



Issue 135 August 2008

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

NEW BAGS MAY END LAPTOP HASSLE AT U.S. AIRPORTS

On July 1st, the New York Times reported that new laptop bags may decrease the hassle for airline passengers traveling with laptops. U.S. airport security procedures currently require laptops to be taken out of carry-on bags for security screenings, because other items such as power cords and mice may prevent security officers from screening the laptop properly. In March, the Transportation Security Administration (TSA) gave luggage manufacturers the green light to produce new bags that would allow laptops to go through security without being removed from the bag. Luggage manufacturers answered the TSA's call for the bags, and prototypes are being tested at three airports. Though the TSA will not rubber-stamp the bags, manufacturers can place a "checkpoint friendly" tag on the bag. Manufacturers such as Targus and Pathfinder stated that the bags would be out in early fall. The TSA press release may be found at http://www.tsa.gov/press/happenings/laptop_case.shtm

The New York Times article may be found at http://www.nytimes.com/2008/07/01/business/01road.html?_r=2&th=&adxnnl=1&oref=slogin&emc=th&adxnnlx=1214917069-iJ39VY+Op0h03gjQb+2bMw&o_ref=slogin

E.U. LAWMAKER SUES U.S. FOR ACCESS TO PERSONAL INFO

On July 1st, the Electronic Frontier Foundation (EFF) announced that it was suing on behalf of Sophie In 't Veld, a member of the European Parliament who travels to the U.S. frequently, and is often detained at the border before being allowed to board her flights. The EFF and In 't Veld are suing to force the U.S. government to comply with In't Veld's Freedom of Information Act request asking for information the U.S. has concerning In't Veld. Requests for information were sent to numerous U.S. government departments, including the FBI, State Department, and Customs. All stated that they either had no information or did not reply. The lawsuit is meant to prove that FOIA requests are not complied with, despite repeated assurance by the Bush Administration that they would be. The lawsuit also sheds light on a main issue of contention between the U.S. and the E.U. that is hindering talks of massive data sharing between the two. The press release on the EFF website, with a link to the full complaint, may be found at <http://www.eff.org/press/archives/2008/07/01>

FIRM HIT WITH MALPRACTICE SUIT FOR DISCOVERY PROBLEMS

On June 25th, chemical company Celanese Corp. filed a legal malpractice suit against law firm Kaye Scholer for discovery mistakes. The complaint alleges that Kaye Scholer committed serious discovery errors that forced Celanese into a \$107 million settlement. Kaye Scholer allegedly failed to turn over hundreds of thousands of documents to plaintiffs in the case, and the consequences were discovery sanctions that forced Celanese into a larger settlement. Without the sanctions, Celanese alleges it would have paid a nuisance settlement with a decreased price tag, and it therefore seeks the difference between the nuisance settlement and the price it paid. The complaint was filed in Texas state court, and was removed to U.S. District Court for the Northern District of Texas. The full complaint may be found at <http://www.nylawyer.com/adgifs/decisions/062708complaint.pdf>

SURVEY REPORTS 8 IN 10 BUSINESSES NOW USING MACS

On June 9th, the Yankee Group announced the results of a survey that found businesses are increasingly using Mac computers. The survey found that almost 80% of businesses have Macs in-house, which was double the amount two years ago. With the amount of Macs used per firm, Apple's market share for corporate clients was up to 8-10% from 1-2%. Research fellow Laura Didio said that the trend was encouraging for Apple, especially since they were not doing anything to reach out to the corporate demographic. One feature that businesses liked about the Mac was its ability to use more than one operating system, as 28% of the firms surveyed said they are running Windows on a Mac machine, and 22% said they are using the Mac's Boot Camp feature to use both Windows and Mac OS X on the same computer. The InfoWorld news article on the survey may be found at http://www.infoworld.com/article/08/06/26/8_in_10_businesses_now_using_Macs_1.html

ICANN TO RELEASE NEW TOP LEVEL DOMAIN NAMES

On June 26th, the Internet Corporation for Assigned Names and Numbers (ICANN) announced that new top level TLDs, which are the end of Internet addresses such as ".com" and ".org," may be up for grabs by the end of 2009 for as little as \$100,000. The new addresses may include unique names for cities, such as ".nyc" or ".berlin," or by areas of interest, such as ".travel." First, ICANN must approve an implementation plan, which it is hoping to do in early 2009 so applications may be submitted starting in the second quarter of 2009. There will be a way for applicants to appeal another applicants' use of a trademark, and a way to screen out offensive names. ICANN's press release may be found at <http://www.icann.org/en/announcements/announcement-4-26jun08-en.htm>

ANITSPAM GROUP EXPLAINS HOW TO GET RID OF SPAM

On June 25th, the Messaging Anti-Abuse Working Group (MAAWG) laid out guidelines for ISPs to block spam e-mail without blocking users who forward their e-mail from one account to another. When users forward e-mails from one account to another, especially from an account that has a lot of spam e-mails, the incoming server blocks all e-mails, including legitimate ones. MAAWG explained that ISPs could fix the problem by separating the servers that received e-mail from servers that forward e-mail. The guidelines also address the problem of computers sending spam after being infected with malicious software. After they are infected, computers then start sending spam e-mails directly to the Internet through a different IP address. The guidelines suggest that ISPs block the different, known as dynamic, IP addresses, or share information about dynamic addresses if they cannot be blocked. The press release may be found at <http://www.maawg.org/news/maawg080625>

The MWAGG recommendations on dynamic IP addresses may be found at http://www.maawg.org/about/publishedDocuments/MAAWG_Dynamic_Space_2008-06.pdf

The MWAGG recommendations on e-mail sharing may be found at

http://www.maawg.org/about/publishedDocuments/MAAWG_Email_Forwarding_BP.pdf

ABC TO PAY WORKERS FOR DOING WORK ON BLACKBERRYS AT HOME

On June 27th, ABC and the Writers Guild of America East settled a dispute about workers being paid for work done on their BlackBerries at home. The issue was whether employees should get paid for time spent on their BlackBerries while out of the office. Both sides reached a compromise, and ABC agreed to pay workers for using their BlackBerries at home, but only for work related usage. The compensation will not include use of the device to check e-mail at night, but writers and producers will be compensated in certain circumstances, such as when an important news story breaks after office hours. The full story may be found at <http://www.wgaeast.org/index.php/articles/1535?wgra=1#wga1535>

COURT RULES NO JURISDICTION OVER NONRESIDENT ONLINE COMMENTS

On June 17th, the North Carolina Court of Appeals ruled that a nonresident's online comments

about a resident did not form a basis for specific personal jurisdiction in North Carolina without intent to target the forum. In the case, plaintiff Jack Dailey filed a defamation lawsuit against Donald Pompa and R.W. Beaver, Jr. because of derogatory remarks made by the two on the Internet. Pompa was a Georgia resident, and filed a motion to dismiss for lack of personal jurisdiction. The court used a test promulgated by the U.S. Fourth Circuit Court of Appeals in *Young v. New Haven Advocate*, which required a defendant to have targeted the specific forum where the defamation took place. The court here found that Dailey showed no evidence indicating that Pompa had specifically targeted North Carolina readers; therefore, it could not exercise specific personal jurisdiction over Pompa. The case is *Dailey v. Pompa*, and the full decision may be found at <http://www.aoc.state.nc.us/www/public/coa/opinions/2008/pdf/070310-1.pdf>

NONPROFIT GROUP REPORTS DATA BREACHES UP 69% THIS YEAR

On June 27th, the Identity Theft Resource Center (ITRC) announced that data breaches have reached an all-time high in the first half of this year. The total number of data breaches recorded by the ITRC from January 1st to June 27th was 342, with 27% of breaches coming from businesses. The ITRC counted the number of breaches, as opposed to the number of records compromised, because the number of compromised records is often incomplete or misleading. Electronic data breaches accounted for the vast majority of breaches at 80%, and most occurred through stolen items such as laptops or thumb drives. Surprisingly, hacking accounted for only 11% of breaches. The full report may be found at http://www.idtheftcenter.org/artman2/publish/m_press/Breach_List_2008_Q2.shtml

SEXUAL PREDATORS USING GAME CONSOLES TO LURE CHILDREN

On July 2nd, USA Today reported that sexual predators are turning to gaming consoles such as the Wii, Playstation and Xbox to meet children online. The gaming consoles offer features that allow children to access the Internet and text message other players. According to the report, sexual predators are now using these features to meet children online. In response, police are going undercover to play games targeted to children and are arresting sexual predators found on the games. In Utah, police arrested a man who lured a 12-year-old boy he met through a game into having sex. In Michigan, the same type of incident happened with a 12-year-old girl. Microsoft has assisted police in how to extract messages from the Xbox, and the consoles also have "family settings" that allow parents to track their children's use of the Internet features. The full story may be found at http://www.usatoday.com/tech/news/2008-07-01-porn_N.htm

DISPUTE COULD GARNER DECISION ON EMPLOYER E-MAIL POLICIES

On May 8th, Scott Sidell filed suit against his former employer in U.S. District Court for the District of Connecticut. The complaint alleges that the employer, Structured Settlements, Inc., read Sidell's personal Yahoo e-mail account after he was fired from the company, including e-mails from Sidell to his attorneys. The employer apparently read Sidell's e-mail when Sidell went to the office after he was terminated, accessed his Yahoo e-mail account and forgot to close it on the computer. The case raises issues about employers' rights to access employees' e-mail accounts. The law is still unclear concerning whether employers may read employees' personal e-mail accounts, and this case may provide some answers. The case is further complicated by the attorney-client privilege claim and that Sidell was not an employee when his e-mail was read. The full complaint may be found at <http://docs.justia.com/cases/federal/district-courts/connecticut/ctdce/3:2008cv00710/81493/1/>

A *New York Times* article that brings light to Sidell's story may be found at http://www.nytimes.com/2008/06/27/technology/27mail.html?_r=1&oref=slogin

AUDIT FINDS CELEBRITY PASSPORT RECORDS ACCESSED IMPROPERLY

On July 4th, the *Washington Post* reported that an audit found that State Department employees had been accessing celebrity passport records without authorization. The audit was conducted in response to reports that Senator Barack Obama and Senator Hillary Clinton's records had been

accessed in March. The report looked at 150 famous Americans – selected from a list of frequent Google searches, Forbes list of richest Americans and Sports Illustrated's list of the richest athletes – and found that of the 150, 127 records had been accessed more than 4,100 times in a 5 1/2 year period. The State Department previously maintained a "watch list" to ensure that the records of high profile persons were not breached but before the scandal only 38 people were on the list. The list now contains over 1,000 individuals. The report issued recommendations that the State Department has promised to implement, including punishment for those responsible for the breaches. The full story may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2008/07/03/AR2008070303799.html?hpid=topnews>

COURT ORDERS YOUTUBE TO TURN OVER USER DATA IN INFRINGEMENT SUIT

On July 1st, U.S. District Judge Louis Stanton ordered YouTube and Google to turn over user data in a copyright infringement suit by Viacom. The lawsuit claims that YouTube encourages users to upload copyright protected materials and that those copyrighted materials are viewed more often than amateur videos on the website. YouTube was ordered to turn over its "logging database," which keeps track of the millions of views each video gets on YouTube each day, and to include the IP address of the user watching and specific information about the video. Privacy advocates worried about potential invasions of privacy for users, and advocated an appeal of the July 1st order. From the controversy, Viacom and YouTube agreed to a stipulation on July 14th that the information of most users would be made anonymous before it was turned over. Judge Stanton's order may be found at http://beckermanlegal.com/Documents/viacom_youtube_080702DecisionDiscoveryRulings.pdf

The July 14th stipulation may be found at http://64.233.179.110/blog_resources/google_youtube_viacom.pdf

ANTISPAM COMPANY SAYS FIGHTING BOTNETS IS A LOSING BATTLE

On July 7th, Anti-spam company Commtouch released its quarterly report detailing the hopeless battle against botnet spam. According to the report, by the time computers are identified as infected with botnets, the identification is futile because the botnet has moved on to other computers. The company uses a "zombie monitor" to track botnets and other spam. A majority of the zombies come from ISPs, with some ISPs having trouble controlling the zombies sent from its subscribers. The report also details that the U.S. is 9th on the list of countries sending the most spam, with Turkey, Brazil, Russia, Italy and India making up the top five. The whole report may be found at http://www.commtouch.com/documents/Commtouch_Q208_Email_Trends.pdf

GAO REPORTS FEDERAL AGENCIES NOT PRESERVING E-MAILS PROPERLY

On July 8th, the Government Accountability Office released a report detailing the inadequacies of four government agencies in preserving e-mails. The four agencies that were surveyed were the Environmental Protection Agency, the Federal Trade Commission, and the Departments of Homeland Security and Housing and Urban Development. The report found that all four agencies were relying on an outdated "print and file" method to preserve e-mails. Only the EPA was converting to an electronic storage system. The report also explained that reviewing agency officials' e-mail preservation indicated that only seven of fifteen officials were complying with regulations on preserving e-mail. The report prompted the House Committee for Oversight and Government Reform to introduce legislation that requires government agencies to preserve e-mail in electronic format. The bill passed in the House on July 9th. The full report may be found at <http://oversight.house.gov/documents/20080708093459.pdf>

Information on the legislation may be found at <http://oversight.house.gov/documents/20080709125536.pdf>

HOMELAND SECURITY CONSIDERS SHOCK BRACELETS FOR FLIGHT PASSENGERS

On July 1st, the Washington Times reported that the Department of Homeland Security (DHS) is

considering using a shock bracelet for airline passengers. Canadian defense company Lamberd Less Lethal (LLL) would provide the bracelet. The bracelet would be worn by passengers on airline flights and would only be activated in the event of a hijacking. The bracelet uses electro-muscular disruption (EMD) technology to shock the wearer and incapacitate them in case of an incident. In addition to its incapacitating ability, the bracelet could also be used instead of a plane ticket and could track the wearer with his or her luggage. The LLL website included a letter from a DHS official indicating the government's interest in the bracelet. The full story may be found at <http://www.washingtontimes.com/weblogs/aviation-security/2008/Jul/01/want-some-torture-with-your-peanuts/>

ADOBE'S PDF BECOMES AN INTERNATIONAL STANDARD

On July 2nd, the International Standards Organization (ISO) announced that Adobe's Portable Document Format (PDF) is a new international standard. Because PDF is a national standard, Adobe must turn over PDF to the ISO. The ISO will now be in charge of publishing specifications for the current 1.7 version, and for updating and developing future versions. The standard sold by the ISO will contain all the essential information for developers with a price tag of about \$360. The ISO praised PDF in a press release for preserving the format of the original documents, something other software programs have struggled with. The full press release may be found at <http://www.iso.org/iso/pressrelease.htm?refid=Ref1141>

GOOGLE SUED FOR SELLING INADEQUATE ADS

On July 11th, attorney Hal K. Levitte sued Google for selling low-quality advertisements on parked domains and error pages. Levitte advertised his legal services using Google's programs last year. 15.3% of his ad campaign was taken up by parked domains, which are web pages with automated links related to a predetermined search keyword. Levitte had 202,528 impressions on parked domain pages, with 668 clicks and zero conversions. For the lack of results, Levitte sued Google for fraud, business code violations, and unjust enrichment. The lawsuit was filed as a class action, as Levitte's attorneys hope to represent others in the same situation. Just six days later, on July 17th, RK West, a company that does business as Malibu Sales, sued Google for the same reasons as Levitte. The second complaint alleges that Google uses ads on parked domains to launder "invalid clicks" on websites that have no content. The complaint claims that because Google charges customers for every click, regardless of validity, it benefits from the ads on parked domains while the customer does not. The RK West complaint may be found at <http://docs.justia.com/cases/federal/district-courts/california/candce/5:2008cv03452/205252/1/>

The Levitte complaint may be found at <http://docs.justia.com/cases/federal/district-courts/california/candce/5:2008cv03369/205116/1/>

THE SAGA CONTINUES FOR MICROSOFT, ICAHN, AND YAHOO

On June 25th, Yahoo released a letter that assured shareholders of the profitability of the Yahoo/Google deal. The letter also indicated that the deal with Google did not prevent a sale of Yahoo to Microsoft, because the Google deal may be terminated by either party upon a change of control. The letter included the reference despite Microsoft's assurance to its stockholders that it would not seek to acquire all of Yahoo, but would still consider a deal where Microsoft would acquire Yahoo's search business. Yahoo rejected the search acquisition because of oppressive terms, including giving Microsoft a right to veto the sale of Yahoo. On July 11th, Microsoft and billionaire investor Carl Icahn proposed an acquisition plan to Yahoo that included Microsoft taking over Yahoo's search service. Microsoft and Icahn gave Yahoo 24 hours to make a decision on the proposal, and the next day, Yahoo rejected the offer. Yahoo stated that it rejected the proposal because the deal with Google would be more profitable and the proposal did not offer to buy Yahoo for a fair price. Yahoo explained that it would sell the whole company for at least \$33 per share or negotiate another search-only transaction. On July 17th, Yahoo sent a letter to its shareholders urging them to accept the current board and stating that Icahn and Microsoft did not represent Yahoo's best interests. On July 21st, in a speedy change of heart, Yahoo made Icahn a member of the Yahoo board to prevent the impending proxy battle with Icahn. With the deal, the Yahoo board

will expand to 11 members to include Icahn and two members appointed from a list of Icahn's recommendations. In exchange, Icahn agreed to withdraw his members from consideration for Yahoo's board and vote in favor of the current Yahoo board at the shareholder meeting. The Yahoo and Icahn deal could help a possible amicable agreement with Microsoft to acquire all or part of Yahoo. The June 25th letter may be found at

<http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=318447>

Yahoo's press release on rejecting the Microsoft/Icahn proposal may be found at

<http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=321697>

Microsoft's press release "setting the record straight" may be found at

<http://www.microsoft.com/Presspass/press/2008/jul08/07-14statement.mspx>

Yahoo's letter to its shareholders supporting the current board may be found at

<http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=322710>

Yahoo's press release announcing the Icahn deal may be found at

<http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=323246>

NEW REPORT COMPARES CYBERCRIME TO THE MAFIA

On July 15th, security firm Finjan released its second quarter Web Security Trends Report that compared cybercrime to organized crime organizations. The report explains that the current structure of cybercrime has moved from a few hackers working together into a hierarchical organization such as the mafia, where there is a "boss" directing the organization but not getting his hands dirty. The hierarchy also includes seconds in command who organize and plan the attacks, "soldiers" who steal the data, and "resellers" who trade the stolen data. Organization is not limited to the attacks, as the cybercrime business also expanded to include "one stop Crimeware shops" where hackers sell toolkits to other hackers who are less technology inclined. Cybercriminals also have determined a way to figure out if the stolen credit card data has expired. As a result of the new organization and technology, the price of credit card numbers and bank accounts has fallen from about \$100 each to \$10-20 each. Finjan's press release with a link to the report may be found at <http://www.finjan.com/Pressrelease.aspx?id=1998&PressLan=1819&lan=3>

EBAY WINS COUNTERFEIT SALES CASE BROUGHT BY TIFFANY

On July 14th, U.S. District Judge Richard Sullivan ruled in favor of online auction website eBay in a lawsuit filed by jewelry giant Tiffany & Co. claiming any seller of five or more pieces of Tiffany jewelry was presumptively selling counterfeit merchandise and should be deleted. The issue in the case was whether Tiffany or eBay should have to police eBay for fake merchandise. Sullivan did not buy Tiffany's argument, and found that eBay did not have to police its auction site for counterfeit merchandise under trademark law, as it is the trademark owner's burden to protect its work. Sullivan found that eBay's general knowledge that counterfeit materials are sold on its site was not enough to hold eBay liable. The decision does not mean that counterfeit merchandise is allowed on eBay. Selling counterfeit merchandise violates federal law, and eBay stated that it spends about \$5 million a year to maintain its fraud search engine to identify counterfeit goods, along with maintaining a program that lets trademark owners identify and remove infringing listings. The full decision may be found at <http://www1.nysd.uscourts.gov/cases/show.php?db=special&id=83>

MEMPHIS POLICE SUE AOL FOR NAMES OF BLOGGERS

On July 10th, Memphis Police Director Larry Godwin and the city of Memphis filed suit in Shelby County Chancery Court to learn the identity of a blogger critical of Godwin's department. Chancellor Kenny Armstrong sealed most of the documents in the case, but the lawsuit asks AOL to turn over information related to an e-mail address linked to the blog. Beyond seeking the identity, it is unclear whether the lawsuit asks for the website to be shut down, or for the website to prevent leaks about current investigations. The case raises important First Amendment issues concerning the right of bloggers to remain anonymous. The bloggers claim the website is an important outlet for citizens to

voice their displeasure with the government, and that to shut it down would violate the First Amendment. The full story from the *Memphis Commercial Appeal* may be found at <http://www.commercialappeal.com/news/2008/jul/22/police-director-sues-find-identity-blogger-critical/>

FCC CHAIRMAN CRACKS DOWN ON COMCAST RESTRICTING P2P USERS

On July 11th, Federal Communications Commission (FCC) Chairman Kevin Martin stated that he will recommend sanctions against Comcast for unreasonably restricting customers who use peer-to-peer (P2P) file sharing. The sanction would not be a fine, but would force Comcast to stop its current practices, report to the FCC on how the practice was used, and inform Comcast customers of any future practices. At the FCC's August 1st meeting, Martin plans to propose that the five FCC commissioners vote to uphold a complaint stating that Comcast violated open Internet principles by blocking peer-to-peer traffic. Martin believes that Comcast's practices violate FCC rules because they were not narrowly tailored to serve a legitimate traffic management goal, and Comcast customers were not informed of the practice. Comcast maintains that it never had such a practice, and argued that the FCC did not have the authority to enforce its open Internet policy. The full story may be found at <http://ap.google.com/article/ALeqM5huAOgy6g1S5wW-7ft0FRulypdzLQD91RTNTO2>

VERIZON SETTLES EARLY TERMINATION LAWSUIT FOR \$21 MILLION

On July 10th, news sources reported that Verizon settled its early termination fee lawsuit in California for \$21 million. The result came in response to many consumer complaints about high early termination fees being a marketing tool to keep customers with a specific provider. FCC Chairman Kevin Martin expressed concern over the fees at a hearing in June. Subsequently, other providers such as AT&T began to reduce early termination fees, although service providers have defended the fees as being necessary to recover costs. Details of the settlement are not public because they had to be approved by a judge. The full story may be found at http://www.informationweek.com/news/telecom/regulation/showArticle.jhtml?article_ID=208808431

PRESIDENT BUSH SIGNS GOVERNMENT WIRETAPPING BILL

On July 10th, President Bush signed into law H.R. 6304, the amendments to the Foreign Intelligence Surveillance Act. The law includes a provision that grants immunity for telecommunications companies involved in government wiretapping, the most controversial aspect of the law that caused delay in Congress. The controversial bill also gives President Bush the authority to wiretap without a search warrant. Bush praised the bill as one that will protect Americans and prevent further attacks on the country, but civil liberties advocates strongly disagreed. The American Civil Liberties Union filed suit against the law the same day it was signed, claiming it violates both the First and Fourth Amendments. The full text of the legislation may be found by searching for bill number H.R. 6304 at <http://thomas.loc.gov>

3RD CIRCUIT HOLDS CHILD ONLINE PROTECTION ACT UNCONSTITUTIONAL

On July 22nd, the United States Court of Appeals for the Third Circuit ruled that the Child Online Protection Act (COPA) was unconstitutional. According to the court's opinion, COPA was enacted to protect children from offensive materials on the Internet by providing jail time for anyone who posts material that is offensive to children online. The law had not taken effect because the American Civil Liberties Union challenged the 1998 law on behalf of a coalition of writers, artists, health educators, and publishers because it claimed the law unconstitutionally restricted freedom of speech online. The appeals court affirmed a district court decision that held COPA was unconstitutional because COPA was not narrowly tailored to promote the government purpose of keeping offensive materials off the Internet, there were less restrictive alternatives to COPA, such as parental controls and filtering technologies, and because COPA is impermissibly overly broad and vague. The case is *ACLU v. Mukasey*, and the full opinion may be found at http://www.aclu.org/pdfs/freespeech/copa_20080722.pdf

PIRACY REPORT REVEALS STATES WITH MOST SOFTWARE PIRATES

On July 16th, the Business Software Alliance (BSA), a firm dedicated to preventing software piracy, announced the results of its 2007 State Piracy Report. The report found that while the United States had the lowest piracy rates throughout the globe, it still does not fully combat piracy. The report was the first to look at piracy rates within each individual state in the United States, and found that six states - California, Florida, Illinois, New York, Ohio and Texas - made up \$3.93 billion in pirated software losses, almost half of the \$8.04 billion in national losses from pirated software last year. The study also assessed the tax revenue losses caused by pirated software to state and local governments, and found \$1.7 billion in revenue was lost from the illegal sales. One encouraging sign was that U.S. software piracy was down to 20% in 2007, a 2% decrease since 2003. The report may be found at http://www.bsa.org/country/Research%20and%20Statistics/%7E/media/Files/statestud_y07/statestudy07.ashx

MYSPACE BULLYING MOTHER SEEKS TO HAVE CHARGES DISMISSED

On July 23rd, lawyers for Missouri mother Lori Drew filed a motion to dismiss the charges against her for creating a fake MySpace profile. The profile posed as a teenage boy and courted Megan Meier, who then committed suicide when the boy broke up with her. The motion claimed that though the fake profile violates MySpace policy, the action is not illegal. Prosecutors charged Drew with accessing a computer without authorization under a statute generally used to prosecute hackers and identity thieves. The charges were the first of their kind, and raise issues of whether an online social networking site will serve as lawmakers, and whether anyone who violates the terms of use on these websites could be liable. A *Wall Street Journal* blog post, with links to the three motions to dismiss, may be found at <http://blogs.wsj.com/law/2008/07/23/lori-drews-lawyer-moves-to-dismiss-indictment-in-myspace-suicide-case/>

CYBERSECURITY LARGE PORTION OF 2009 BUDGET

On July 21st, the House Select Committee on Intelligence released a report that revealed that the largest portion of the new budget would go to the Comprehensive National Cybersecurity Initiative. The details of the plan remain vague, but the massive program would gear up to secure government computer systems against intrusions, prepare for future threats, and to secure vital infrastructure data. The House Committee report indicated that the privacy concerns of private citizens would be protected, a major concern of privacy advocates since the initiative was announced. The committee recommended a committee made up of lawmakers, executive branch officials, and private sector representatives to oversee the intelligence community's implementation of the program. If implemented, the oversight committee would be a unique partnership between the public and private sectors. The House Select Committee on Intelligence report on the cybersecurity bill may be found at <http://intelligence.house.gov/Media/PDFS/IAAFY09.pdf>

NEW COURT CASE ANOTHER EXAMPLE OF E-DISCOVERY DISASTER

On June 23rd, U.S. District Judge Janet C. Hall for the District of Connecticut awarded default judgment in favor of the plaintiffs in the case of *Southern New England Telephone Company ("SNET") v. Global NAPS, Inc.* for various e-discovery blunders made by the defendants throughout the discovery process. The default judgment came after defendants refused to comply with discovery requests, including denying that documents existed and using computer software to erase relevant documents before the computer was examined by computer forensics experts. Conrad Jacoby explains in his e-discovery column the lessons that may be learned from the bad example set by the Global NAPS, Inc. The first lesson is not to underestimate computer forensics, because though Global tried to destroy documents by wiping them off the computer, computer forensics experts could determine how and when the documents had been wiped, along with what documents had been wiped by viewing metadata backed up in the Windows system. Other lessons Jacoby took away from the case are that computer forensics should be considered bipartisan experts, and that even the best lawyer cannot get a party out of its own e-discovery blunders. Jacoby's article may be found at <http://www.llrx.com/columns/ediscoverydisaster.htm>

The Southern New England Telephone Company decision may be found at

http://www.electronicdiscoveryblog.com/cases/new_england_tel.pdf

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

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