



Issue 130 March 2008

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

SIX LAWYERS SANCTIONED FOR INCOMPLETE E-DISCOVERY SEARCHES

On January 7th, in the United States District Court for the Southern District of California, Magistrate Judge Barbara Major issued an order that sanctioned and referred six attorneys to the California Bar because electronic discovery was not conducted properly. In the case of *Qualcomm Inc. v. Broadcom Corp.*, the judge found that the lawyers had failed to conduct a routine search of client e-mail. After the jury returned a verdict, Qualcomm's new attorneys found 46,000 more responsive documents. The attorneys located the documents by searching the e-mail archives of Qualcomm employees, something that, according to Major, should have been a routine search. Had the search been conducted, it was likely the case never would have gone to trial. Major further found that failing to conduct the search was the equivalent of intentionally withholding documents. The sanction imposed was \$8,568,633; the total cost of Broadcom's legal fees. Since the trial judge had already awarded that amount in damages, no additional sanction was imposed. But if Qualcomm got a reversal on the merits, but not on the discovery abuse counts, the sanction would still stand. No further monetary sanctions were imposed because Major was unsure of her own authority to impose sanctions, so she also referred the attorneys to the California Bar and ordered the preparation of a document analyzing where the entire discovery process had gone wrong. The full order may be found at

http://www.klgates.com/files/upload/eDAT_Qualcomm_Jan_7_2008_Order.pdf

MICROSOFT'S \$44.6 BILLION BID FOR YAHOO REJECTED

On February 1st, Microsoft announced it was willing to pay \$31 per share to acquire Yahoo!, which was 62% above the market closing price of \$19.18 on January 31st. Microsoft put forth a blunt proposition to Yahoo! shareholders in a letter explaining the situation and why they would benefit from the merger. Microsoft claimed the merger would allow both companies to compete in the online search and advertising market, both of which are currently dominated by Google. On February 11th, Yahoo! rejected Microsoft's offer, saying that it undervalued the company and was not in the shareholders' best interest. Microsoft responded by saying the fight was not over, and it would continue to try to acquire Yahoo!. Analysts said Microsoft had a few options: it could bid higher, try to buy the stock from shareholders directly, or try to take over Yahoo!'s board of directors. As of February 19th, Microsoft had not given any indication it would bid higher, but had hired a proxy solicitation firm to help oust Yahoo!'s board of directors, all of whom are up for re-election.

The initial Microsoft press release and letter to Yahoo!'s shareholders may be found at <http://www.microsoft.com/presspass/press/2008/feb08/02-01CorpNewsPR.msp>

Yahoo!'s response letter to its shareholders may be found at <http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=294288>

Microsoft's response to Yahoo!'s rejection may be found at

<http://www.microsoft.com/presspass/press/2008/feb08/02-11msft-response.msp>

JUDGE RULES MICROSOFT SUBJECT TO SCRUTINY UNTIL 2009

On January 29th, in the United States District Court for the District of Columbia, Judge Colleen Kollar-Kelly ruled that court supervision of Microsoft's compliance with the requirements of an antitrust settlement would continue until November 12, 2009. The ruling was a response to filings by ten states pushing to extend oversight until 2012. Kollar-Kelly noted that the decision should not be viewed as a sanction against Microsoft, but the decision came because some technical documentation the court required had not been made available in readily useable form. The ruling was meant to give Microsoft time to make the documents available in readily useable form. The information would make it easier for other software makers to make products that work well with the Windows operating systems. The full opinion may be found at https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?1998cv1233-682

DISTRICT JUDGE SLAMS SPAMMERS FOR VIOLATION OF FTC ACT

On February 4th, in the United States District Court for the Northern District of Illinois, Judge David H. Coar ordered Sili Neutraceuticals and Brian McDaid to stop sending illegal spam and misrepresenting products. Coar also ordered the company and McDaid to pay \$2.5 million for violating the FTC Act and CAN-SPAM Act. The FTC Act violations stemmed from the company misrepresenting that products caused weight loss or slowed the aging process. The CAN-SPAM Act violations were for transmitting this information through unwanted e-mails to protected computers. The defendants sent out the spam e-mails, which then directed consumers to the defendant's website where they could buy the product. The FTC press release may be found at <http://www.ftc.gov/opa/2008/02/sili.shtm>

The full opinion may be found at <http://www.ftc.gov/os/caselist/0723124/080123silidefaultjdgmnt.pdf>

FTC OFFERS INFORMATION ON PROTECTING COMPUTERS FROM MALWARE

On January 31st, the Federal Trade Commission announced that tips on how to protect your computer from malware are available on the OnGuard Online website. The FTC warned that criminals have come up with creative ways to get malware on your computer. Malware is short for malicious software, and criminals could use it to steal your personal information, send spam or commit fraud. The FTC explained that it is very important that consumers protect themselves from this risk. The full tips on malware protection may be found at <http://www.onguardonline.gov/malware.html>

IRS WARNS OF IDENTITY THEFT SCAMS USING ITS NAME

On January 30th, the Internal Revenue Service warned taxpayers to beware of phone or e-mail scams using the IRS name, especially those concerning advance payment checks. The government is considering an advance payment check program, but has not yet adopted one, so any contact about advance payment checks would likely be a scam. The scammers are looking to steal personal information to commit identity theft. Both Sensei principals have received these phishing e-mails. Some of the scams the IRS encountered were rebate phone calls, refund e-mails, audit e-mails, changes to tax law e-mails, and paper check phone calls. The IRS stated that it does not contact taxpayers by phone or e-mail about any of this information. The IRS cautioned taxpayers to access the IRS website only by typing in IRS.gov, and not through clicking on any external links. More detail about the types of scams and how to respond may be found at <http://www.irs.gov/newsroom/article/0,,id=178061,00.html>

HEALTH INSURER HAD LAPTOP WITH PERSONAL DATA STOLEN

Horizon Blue Cross Blue Shield of New Jersey announced that an employee laptop was stolen on January 5th. The laptop contained the personal information of 300,000 individuals, including Social Security numbers, but not including any medical information. The company sent letters to the affected individuals informing them of the theft, and offered free credit monitoring for one year. The company claimed it was unlikely that any data was stolen, because the computer was password protected and a security feature was initiated on January 28th that destroyed the data on the stolen laptop. The press release from Horizon may be found at <http://www.horizon->

bcbsnj.com/newsroom_pop.asp?id=5

HOUSE AND SENATE BATTLE OVER TELECOM IMMUNITY

On January 29th, Congress voted to extend the controversial Protect America Act for another fifteen days, as it was set to expire February 1. The House passed the 15-day extension, and there was some question as to whether the Senate would pass it as well. The Senate eventually ended up passing the measure by voice vote, with some coaxing by Senate Majority leader Harry Reid. The major issue with Congress was whether the new legislation gets telecom companies out of past lawsuits alleging illegal cooperation with government spy agencies. President Bush signed the extension on January 31st. After passing the extension, on February 12th, the Senate voted 31 to 67 against a Democrat sponsored amendment that would allow the telecom lawsuits to continue. On February 13th, the House refused to extend the Protect America Act in its current form which would halt the lawsuits. Whether the bill would ultimately pass was up in the air.

The full story on the first extension may be found at http://www.news.com/8301-10784_3-9860581-7.html

The rejected Senate Amendment may be found at <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:SP03907>:

The House vote and legislation may be found at <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.05349>:

PRESIDENT BUSH SIGNS DIRECTIVE TO MONITOR FEDERAL COMPUTER SYSTEMS

On January 8th, President Bush signed a classified directive that would give expanded power to intelligence agencies to monitor Internet traffic. The directive would give expanded power to intelligence agencies to monitor federal agency computer networks. The directive was intended to protect federal agencies from cyber attacks, as there previously were attacks on computer networks at the State, Commerce, Defense and Homeland Security Departments. Critics expressed concerns about increasing power of intelligence agencies in a way that could result in privacy concerns. The full Washington Post article may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html>

EU COURT RULES COUNTRIES CAN REFUSE TO IDENTIFY FILE SHARERS

On January 29th, the European Union Court of Justice ruled that its member countries did not have to disclose the names of file sharers on the Internet in civil cases. The case involved a dispute between Promusicae, a Spanish music rights holders association, and Telefonica, a Spanish telecommunications operator. Telefonica claimed that under EU rules, it only had to disclose file sharers names under criminal actions, and not for civil actions. The issue balanced intellectual property rights with users' right to privacy, with the right to privacy tipping the scales. The court said EU rules did not prohibit a country from requiring a telecommunications firm to provide user data, but it did not compel them to do so either. The EU press release may be found at <http://curia.europa.eu/en/actu/communiqués/cp08/aff/cp080005en.pdf>

EIGHTH CIRCUIT UPHOLDS CHILD PORNOGRAPHY CONVICTION

On January 17th, the United States Court of Appeals for the Eighth Circuit upheld the conviction of a man downloading and sharing files containing child pornography using Kazaa, a peer-to-peer (P2P) file sharing program. At issue was a federal statute intended to stifle child porn advertising by imposing a mandatory 15-year prison term to anyone who offered to distribute child porn across state lines. The Defendant was the first to be prosecuted under an innovative use of the statute that argued the defendant was in effect advertising with his Kazaa use. The defense argued that what his client did was not advertising, but conceded that his client was guilty of distributing child pornography, which usually has the lesser sentence of 5 years. The court disagreed and found that the descriptive fields on Kazaa let other users know they could download the illegal materials from the Defendant. The Defendant stated that he planned to appeal the decision to the Supreme Court.

The full Eighth Circuit decision may be found at <http://blog.wired.com/27bstroke6/files/kazaasmut.pdf>

HOW TO HOLD ON TO XP

On January 28th, InfoWorld published an article letting users and businesses know how to get Microsoft XP licenses past the deadline of June 30th, when Microsoft said that no more shrink-wrapped XP licenses would be available for order. The article explained how to keep XP for various types of users. For retail licenses, the only option was to stock up before the deadline, and chances are these will sell out quickly. For OEM licenses, enterprise licenses, and subscription licenses, the options were more complicated. Organizations can keep using existing XP licenses indefinitely, even after no new licenses are available, but Microsoft will stop technical support and updates beginning in mid-2009. The full article may be found at http://www.infoworld.com/article/08/01/28/04NF-save-xp-license_1.html

NY BILL WOULD KEEP SEX OFFENDERS OFF SOCIAL NETWORKING SITES

On January 29th, New York Attorney General Cuomo announced new legislation introduced in the New York legislature, entitled the Electronic Security and Targeting of Online Predators Act (e-STOP), which is designed to protect children from the many hazards on the Internet. The bill would require all convicted sexual predators to submit their online identifiers such as e-mail addresses or instant messaging screen names to the state. The state would then pass the information on to social networking sites, which could then block those users from the site. Also, predators that committed the highest level crime or used the Internet to commit the crime would be subject to severe restrictions on their ability to use the Internet at all. Advocates of the bill explained that this legislation would be a new way to protect children in the ever-changing information age. The Attorney General's press release may be found at http://www.oag.state.ny.us/press/2008/jan/jan29a_08.html

FBI MOVING FORWARD WITH NEW IDENTIFICATION SYSTEM

On February 12th, the FBI announced that Lockheed Martin Transportation and Security Solutions was awarded a contract to develop the FBI's Next Generation Identification (NGI) System. The NGI will encompass the most traditional identifying technique, fingerprinting, along with new identification technologies such as palm printing, a scar and tattoo database, an iris eye pattern database, and a facial shape database. The FBI explained that the new system's necessity results from increased identity theft and security threats. The new program would not expand the number of people in the database, but would try to gather more accurate information for identifications. The FBI press release may be found at <http://www.fbi.gov/pressrel/pressrel08/ngicontract021208.htm>

MICROSOFT APPLIES FOR PATENT TO MONITOR WORKERS

On January 17th, the Patent Office posted a Microsoft patent application for a monitoring system that could link workers to their computers. The system could monitor worker's heart rates, body temperatures, movements, and blood pressure. Further, the system could pick up stress or frustration, and let the employer know the employee needed help. Commentators expressed their concern about privacy issues and worried that workers could be fired based on what the computer said they were doing. The full copy of the application may be found at <http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnethtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%2220070300174%22.PGNR.&OS=DN/20070300174&RS=DN/20070300174>

CALIFORNIA COURT PROTECTS CHAT ROOM CRITIC'S IDENTITY

On February 6th, the Sixth Appellate District for the California Court of Appeal ruled that a chat room user who posted scathing remarks about the executives of a Florida company could remain anonymous. One of the executives brought a defamation lawsuit against the users, and applied for a subpoena for Yahoo! to turn over the real names of the online critics. The court stated in its ruling

that while the remarks made by the user on the message board were offensive, they were not assertions of fact, therefore the executive had no recourse under Florida defamation law. A copy of the full ruling may be found at <http://www.courtinfo.ca.gov/opinions/documents/H030767.PDF>

MICROSOFT HELPS PUT AWAY PIRACY RING

On December 31st, a court in Taiwan handed down a four-year prison sentence for the ringleader in an operation that pirated more than \$900 million in Microsoft products. The sentence was the longest that had been given in Taiwan in that type of crime. Microsoft assisted in the global investigation. The investigation was global because the pirated products were sold in seven different languages, and twenty-two known countries. The investigation took six years, and resulted in the elimination of a counterfeiting ring that accounted for about 90% of the fake Microsoft products on the market. The full Microsoft press release may be found at http://www.microsoft.com/presspass/press/2008/feb08/02-04TaiwanConvictionsPR.msp_x

HOUSE PASSES ANTI-PIRACY RULES FOR COLLEGES

On Thursday, February 7th, the House of Representatives passed the College Opportunity and Affordability Act, which contained provisions that would force colleges to deal with privacy concerns. The provisions stated that colleges should make plans to provide alternative legal downloading, such as subscription based services or should make other plans to deter illegal downloading. Critics of the provision stated that it would be overly burdensome on colleges and could result in loss of funds. The Motion Picture Association of America and the American Federation of Musicians expressed their approval of the provisions. It was also unclear whether the provision would remain in the bill when the House and Senate reconcile differences in the bill. The full text of the legislation may be found by searching for H.R. 4137 at <http://thomas.loc.gov>

SYMANTEC REPORTS EUROPE TOP SOURCE OF SPAM

In its February "State of Spam" report, Symantec found that spam was originating in Europe more than most folks had supposed. For the third month in a row, the amount of spam coming from Europe was greater than that coming from the United States. The report attributed the trend to the increase in broadband users in Europe. The full report may be found at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Symantec_Spam_Report_-_February_2008.pdf

PROJECT TRACKS ONLINE CHILD PROTECTION LEGISLATION

On February 6th, a joint project was released from the Center for Democracy & Technology and the Progress and Freedom Foundation that tracked federal legislation to protect children online. The organizations were concerned with the effect of the legislation on First Amendment freedom of speech rights. The organizations combined efforts on a bill tracking report, and each issued a separate analysis of the bills. The bill tracking report may be found at <http://www.cdt.org/speech/110thSafetyContentBillsCDT-PFF.pdf>

The Center for Democracy and Technology analysis may be found at <http://www.cdt.org/speech/20080206freespeechincongress.pdf>

The Progress and Freedom Foundation analysis may be found at <http://pff.org/issues-pubs/ps/2008/ps4.4childprotection.html>

MYSPACE WINS DOMAIN NAME FIGHT IN THE UNITED KINGDOM

On January 31st, independent expert Antony Gold awarded MySpace use of the domain name MySpace.co.uk. Another company, Total Web Solutions (TWS), had registered the domain name before MySpace was around, but once the social networking site was launched, TWS used the address to offer services to other websites. Gold found TWS was exploiting MySpace's popularity

and profiting unjustly from use of the domain name. The full ruling may be found at http://www.nic.uk/digitalAssets/27270_myspace.pdf

SENATORS INTRODUCE ANTI-ROBOCALL LEGISLATION

On February 12th, Senators Dianne Feinstein, Daniel Inouye, and Arlen Specter introduced a bill on the Senate floor to control the amount of political "robocalls" received by Americans. The legislation defined "political robocalls" as computer generated phone calls that promote or oppose a candidate for political office. The rules would limit the calls in the following ways: no calls may be made between 9p.m. and 8 a.m., only two calls may be made to the same number in one day, the identity of the "robocall" cannot be hidden on caller ID and the calls must say that it is recorded and who it is from. Further, the law would only apply to candidates running for federal office, and would be limited to time periods leading up to an election. The full text of the legislation may be found by searching for S. 2624 at <http://www.thomas.gov>

JUDGE SAYS MYSPACE FRIEND REQUEST VIOLATED RESTRAINING ORDER

New York Judge Matthew A. Sciarrino ruled that a teen violated a restraining order when she submitted friend requests to the three protected parties. The teen was charged with three counts of second-degree criminal contempt. She applied for a motion to dismiss, which was denied by Judge Sciarrino. The judge explained that the restraining order provided for no contact between the teen and the protected parties. Even though the protected parties could reject the friend requests, the teen still made indirect contact through the MySpace e-mails, which was prohibited under the restraining order. The full New York Law Journal article may be found at <http://www.law.com/jsp/article.jsp?id=1202904867035>

SIIA FILES NINE LAWSUITS AGAINST ILLEGAL SOFTWARE SELLERS ON EBAY

On February 13th, the Software & Information Industry Association (SIIA) announced that it had filed nine lawsuits against software sellers on eBay. The suits were filed in the U.S. District Court for the Northern District of California, and charged residents of California, Texas, Washington, and Illinois of knowingly selling illegal copies of Adobe and Symantec software on eBay. The SIIA stated it wanted to send a message to sellers of illegal software that their conduct is illegal and they will be prosecuted for it. The lawsuits were filed as part of the SIIA's Auction Litigation Program that explains the dangers of pirated software for both the buyer and the seller, and gives buyers an incentive to report the illegal software. The full press release from the SIIA may be found at http://www.sii.net/press/releases/ALP-Nine_Suits_Filed_2-08.pdf

LAWSUIT SEEKS INFORMATION ON GOVERNMENT BORDER SEARCHES

On February 7th, the Electronic Frontier Foundation and the Asian Law Caucus filed suit against the Department of Homeland Security for failing to provide information about border searches of U.S. citizens. The lawsuit was filed under the Freedom of Information Act (FOIA) in response to members' complaints about lengthy interrogations at the border. Aside from asking questions, the members also complained about laptop computer and cell phone searches that sometimes resulted in the information being copied. The two agencies filed suit after an initial FOIA request did not garner a response. A copy of the full complaint may be found at <http://www.eff.org/files/filenode/alc/alc-complaint.pdf>

BLACKBERRY BLACKOUT LEAVES USERS WITHOUT DATA FUNCTIONS

On February 11th, for a few afternoon hours, BlackBerry users were unable to check their e-mail. Research In Motion (RIM), the maker of the BlackBerry, stated that the outage was due to a malfunction in a recently updated server. RIM apologized for the inconvenience and said it is committed to making sure all users continue to have reliable service. Meanwhile, people dependent on their BlackBerry were forced to go without checking their e-mail or surfing the Internet on it for a few hours until service was restored in the early evening. The full story may be found at <http://afp.google.com/article/ALeqM5gOXmpqRWVNJ9P8eXTwwaHow8z5wg>

PRINCETON RESEARCHERS DISCOVER HOW TO STEAL ENCRYPTED DATA

On February 21st, researchers at Princeton University announced that they had discovered a new vulnerability in the dynamic random access (DRAM) chip found in computers, which is commonly known as computer memory. Experts previously believed that the data was lost when the computer was turned off. The Princeton team discovered that the data actually fades out over a period of time ranging from seconds to minutes. This was significant because, according to the research team's blog post, this would enable an attacker "to read the full contents of memory by cutting power and then rebooting into a malicious operating system." Further, the research found if the DRAM chips are cooled, they retain the data for much longer. The research website with background information may be found at <http://citp.princeton.edu/memory/>

The full report may be found at <http://citp.princeton.edu.nyud.net/pub/coldboot.pdf>

MICROSOFT FINED 1.3 BILLION BY EU FOR ANTITRUST VIOLATIONS

On February 27th, the European Union Antitrust Commission fined Microsoft a record \$1.3 billion for failing to comply with a previous EU order. In 2004, the EU found that Microsoft overcharged its rivals for software information to help the rivals develop products compatible with the Windows operating system. The EU commission found that until last October, when Microsoft lowered the rates it charged other companies on its patents, the company was still overcharging its competitors for access to its patents. The fine is notable for two reasons: it is the largest fine ever handed out by the EU and the first handed out for violation of an antitrust order. The full EU press release may be found at <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/318&format=HTML&aged=0&language=EN&guiLanguage=en>

"*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.