



Issue 134
July 2008

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

JUDGE RULES PRIVILEGE WAIVED ON DISCLOSED ELECTRONIC DOCUMENTS

On May 29th, Magistrate Judge Paul W. Grimm of the U.S. District Court for the District of Maryland ruled that privilege was waived when defendants disclosed 165 electronic documents to the plaintiff. The case was a copyright infringement suit, and defendants turned over the documents as part of discovery after using keyword searches to identify privileged documents. The court found that because defendants did not demonstrate that their search was reasonable, defendants had waived privilege by disclosing the documents. The court stated that defendants could have showed reasonableness if they had stated why certain keywords were chosen, what the search was supposed to accomplish, and how the search protected against disclosure of privileged materials. In his opinion, Grimm emphasized the problems with keyword searches, including the risk of under-inclusive or over-inclusive terms resulting in privileged information being disclosed, and non-privileged information not being disclosed. These problems demonstrated why the party performing the search needs to present a rationale for the method chosen, show that the search was appropriate for the task, and show that it was properly implemented. The court also explained how to adequately assert privilege under the Federal Rules of Civil Procedure. Grimm explained that the reasons for claiming privilege must be laid out in a privilege log, and that disputes would be settled by an in-camera review of the documents by the courts. The case is *Victor Stanley Inc., v. Creative Pipe Inc.*, and the full opinion may be found at

<http://www.mdd.uscourts.gov/Opinions/Opinions/VictorStanley052908.pdf>

ACROBAT RELEASES NEW VERSION WITH FEATURES FOR LAWYERS

On June 2nd, Adobe announced that Adobe Acrobat 9 will be released in July, and that it includes new features specifically for lawyers. The features include enhanced redaction and bates numbering, file splitting, PDF Portfolios that allow lawyers to assemble multiple media types, more powerful document comparison, and the ability to directly embed Flash files for playing in Acrobat. In addition, Adobe also unveiled Adobe.com, a new online service that allows users to create and upload documents, convert documents to PDF, and hold free 3-person web conferences. The full Adobe blog post unveiling the new features may be found at

http://blogs.adobe.com/acrolaw/2008/06/acrobat_9_announced_new_features.html

W.V. LAWYER SUSPENDED FOR E-MAIL INTRUSION

On May 23rd, the West Virginia Court of Appeals sanctioned an attorney to a two-year suspension of his license for accessing the e-mail account of his wife, an attorney at another law firm. Michael Markins looked at the e-mail to see if his wife was having an affair. Once Markins figured out how easy it was to break into the password system for the e-mail, he accessed the e-mail accounts of eight other attorneys on almost a daily basis, and did not stop until he was about to be caught by the firm's computer experts. In addition to reading confidential e-mails, Markins's firm was also engaged in a massive tort suit with his wife's firm, though the opinion stated that no information relating to the case had been compromised. The court stated that though there was no evidence the information had been misused, the court imposed a sanction as a deterrent to others. The full opinion may be found at <http://www.state.wv.us/wvsca/docs/Spring08/33256.htm>

XEROX SURVEYS LEGAL PROFESSIONALS ON E-DISCOVERY

On June 2nd, Xerox announced the results of its survey of legal professionals on their views of

electronic discovery. The survey found that 95% of participants had faith in their company's ability to handle e-discovery, but only 29% of participants felt that they themselves were "extremely prepared" to handle e-discovery. The survey asked over 200 legal professionals about their e-discovery problems, which included slow turnaround, inadequate system support, lack of important features, and IT department inability to deal with the document review system. The participants answered that there were some benefits to outsourcing the e-discovery process, including cost effectiveness and decreased processing time. Xerox's Vice President for Litigation Services, Craig Freeman, offered advice to firms dealing with the e-discovery process, mainly to have a litigation plan and to seek advice when encountering an e-discovery problem. The full Xerox press release may be found at http://www.xerox.com/go/xrx/template/inv_rel_newsroom.jsp?app=Newsroom&ed_name=NR_2008June2_Xerox_Litigation_Services_e-discovery_survey&format=article &view=newsrelease&Xcntry=USA&Xlang=en_US

'SUPER POWERED' WEBSITES PERFORM INNOVATIVE FUNCTIONS

On May 19th, *Law Technology News* reported about three new web functions that allow users to have a superhuman memory, a visual search engine, and to communicate from beyond the grave. The first web function described was EverNote, which allows a person to store all notes and clips in a perpetual scrolling window. EverNote recently released its version 3.0, which allows you to synchronize notes across your desktop, online, and on a mobile phone. The second web program was entitled Searchme, a new site that delivers image results of each responsive webpage instead of text results. The third program was entitled iGoodbye, which keeps personal information such as passwords, assets or financial accounts private until after death. Once the person dies, the information is released with a valid death certificate so loved ones can access the accounts more easily. More information about the programs may be found at <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202421467321>

SOFTWARE UPDATE CAUSES NUCLEAR POWER PLANT SHUTDOWN

On June 5th, the *Washington Post* reported that a nuclear power plant in Georgia was on emergency shutdown March 7th for 48 hours after a routine software update was installed on a plant computer. The update was supposed to synchronize data on the plant's primary control systems, but when the computer restarted as part of the update, it reset the data on the system. The automated safety system then interpreted the lack of data as a drop in water that cooled the plant's nuclear fuel rods, and shut down the plant as a safety measure. A spokeswoman for Southern Company, who performed the software update, stated that the plant reacted normally under its emergency protocol, and at no time was the plant in jeopardy. The incident triggered concerns about the vulnerability of nuclear power plants to cyber attacks. The full story may be found at http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958_pf.html

AMAZON BEGINS TO COLLECT SALES TAX IN NY DESPITE LAWSUIT

On June 2nd, the *New York Times* blog reported that Amazon.com and other online retailers had started to collect taxes on goods shipped to New York, as required under a recently passed New York law. According to the blog, the law provides an incentive for companies to start collecting the tax, because if they started collecting by June 1st, they will not have to pay any retroactive taxes for sales before the law was passed. In response, Amazon decided to collect the tax and forego the possibility of having to pay retroactive tax, and filed suit over the law. Another option would have been to cut off all New York affiliates, which is what online retailer Overstock.com did, along with filing suit as well. The full blog post may be found at <http://bits.blogs.nytimes.com/2008/06/02/let-the-tax-collection-begin/>

FAKE ONLINE PROFILES CAUSE VICTIMS TO FILE LAWSUITS

On June 2nd, the *National Law Journal* reported an increasing number of lawsuits over fake online profiles on social networking sites such as Facebook and MySpace. Victims of the fake profiles are suing the creators, claiming defamation over derogatory comments or sexually offensive information

posted on the profiles. Victims that filed suit include a Texas assistant principal, an Indiana high school dean, and a Chicago town president. In the Indiana case, a judge ordered Facebook to turn over information to identify who set up the fake profile. The lawsuits raise First Amendment concerns, with some claiming that the fake profiles are protected speech, especially if they are parody, satire or criticism. But people on the other side explain that not all speech is protected, and do not consider fake online profiles protected speech. The debate sparks interesting questions, and the full article may be found at <http://www.law.com/jsp/article.jsp?id=1202421864062>

COMCAST, TIME WARNER TESTING NEW PRICING FOR HEAVY INTERNET USERS

On June 4th, the *Washington Post* reported that Comcast and Time Warner Cable would be testing new approaches to charge heavy Internet users higher rates for Internet service. Comcast is testing its scheme in Chambersburg, Pa., and Warrenton, Va., by delaying traffic for its heaviest Internet users. The FCC investigated Comcast for allegedly blocking users who used Bit Torrent sites, but Comcast promised that specific websites would not be targeted with the new plan. Time Warner Cable is using a metered billing test, which charges customers more for larger data volumes and faster Internet access. The scheme was compared to cell phone structures that charge a user for going over allotted minutes, and is being tested in Beaumont, Texas. The full story may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2008/06/03/AR2008060303248.html>

PRIVACY GROUPS URGE GOOGLE TO MAKE PRIVACY POLICY MORE VISIBLE

On June 3rd, privacy rights groups urged Google to place a link to its privacy policy on its home page, where the policy would be more visible. Google's privacy policy may be accessed through clicking on "About Google," which then links to the privacy policy. The groups claimed that Google was in violation of the California Online Privacy Protection Act, which requires a website that collects personal information to conspicuously post its privacy policy. The law defined "conspicuously posting" as on the home page or the first significant page after entering the site. Google commented that its privacy information was easily accessible to users, as Google has many ways to discover its privacy policies, including a YouTube channel. A news article with Google's comment may be found at http://news.cnet.com/8301-10784_3-9958252-7.html

The privacy rights organization letter sent to Google may be found at

<http://www.privacyrights.org/ar/Google-HomePage-Alert-080603.htm>

VERIZON TO OFFER TOOLS TO IMPROVE CHILD SAFETY ONLINE

On June 3rd, Verizon Communications chairman and CEO Ivan Seidenberg spoke at WiredSafety's Stop Cyberbullying Conference. Seidenberg explained that Verizon broadband customers will have free access to parental controls. The controls will give parents the ability to block certain content they do not want their children to see, block software through an applications filter, and limit how much time their child spends online. At the conference, Seidenberg also received WiredSafety's Internet Superhero Award for his commitment to Internet safety. A webcast of Seidenberg's speech may be found at http://72.32.208.177/webcast/prcast/verizon_CEO.htm

GOOGLE FILES MOTION TO DISMISS IN STREET VIEW CASE

On May 30th, InformationWeek reported that Google filed a motion to dismiss in a lawsuit by a Pennsylvania couple that claims Google's Street View violated their privacy. Google countered the invasion of privacy claim by stating that the couple's property is not private under the law, as it is customary for people to drive on another driveway to get home. Further, the couple did not give any indication that their property was protected through fencing, guard dogs, or 'keep out' signs. Google also pointed out that the couple brought themselves into the public eye with the lawsuit, as they did not seal their complaint, placed their address in the complaint, and did not ask Google to remove the images before filing suit. The full story may be found at <http://www.informationweek.com/news/internet/google/showArticle.jhtml?articleID=208401206>

SUPREME COURT LIMITS ABILITY TO COLLECT MULTIPLE ROYALTIES ON PATENTS

On June 9th, the U.S. Supreme Court, in a unanimous decision entitled *Quanta Computer v. LG Electronics*, the court limited the rights a patent holder has after the first sale of its patent. The court upheld the "patent exhaustion doctrine," which provides that a sale of a patented item ends all patent rights for that item. The case concerned control over purchasers of Intel Corp. components. LG claimed that Quanta used Intel parts in combination with non-Intel parts, in violation of an LG patent agreement. LG sued for patent infringement, and won in the U.S. District Court for the Federal Circuit, which held the patent exhaustion doctrine did not apply to "method" patents such as LG's. The Supreme Court instead held that the patent exhaustion doctrine applies to method patents, because if the Circuit Court decision stood, patentees would get around the patent exhaustion doctrine simply by calling patents method patents. The Supreme Court found that this would result in downstream purchasers being liable for patent infringement. The full decision may be found at <http://www.supremecourt.gov/opinions/07pdf/06-937.pdf>

JUDGE SUSPENDS TRIAL AFTER EXPLICIT IMAGES FOUND ON HIS WEBSITE

On June 12th, the L.A. Times reported that Chief Judge for the 9th Circuit Court of Appeals, Alex Kozinski's website contained explicit images that were accessible to the public. The site was maintained on Kozinski's home server, and was meant to be accessible only by viewers who knew a special address for the site. The site was shut down shortly after the story broke. Kozinski maintained that he did not believe that the images were publicly accessible, and thought they were there for his own personal use. The story caused Kozinski to grant a 48-hour stay in an obscenity trial that would have had jurors watching hours of explicit footage. After the stay was up, Kozinski recused himself from the obscenity case, and asked an ethics panel to investigate his conduct concerning the matter. The full story may be found at <http://www.latimes.com/news/nationworld/la-me-kozinski12-2008jun12,0,277290.stor y>

YAHOO REJECTS MICROSOFT FOR GOOD, COMBINES WITH GOOGLE IN ADVERTISING DEAL

On June 12th, Microsoft issued a brief statement saying that it had offered Yahoo a deal worth more than its original \$33 per share offer for the company. Microsoft further relayed that it was in talks for an alternative deal that was still under consideration. On the same day, Yahoo issued a statement that it was no longer in talks with Microsoft, and relayed that the alternate deal that was discussed was Microsoft purchasing Yahoo's search business. Yahoo concluded that selling its search business was not advisable. Yahoo also announced a strategic move to combine with Google in an advertising deal. Yahoo explained that it would run some Google advertisements alongside Yahoo search results, sealing a deal that had been speculated about for months. Yahoo assured shareholders that the combination with Google was the next best thing to a combination with Microsoft. Yahoo executives stated that it would strengthen Yahoo's position and capitalize on the growing online advertising market. The deal is nonexclusive, so Yahoo could make deals with other companies, and flexible terms allow Yahoo to choose what search terms the Google ads will appear by and what pages the ads will appear on. The payment comes from advertisers who will pay Google, and Google will then pay Yahoo a portion of the revenue. Though the plan does not require formal review by the Justice Department, Yahoo and Google agreed to delay the implementation of the plan 100 days for review. The Microsoft press release on Yahoo may be found at <http://www.microsoft.com/presspass/press/2008/jun08/06-12statement.mspx>

The Yahoo press release on ending talks with Microsoft may be found at <http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=316365>

The Yahoo press release on the Google ad deal may be found at <http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=316450>

N.Y. ATTORNEY GENERAL STATES ISPS WILL BLOCK CHILD PORNOGRAPHY SITES

On June 10th, New York Attorney General Andrew Cuomo announced that certain Internet Service

Providers would block sources of child pornography. According to the release, the ISPs will block sources by purging their servers of child porn websites identified by the National Center for Missing and Exploited Children. ISPs will also block access to child porn Newsgroups, a large supplier of the illegal images. Newsgroups are online message boards, accessed through ISPs, where users can upload and download files. New York's agreements with Time Warner, Verizon, and Sprint also include a provision where the three ISPs will implement a new system to respond to user complaints about child pornography more quickly, and will pay \$1.125 million collectively to help stop the spread of child pornography. The full press release from Attorney General Cuomo may be found at http://www.oag.state.ny.us/press/2008/june/june10a_08.html

ONLINE PHARMACY TO PAY FTC \$15.8 MILLION

On June 4th, U.S. District Judge Charles A. Pannell ruled that the Federal Trade Commission was entitled to \$15.8 million from online pharmacies for fraud claims associated with the drugs sold on the websites. The companies advertised through spam e-mails many fraudulent claims about their products, including that their products would cause miraculous weight loss, cure erectile dysfunction, not have any side effects, and were over 90 percent effective. The court found that the advertising claims of success with the drugs were false. The defense claimed that "puffery" of products in order to sell them was allowed, but Pannell disagreed, finding that "puffery" was no excuse for the misrepresentations presented by the online pharmacies. A National Law Journal article on the case may be found at <http://www.law.com/jsp/article.jsp?id=1202422192464>

HACKER GETS FIVE YEARS FOR DESTROYING DATA

On June 9th, the United States Attorneys Office in San Diego announced that Jon Paul Oson had been sentenced to over five years in prison on computer hacking charges, one of the longest sentences for hacking. Oson was employed as a network engineer by the Council of Community Health Clinics (CCC), and resigned after he received a negative performance review. Subsequently, Oson hacked into the CCC computer system and disabled the process that preserved patient data at one of the clinics. The jury also found that Oson deleted patient data and software. In addition to jail time, Oson's sentence also requires that he pay hundreds of thousands of dollars in restitution to the clinics. The full press release may be found at <http://www.usdoj.gov/usao/cas/press/cas80609-Oson.pdf>

NEW REPORTS LOOK AT CAUSES AND VICTIMS OF DATA BREACHES

On June 3rd, the Identity Theft Resource Center announced its study "The Aftermath 2007," which looked at the impact of identity theft on victims. The study found that financial crimes were reported by 78% of the respondents to the study, with 57% having fraudulent lines of credit issued in their names and 13% having their information used to obtain cable or Internet service wrongfully. Disturbingly, 62% of victims reported that the thief had committed a financial crime that led to a warrant issued in the victim's name. 82% of the victims learned of the crime through creditors or collection agencies. Only 10% of victims found out through their credit reports or other action. In another study looking at the causes of the data breaches, Verizon Business reported on the results of over 500 forensic investigations of data breaches. Verizon found that 9 out of 10 data breaches could have been prevented with appropriate security measures. Most of the data breaches were caused by outside sources, with only 18% of the breaches stemming from inside sources. Of those outside sources, business partners caused 39%. Also, most of the breaches were caused by multiple events, rather than one event. The full Verizon report may be found at <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>

The Identity Theft Resource Center study may be found at http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2007_20080529v2_1.pdf

CONGRESSMAN REPORTS CHINESE HACKED GOVERNMENT COMPUTERS

On June 11th, Representative Frank Wolf introduced a resolution on the House floor that called for greater protection of computers in the House of Representatives. Wolf issued the resolution in

response to discovering that four of his computers had been hacked by sources in China. Wolf stated that his computers were hacked after staff members researched human rights issues in China. Wolf also stated that other computers had been compromised in the House, and he worried that other computers were being hacked in Congress without members realizing it. The resolution and press release may be found at <http://wolf.house.gov/index.cfm?sectionid=34&parentid=6§iontree=6,34 &itemid=1174>

VA APPEALS COURT UPHOLDS LAW PROHIBITING SOLICITATION OF A MINOR

On June 10th, the Virginia Court of Appeals upheld the conviction of Dean Robert Podracky for solicitation of a minor for sex over the Internet. According to the opinion, Podracky solicited a sixteen-year-old girl over the Internet to come to a hotel and perform sexual acts with him. Podracky appealed his conviction claiming that the state law violated the First Amendment to free speech. The appeals court panel unanimously rejected Podracky's argument, and held that the First Amendment did not protect criminal solicitation. The full opinion may be found at <http://www.courts.state.va.us/opinions/opncavwp/0113071.pdf>

TSA TO REQUIRE ID ON ALL FLIGHTS FOR A SUPPOSED SAFETY INCREASE

On June 6th, the Transportation Security Administration announced that passengers would no longer be able to fly if they refuse to show ID. The new policy went into effect on June 21st, and applies only to passengers that refuse to show ID. The policy does not apply to those who claim to have lost or forgotten their ID. The new policy is a departure from the previous TSA policy that allowed passengers to fly without ID if they submitted to a more thorough secondary search. The TSA stated that the goal of the new policy was to increase safety, but critics were concerned that the measure would do the opposite. A concerned blogger stated that all a potential terrorist would have to do is lie about forgetting ID or present a fake ID to be let on a plane. The TSA press release may be found at http://www.tsa.gov/press/happenings/enhance_id_requirements.shtm

The full blog post may be found at http://news.cnet.com/8301-13739_3-9962760-46.html

FEDERAL JUDGE AFFIRMS RIGHT TO SELL USED SOFTWARE

On May 20th, U.S. District Judge Richard A. Jones of the Western District of Washington ruled that selling used software on eBay was not copyright infringement. In the case, Autodesk, a software company, sued Timothy Vernor, an eBay vendor who sold used copies of its software. Autodesk claimed that Vernor was violating its copyright protection because it only issued a license to purchasers of its software, therefore any resale of its software constituted copyright infringement. Vernor claimed that the sales were allowed under the First Sale Doctrine, which assures the right to re-sell used copies of copyrighted works. The court agreed with Vernor, and found that though Autodesk claimed that its sale was a license, the actual characteristics of the transaction made clear that it was a sale. On Autodesk's website there was no mention of the purchase being a license, and the sale requires a purchaser to pay a lump sum at the beginning of the transaction, with no further payments. The court found that these characteristics showed that Autodesk was selling, not licensing its product. The full opinion in Vernor v. Autodesk, Inc. may be found at <http://www.citizen.org/documents/vernorder.pdf>

SURVEY FINDS THAT 1/3 OF IT PROFESSIONALS SNOOP ON CO-WORKERS

On June 19th, information security company Cyber-Ark announced the results of a survey of 300 IT professionals. The survey found that 1/3 of those surveyed had secretly snooped to discover information such as co-workers salaries, e-mails or meeting minutes. Further, 47% of those surveyed said they had accessed information unrelated to their role at the company. The tool that was most used were administrative passwords, which are changed less frequently than user passwords. 30% of the passwords are changed quarterly, and 9% were never changed at all. The full Cyber-Ark press release may be found at http://www.cyber-ark.com/news-events/pr_20080619.asp

PAY THE PRICE IN MICHIGAN TO PRACTICE FORENSICS WITHOUT A LICENSE

On May 28th, Michigan Governor Jennifer Granholm signed Michigan House Bill 5274 into law, which makes it a felony to engage in computer forensics in Michigan unless the person is licensed as a private investigator in Michigan or falls under an exception. The punishment for violation is up to four years in prison and a \$25,000 fine. Exceptions include attorneys licensed in Michigan, and an employee acting within the scope of full time employment. Licensing requirements include three years experience, which can include a graduate degree in computer forensics, being employed by an investigator full time, or as an investigative reporter employed by a media outlet. The full legislation may be found at <http://www.legislature.mi.gov/documents/2007-2008/publicact/pdf/2008-PA-0146.pdf>

COURT RULES EMPLOYERS CANNOT READ TEXT MESSAGES WITHOUT CONSENT

On June 18th, the U.S. Court of Appeals for the 9th Circuit held that an employer has no right to read employees' text messages without their knowledge and consent. The court also held that a cell phone provider may not turn over the contents of the text messages to the employer under federal law. The case involved Jeff Quon, an officer in the Ontario County police department who exceeded the 25,000 character limit for text messaging. The department put employees on notice that their Internet and e-mail usage would be monitored, but did not notify the employees that their text messages would be viewed. The police chief requested a transcript of the text messages to determine whether the messages were used in relation to work, and the service provider sent the police department transcripts of the messages. Quon then sued for violation of his Fourth Amendment protection against unreasonable searches and seizures. The court considered many factors to reach its decision, including whether Quon knew his communications were not private and whether Quon had allowed the department to view his text messages. The court found that the service provider violated the Federal Stored Communications Act, which prohibits providers from giving up the contents of communications on its service. The court also found that Quon had a reasonable expectation of privacy and that viewing Quon's text messages to determine whether the messaging was work related was not reasonable. The full opinion may be found at [http://www.ca9.uscourts.gov/ca9/newopinions.nsf/D2CDDDB4098D7AFB28825746C0048ED24/\\$file/0755282.pdf?openelement](http://www.ca9.uscourts.gov/ca9/newopinions.nsf/D2CDDDB4098D7AFB28825746C0048ED24/$file/0755282.pdf?openelement)

MALWARE CLEARS WORKER OF CHILD PORN CHARGES

On June 16th, the *Boston Herald* reported that a Massachusetts state worker was cleared of child pornography charges after a computer forensic investigation indicated that his computer was infected with malware that was visiting illegal websites. The accused, Michael Fiola, was fired as an investigator with the Massachusetts Department of Industrial Accidents after the IT department noticed his Internet usage was four times greater than his co-workers and found child porn images on his computer. After he was accused, Fiola hired a forensics expert who discovered the malware, which was there because the IT department had not properly installed anti-virus software on the machine. Fiola was cleared of all charges, and plans to sue the agency over his firing. The full story may be found at <http://www.bostonherald.com/news/regional/general/view.bg?&articleid=1101074&format=&page=1&listingType=loc#articleFull>

MOTHER ACCUSED IN MYSPACE SUICIDE CASE PLEADS NOT GUILTY

On June 16th, Lori Drew, the Missouri mother accused of MySpace harassment that drove a teenager to commit suicide pled not guilty to federal harassment and conspiracy charges. The indictment accuses Drew of violating MySpace's terms of use by creating a fake profile as a sixteen-year-old boy. Drew allegedly pretended to be romantically interested in the girl, Megan Meier, and after the boy told her the world would be a better place without her, she committed suicide. Drew could face up to five years in jail for the harassment charges, and up to five years for each of three conspiracy counts if convicted. The full story may be found at http://www.informationweek.com/news/internet/social_network/showArticle.jhtml?articleID=208700165

COURT RULES WHITE HOUSE DOES NOT HAVE TO RELEASE E-MAILS

On June 16th, U.S. District Judge Colleen Kollar-Kotelly ruled that the White House's Office of Administration is not subject to the Freedom of Information Act (FOIA). Citizens for Responsibility and Ethics in Washington (CREW) filed the case to compel the Office of Administration (OA) to produce e-mails that disappeared during the more controversial times of the Bush Administration. In August 2007, the OA announced that despite two years of compliance with the FOIA, it would no longer comply, three months after the lawsuit was filed to discover what happened to the e-mails. Kollar-Kotelly granted the OA's motion to dismiss, stating that the OA lacks the independent authority to be subject to the FOIA since it performs mostly administrative functions. Further, the OA's past compliance with the FOIA was not enough in itself to subject it to the law. CREW stated it planned to appeal the decision. The full opinion may be found at <http://www.citizensforethics.org/files/OA%20Opinion%20June%2016%202008.pdf>

REPORT FINDS BLOGGER ARRESTS INCREASING AROUND THE GLOBE

On June 8th, the World Information Access released its "Blogger Arrest Report," which indicated that 64 people around the globe have been arrested for publishing their views on a blog since 2003. The arrests were for blogging about various things, such as government corruption, human rights abuses, or criticizing public policies or officials. Many of the bloggers arrested were put in jail, with the average jail time being 15 months and the longest jail time 8 years. Over half of the arrests were made in China, Egypt and Iran. The report credits the increased importance and popularity in blogging for the increase, and predicts that the number of bloggers arrested would increase from the 36 arrests in 2007. The full story may be found at <http://www.wiareport.org/index.php/56/blogger-arrests>

GOOGLE RELEASES NEW TOOL TO HELP TARGET ADVERTISEMENTS

On June 24th, Google announced the release of Google Ad Planner, a tool to help advertisers choose the best websites to reach their target audience. According to the Ad Words Agency Blog, the tool allows advertisers to enter information about its target audience and get information about sites that the target audience is likely to visit. The tool is not limited to sites on the Google network, as it includes sites both on and off the network. Also, the tool offers even more detail about the target audience such as demographics and related searches. The full blog post may be found at <http://adwordsagency.blogspot.com/>

HOUSE PASSES SURVEILLANCE LAW WITH TELECOM IMMUNITY

On June 23rd, the House of Representatives passed Amendments to the Foreign Intelligence Surveillance Act 293 – 129. The legislation provides for immunity for telecommunications companies from lawsuits based on the governments' warrantless wiretapping post-9/11, the most controversial issue in the bill. As a compromise, a federal district court has to review certifications from the Attorney General saying that the telecommunications companies received presidential orders telling them wiretaps were needed to prevent a terrorist attack. If the certification is good, the district court will dismiss the lawsuit. The bill also requires an investigation of the wiretapping by the Justice Department, Pentagon and Intelligence agencies. Other provisions include requiring the government to get FISA permission to wiretap Americans overseas, prohibits targeting a foreigner to listen on American phones without court permission, and would allow eavesdropping in emergencies as long as the paperwork was filed within a week. The Senate has delayed consideration of the bill until after the July recess. The full text of the legislation may be found by searching for H.R. 6304 at <http://thomas.loc.gov>

"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.