in 2007, a 33.1% increase. The total dollar loss from Internet fraud was \$265 million, about \$25 million more than in 2007. The different types of complaints included not receiving ordered merchandise, auction fraud, credit card fraud, and investment scams. Officials explained that the report indicates a need for better law enforcement and consumer education to prevent Internet fraud, particularly during these rough economic times. The IC3 press release may be found at

<http://www.ic3.gov/media/2009/090331.aspx>

---

## **LIBEL SUIT FILED OVER TWITTER POSTS**

On March 26th, fashion designer Dawn Simorangkir sued singer Courtney Love for libel in Los Angeles Superior Court over Love's angry Twitter posts about Simorangkir. Court documents indicate that Love was furious with Simorangkir after she stopped working for Love because Love did not pay her bill. The tweets posted by Love supposedly accuse Simorangkir of dealing drugs, losing custody of her child, committing assault and burglary, and being a "nasty, lying, hosebag thief." Simorangkir claims that these comments have destroyed her reputation and her business, and she seeks punitive damages. The story may be found at

<http://www.independent.co.uk/news/media/online/loves-online-spat-sparks-first-twitter-libel-suit-1656621.html>

---

## **COURT GRANTS MOTION TO COMPEL RE-PRODUCTION OF CERTAIN ESI**

On March 18th, the U.S. District Court for the District of Kansas ordered re-production of certain e-mail files in native format after the Plaintiff Julie White, discovered discrepancies between relevant e-mail sent dates and creation dates of their attachments. The lawsuit was a wrongful termination claim, where White was trying to determine when the Defendants, her former employers, made the decision to fire her. White requested re-production of e-mails in native format, production of relevant PST (Outlook Personal Storage) and OST (Offline Outlook Storage) files, and access to the hard drives used to create any of the e-mail attachments. The court partially granted White's motion to compel, and considered each type of production in turn. First the court considered production of the e-mails in native format, and found that production was necessary. Defendants claimed that the e-mails may not be available, but provided no explanation. Further, Defendants' attorneys did not sufficiently familiarize themselves with their clients' e-mail systems, as the briefing did not provide sufficient information for the court to determine where the ESI could be located. Second, the court considered production of

the relevant PST files, and also found that production was necessary. The court explained that production of these files would help White resolve the discrepancies between the e-mails and their attachments, given the insufficient information about Defendants' computer systems. Third, the court considered whether the OST files must be produced, and found that it did not have sufficient information to make a decision. The court therefore ordered the parties to meet and confer with their computer experts to determine a process to produce the OST files. Finally, the court explained that Federal Rule of Civil Procedure 34 allows a party to inspect, copy, test, or sample ESI. The court relied on the Advisory Committee notes and explained that the inspection was not routine but may be justified in some circumstances, as inspection of ESI raises privacy concerns. In light of the e-mail discrepancies, the court found that more information was needed. The court again ordered the parties to meet and confer regarding the location of the information needed and a protocol to assess that information. The decision may be found at [http://www.ediscoverylaw.com/uploads/file/Westlaw\\_Document\\_White.doc](http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_White.doc)

---

## **LIVE VIDEO FEED IN FLORIDA HOME CATCHES BURGLARS IN THE ACT**

On April 8th, Jeanne Thomas of Boynton Beach, Florida was at work watching a live video feed of her dogs from the hidden camera installed in her home. Eventually, two men walked into her house and started robbing it, all as Thomas was watching remotely from her office. She called 911 and the police went to her house and apprehended the two suspects. The suspects were accused of trying to steal a flat screen TV, a video game system, and a safe. Police also caught two other suspects who were robbing a nearby house. The story and video may be found at [http://news.cnet.com/8301-17852\\_3-10216518-71.html](http://news.cnet.com/8301-17852_3-10216518-71.html)

---

## **REPORTING PIRACY PAYS**

On April 9th, the Software & Information Industry Association (SIIA) announced that it paid almost \$90,000 in March to ten sources who reported cases of corporate end-user software piracy to the SIIA. The organization is the principal trade organization for the software and digital content industries. To curb piracy, the SIIA offers rewards to its tipsters ranging from \$500 for settlements of \$10,000 and up to \$1 million for cases that settle over \$20 million, if the tips are confirmed. After receiving a tip, the SIIA investigates the cases and seeks a settlement, which usually includes a promise to stop using pirated programs. The program allows the SIIA to combat piracy and ensures that they obtain accurate and reliable information. The SIIA press release may be found at [http://www.sii.net/press/releases/AP%20awards%20release%20FINAL%20FINAL%20040809%20\\_3\\_%20\\_2\\_.pdf](http://www.sii.net/press/releases/AP%20awards%20release%20FINAL%20FINAL%20040809%20_3_%20_2_.pdf)

---

## **ELECTRICITY GRID HACKED INTO BY SPIES**

On April 8th, the Wall Street Journal published a report that indicated spies had hacked into the United States electricity grid. National security officials indicated that the spies came from China, Russia, or other countries. The spies did not attack the infrastructure, but tried to map it out, which could be used against the U.S. in wartime. There have been longstanding concerns about electricity infrastructure, heightened by the increase in technology that makes accessing the infrastructure easier. Research also indicated that there was no immediate threat of danger, as China relies on the U.S. economy and holds much of our national debt. On April 9th, Chinese officials denied responsibility for the attacks, claiming that the U.S. was simply preoccupied with the "China threat." The report may be found at <http://online.wsj.com/article/SB123914805204099085.html>

The story on China's response may be found at <http://blogs.wsj.com/chinajournal/2009/04/09/china-denies-hacking-us-electricity-grid/>

---

## **COURT STRESSES IMPORTANCE OF RECORDS MANAGEMENT**

On March 30th, the U.S. District Court for the District of Utah determined that a computer company's questionable electronic document retention policies rendered it sufficiently culpable for sanctions to be imposed. Plaintiff Phillip M. Adams & Associates filed suit against a variety of computer companies, including ASUS, alleging patent infringement. The Plaintiff filed a motion for sanctions during discovery, alleging that ASUS did not produce many responsive documents. The court first addressed two threshold issues. The first was whether the evidence was lost

and destroyed, and the court found that ASUS's production should have been more voluminous than it was. Second, the court addressed when the duty to preserve such evidence arose, and found that the duty arose when multiple lawsuits were filed surrounding disk defect issues, which ASUS should have been aware of. The court then addressed ASUS's argument that it was entitled to the "safe harbor" provision of Federal Rule of Civil Procedure 37(e) because the information was lost due to the routine, good faith production of its computer systems. The court rejected this argument, and found that there was no support for ASUS's assertion that its policies were reasonable, as neither its expert nor its employees could describe a data backup system, leaving the system "at the mercy of individual employees' backup practices." The court then considered what sanction would be appropriate in this situation, considering the degree of culpability of the party who lost or destroyed evidence and the degree of prejudice to the other party. The court found that ASUS was culpable because ASUS had a duty to third parties to have reasonable retention policies. The court then explained that it could not determine the amount of prejudice to the Plaintiff, as discovery was ongoing. The court ordered the parties to brief the issue of appropriate sanctions. The decision may be found at

[http://www.ediscoverylaw.com/uploads/file/Westlaw\\_Document\\_Phillip%20Adams.doc](http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_Phillip%20Adams.doc)

---

### **PENTAGON SPENDS \$100 MILLION TO FIX CYBERATTACK DAMAGE**

On April 7th, military leaders announced that the Pentagon spent more than \$100 million in the last six months fixing damage from cyberattacks and other computer network problems. General Kevin Chilton, head of U.S. Strategic Command stated that the military is only beginning to track the costs of cyberattacks, as there are constant daily attacks against military networks around the country. The Strategic Command is responsible for protecting and monitoring the military's information grid and coordinating any offensive cyber warfare for the U.S. The attacks vary from mere vandalism to espionage. In addition to fixing the problems from attacks, the Strategic Command also corrects internal mistakes such as viruses. General Chilton's speech may be found at

<http://www.stratcom.mil/speeches/23/>

---

### **WSJ, AP ATTACK GOOGLE AND OTHER AGGREGATE NEWS SITES**

On April 6th, managers at major news sources the Wall Street Journal and the Associated Press took aim at Google and other aggregate news sites. Robert Thompson, editor of the WSJ described certain websites as "parasites" of the Internet, and stated that aggregators like Google profit from the mistaken perception that all online content should be free. William Dean Singleton stated that the AP was not going to stand by and watch others walk off with its work. Google on the other hand maintains that news site owners have a means to prevent Google from crawling their websites and indexing headlines. AP has an agreement with Google so Google can use AP's content, but AP representatives stated that they want Google's help in preventing misappropriation of content. The comments raise questions of whether Google or other sites will be forced to defend themselves against copyright infringement lawsuits. The story may be found at [http://news.cnet.com/8301-1023\\_3-10213336-93.html](http://news.cnet.com/8301-1023_3-10213336-93.html)

---

### **ISPS IN EUROPE TO RECORD ALL E-MAILS AND PHONE CALLS**

On April 6th, new European Union regulations went into effect that require all Internet Service Providers to keep records of e-mails and online phone calls for twelve months to assist in criminal investigations. ISPs will record the date, time, duration, and recipients of online communications, but not the content of the communications. The new regulations expand on current regulations that apply to telecommunications providers. The initial regulation was drafted after the 2005 London bombings. Privacy advocates worried about the consequences of the government having access to such extensive amounts of information, but others believe that the information will be valuable. The regulations may be found at [http://www.opsi.gov.uk/si/si2009/draft/ukdsi\\_9780111473894\\_en\\_1](http://www.opsi.gov.uk/si/si2009/draft/ukdsi_9780111473894_en_1)

---

### **SENATORS INTRODUCE BILL TO ALLEVIATE CELL PHONE SPAM**

On April 2nd, Senators Olympia Snowe and Bill Nelson introduced new legislation that would prohibit commercial text messages to cell phone numbers listed on the Do Not Call registry. The bill would give the Federal Communications Commission and the Federal Trade Commission the authority to regulate unwanted text

messages. Senator Snowe explained the importance of preventing these types of messages as mobile spam increases a customer's monthly bill and could spread viruses or malicious spyware. Mobile spam could also be used for phishing attacks, where scammers try to get users to reveal personal data over the phone. As text message use increases, so does the need for curbing mobile spam. Senator Snowe's press release may be found at

[http://snowe.senate.gov/public/index.cfm?FuseAction=PressRoom.PressReleases&ContentRecord\\_id=683ec526-802a-23ad-42b5-5448caaa57d3&Region\\_id=&Issue\\_id=](http://snowe.senate.gov/public/index.cfm?FuseAction=PressRoom.PressReleases&ContentRecord_id=683ec526-802a-23ad-42b5-5448caaa57d3&Region_id=&Issue_id=)

---

## **POLICE USING FACEBOOK, MYSPACE TO MONITOR STUDENT BEHAVIOR**

On April 6th, the Washington Post reported that school police officers are monitoring social networking sites to keep a handle on school crime. The default setting for many social networking sites is to allow anyone to view your profile (Facebook default is only friends) and few students change those settings to "private," it is relatively easy for the police to use these tools to their advantage. The officers use the sites to break up fights, monitor gangs, and even solve crimes. For example, Fairfax County, VA police arrested seven gang members in Chantilly, VA for trying to recruit middle school students into a gang. Also, students who have run away from home sometimes get online to see what their friends are doing, which could provide an officer with information on the runaway's location. Some students were disturbed that officers were looking at their profiles, as some of the postings were provocative. But others stated that they know officers look at social networking sites, and if you put up incriminating pictures you should pay the consequences. The story may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2009/04/05/AR2009040501880.html>

---

## **COURT FINDS SANCTIONS UNNECESSARY WHEN EVIDENCE DESTROYED BEFORE DUTY TO PRESERVE AROSE**

On March 27th, a U.S. District Court in Northern California found that the Defendant in the case could not be sanctioned because the evidence showed the relevant electronic discovery was destroyed before the duty to preserve it arose. The case stemmed out of the joint purchase of the Headwaters Forest by the U.S. Government and State of California. The Defendant is Maxxam, Inc., a lumber company accused of making false statements to the government that caused the government to purchase some of the forest. The government claimed that Maxxam spoliated evidence by failing to preserve relevant computer files relating to the purchase. The court first explained that the duty to preserve evidence can arise before litigation is commenced, and that sanctions may be imposed if Maxxam knew or should have known that the documents were relevant to the potential litigation. Applying that standard here, the court found that Maxxam's duty to preserve arose in 2006, when a claim was filed against the State of California dealing with the Headwaters agreement. The court then considered whether the evidence existed in 2006, and found that the government did not satisfy their burden to show it did. Maxxam first searched for one of the files in 2006 and could not locate it, indicating that it was destroyed before 2006 and the duty to preserve the evidence arose. While the court found it troubling that Maxxam did not impose a litigation hold, it explained that it could not hold Maxxam liable for evidence destroyed before the duty to preserve it arose. The decision may be found at [http://www.ediscoverylaw.com/uploads/file/Westlaw\\_Document\\_Maxxam.doc](http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_Maxxam.doc)

---

## **ORGANIZED CRIME CONSIDERED BEHIND MOST DATA BREACHES**

On April 15th, Verizon released its 2009 Data Breach Investigations Report that indicated organized criminals were responsible for many of the data breaches that occurred in 2008. More than 90 percent of the records compromised came from targeted attacks where the hackers carefully determined their victims and figured out how to exploit them. This resulted in over 100 data breaches involving about 285 million consumer records in 2008 – more than the numbers from 2004-2007 combined. Bryan Sartin, director of investigative response at Verizon Business explained that many of the breaches came from criminals in Eastern Europe, particularly those data breaches that took place in the first five months of 2008. Two separate criminal groups out of this area are thought to be behind the two largest data breaches, namely those that hit RBS WorldPay and Heartland Payment Processing. To mitigate the possibility of these breaches, the report suggested that companies ensure essential controls are met, audit user accounts and credentials, and test and review web applications. The report may be found at [http://www.verizonbusiness.com/resources/security/reports/2009\\_databreach\\_rp.pdf](http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf)

---

## **COURT FINDS SANCTIONS WARRANTED WHERE PARTY HAD EMPLOYEES “PRINT AND DELETE” DOCUMENTS**

On April 9th, the U.S. District Court for the Southern District of Florida found that sanctions were necessary when a Defendant's attorneys instructed Defendant's employees to print 10,000 documents and then delete the documents from their computers. In the case, Preferred Care Partners Corp. (PCP) alleged that Humana, Inc. violated a confidentiality agreement between the parties. PCP brought the motion for sanctions, alleging that Humana's employees could not be trusted to fully produce the electronic documents. The court first stated that it was clear that Humana did not comply with the Federal Rules of Civil Procedure or the Local Rules when producing these documents. For that reason, the court explained that it could impose sanctions under Federal Rule 37 based on what was reasonable under the circumstances. The court found that a default judgment or adverse inference instruction, particularly harsh sanctions, were not necessary in this case. Although Humana's conduct was careless and showed bad judgment, it was not willful and did not show bad faith. But the court shared PCP's concerns that some documents may be missing, and ordered sanctions to remedy that situation. The court ordered that Humana allow an inspection of its backup system at its own expense to verify that the backup system retains copies of the e-mails that were produced, despite the print and purge directive. Any information not deleted and not produced would be provided to PCP. The decision may be found at

[http://www.ediscoverylaw.com/uploads/file/Westlaw\\_Document\\_PREFERRED%20Care.doc](http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_PREFERRED%20Care.doc)

---

## **FOUR FROM PIRATE BAY CONVICTED OF COPYRIGHT INFRINGEMENT**

On April 17th, the Stockholm district court in Sweden convicted four men behind the file-sharing site Pirate Bay of violating Sweden's copyright laws. The four men, Gottfrid Svartholm Warg, Peter Sunde, Fredrik Neij and Carl Lundstrom were sentenced to one year in prison and ordered to pay 30 million kronor (\$3.6 million) in damages to entertainment companies including Warner Bros, Sony Music Entertainment, EMI and Columbia Pictures. Although defense counsel argued that the four men were not actually violating the copyright laws themselves, the court found that the men were guilty of helping others commit copyright infringement through the website. The men intended to appeal the ruling, and stated that an "I owe you" was as close as the entertainment companies would get to their damage payments. On April 23rd, one of the Pirate Bay lawyers called for a retrial after reports that the judge is a member of several copyright protection associations and serves as a board member on one of the groups of which the Motion Picture Association of America's attorney is a member. The attorneys claimed that the lack of impartiality makes a retrial necessary. The judge claimed that his involvement in these types of activities did not sway him in the case or constitute a conflict of interest. The story may be found at

[http://www.usatoday.com/tech/news/2009-04-17-pirate-bay\\_N.htm](http://www.usatoday.com/tech/news/2009-04-17-pirate-bay_N.htm)

A story on the retrial may be found at <http://www.thelocal.se/19028/20090423/>

---

## **CALIFORNIA STATE SENATE PASSES MORE STRINGENT DATA BREACH LAW**

On April 27th, the California State Senate passed SB-20, which will force businesses in California to give customers more specific information in the event of a data breach. California's current data breach notification law requires businesses to notify consumers of a breach, but does not require any further information. The new bill requires businesses to report the type of personal information breached and the date of the breach. Further, if more than 500 California residents are affected by a single breach, then the business will have to submit a copy of the breach notification to the Attorney General. State Senator Joseph Simitian introduced the bill, and explained that the new requirements would greatly improve the existing data breach law and help get consumers out of the dark about data breaches. Simitian's press release may be found at

[http://www.senatorsimitian.com/news/entry/senate\\_strengthens\\_consumer\\_privacy\\_protection/](http://www.senatorsimitian.com/news/entry/senate_strengthens_consumer_privacy_protection/)

---

## **MED STUDENT ACCUSED OF KILLING WOMEN HE MET ON CRAIGSLIST**

On April 19th, police arrested Boston University medical student Phillip Markoff for the murder of one woman and the robbery of another woman, both of whom he met on Craigslist. The first victim, Julissa Brisman of New York

City, was found dead in a Boston hotel April 14th after being bashed in the head and shot three times. Brisman and Markoff had allegedly set up a meeting after Brisman advertised erotic massages on Craigslist. Police traced Markoff's e-mail address, and he was arrested shortly thereafter. Markoff is also accused of robbery of a Rhode Island woman, where he again used Craigslist to contact the woman. She met him in a Boston hotel, and he allegedly pointed a gun at her, tied her up, and robbed her of more than \$800 and personal items. It is rumored that Markoff has a gambling problem, and was committing the robberies to pay off debts, until Brisman's robbery went horribly wrong. Markoff was arraigned on April 21st and is being held without bail. Markoff's family and friends state that this is not the Markoff they knew, as he was a motivated medical student who was getting married in August. The story may be found at [http://www.boston.com/news/local/breaking\\_news/2009/04/surveillance\\_ph.html](http://www.boston.com/news/local/breaking_news/2009/04/surveillance_ph.html)

---

## NEW GPS SYSTEM ALLOWS OWNERS TO FIND LOST DOGS

On April 20th, news sources reported a new GPS dog collar that can help owners locate a lost pet. The device, called a SpotLight, is going to be marketed by the American Kennel Club starting next month. It will cost \$250.00, and allows dogs to be located by cell phone, smartphone or computer. Owners can call or text message the service anytime to receive the location of their pet. Owners also can set up "SafeSpots," which are safe areas identified by the owners. If a pet leaves a SafeSpot, the owner can be notified by text message or e-mail. The tracking device attaches to an existing collar and also contains an LED light that is visible from 100 yards. The LED can be activated remotely via a web browser or by sending the text message "Spot SpotLight On." Co-editors John Simek and Sharon Nelson have spent WAY too much time searching for their adventurous labs when the back yard gate was left open by a vendor or forgetful dog sitters, and therefore designated this one of the most important tech stories of the month. The story may be found at [http://www.boston.com/business/technology/articles/2009/04/20/satellites\\_beat\\_id\\_chips\\_for\\_recovering\\_lost\\_pets/](http://www.boston.com/business/technology/articles/2009/04/20/satellites_beat_id_chips_for_recovering_lost_pets/)

---


*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, 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  SafeSubscribe<sup>SM</sup>  
For Email Marketing you can trust

---

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