



Issue 132
May 2008

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

COURT SANCTIONS BUYER FOR DESTROYING DOCUMENTS

On October 27th, 2006, the United States Bankruptcy Court for the District of Delaware issued sanctions in the case *In re Quintus Corp.*, which involved an asset buyer who was sued for alleged failure to pay the debtor's liabilities. During discovery, the buyer could not produce the debtor's financial records. The court found that the buyer had a contractual duty to keep the files and that the buyer had intentionally deleted the files to create more space on its hard drives. Therefore, the court sanctioned the buyer with a default judgment against him for \$1.88 million. James Mention, Jr. explained in an ABA article that many lessons could be learned from the decision for similar asset buyers. For example, buyers should specify relevant records that need to be kept, and use due diligence in retaining the records. Mention's full article may be found at

<http://www.abanet.org/genpractice/newsletter/lawtrends/08-winter/business-menton.html>

COURT DENIES PRODUCTION AND SANCTION REQUESTS

On February 25th, the United States District Court for the Northern District of Georgia denied a production request under Federal Rule of Civil Procedure 26(b)(2)(B), and denied a sanctions request under Federal Rule 37. The case involved four female employees suing for sexual harassment through e-mails. The employees requested that the defendant, a transportation company, produce all e-mails of a sexual or gender derogatory nature. The court found that the request was overly broad, and that it would be unduly burdensome to produce e-mails on backup tapes for all 5,300 employees at a cost of \$79,300 per employee. The court also refused to issue sanctions under Rule 37 because it did not appear that the company acted in bad faith. Even though the company continued to follow its established policy for retention of documents after the litigation began, the employees did not request company-wide e-mail retention. Also, the prejudice to the employees was insignificant because other evidence was available. A copy of the full decision in *Petcou v. C.H. Robinson Worldwide, Inc.* may be found at

http://www.klgates.com/files/upload/eDAT_Westlaw_Document_Petcou.doc

FTC SETTLES WITH COMPANIES FOR FAILING TO SECURE CONSUMER DATA

On March 27th, the Federal Trade Commission announced settlements with discount retailer TJX and data brokers Reed Elsevier and Seisint on charges that accused the companies of failing to adequately protect sensitive consumer information. In the complaint against TJX, the FTC referred to its massive data breach that exposed over 455,000 customers' credit information through an unsecured computer network. The settlement requires TJX to implement a new security system reasonably designed to protect consumer data. Reed Elsevier and Seisint used easy-to-guess passwords that allowed customers to gain access to millions of consumer records with personal information such as social security numbers. This resulted in the theft of at least 316,000 records. The settlement requires Reed Elsevier and Seisint to establish a security program that protects non-public personal information. Both settlements also require an independent security auditor to evaluate the security measures every two years. The full FTC press release may be found at

<http://www.ftc.gov/opa/2008/03/datasec.shtm>

COURT RULES SPOILIATION CLAIM MAY BE ADDED TO COMPLAINT

On March 11th, in the case of *Ed Schmidt Pontiac-GMC Truck, Inc. v. DaimlerChrysler Motors Co., LLC*, the United States District Court for the Northern District of Ohio allowed a plaintiff to add a

spoliation claim to its initial complaint. The plaintiff alleged that the defendant violated a settlement agreement when it refused to grant the plaintiff a Chrysler franchise, and wanted to add a spoliation claim to the complaint. The court explained that, in Ohio, the elements of a spoliation action are: 1) pending or probable litigation, 2) knowledge that the litigation exists or is probable, 3) willful destruction of evidence designed to disrupt the plaintiff's case, 4) disruption of the plaintiff's case, and 5) damages proximately caused by the defendant's actions. The court found that the plaintiff had alleged facts to support all five of these elements. The plaintiff met the first two elements because both parties had filed pleadings in the case. The plaintiff met the third and fourth elements because the plaintiff alleged that the defendant had failed to implement a litigation hold, and had intentionally destroyed evidence by replacing employee hard drives. For the fifth element, the court said that a jury might conclude that replacing the hard drives was a disruption and caused damage to the plaintiff. For these reasons, the court granted the plaintiff's request to amend the complaint to include the spoliation claim. A copy of the full decision may be found at http://www.klgates.com/files/upload/eDAT_Westlaw_Document_Ed_Schmidt.doc

WEB GIANTS LAUNCH OPENSOCIAL FOUNDATION

On March 25th, Google, Yahoo, and MySpace announced the launch of the OpenSocial Foundation to help standardize applications found on social networking sites. Originally, the applications for photos and other various things on social networking sites would only work on one site, and would have to be rebuilt to work on another site. The goal of the OpenSocial Foundation is to control the intellectual property rights pertaining to the applications, and ensure that all members have a say. The Foundation is a non-profit that will not receive any revenue directly from the applications. The full press release from Google may be found at http://www.google.com/intl/en/press/pressrel/20080325_opensocial.html

COURT SETS PROTOCOL FOR REVIEW OF TEXT MESSAGES

On March 20th, in the case of *Flagg v. City of Detroit*, Federal Judge Gerald Rosen of the U.S. District Court for the Eastern District of Michigan issued two orders, one that denied a motion to quash a subpoena requiring production of text messages, and another that set a protocol for production and review of the text messages. The case involved the son of a murder victim, who sued the city of Detroit alleging it was lax in its investigation of the crime, and ignored and concealed evidence. The plaintiff moved for production of text messages from certain city officials, and subpoenaed the city's service provider to produce the messages. The court ruled that the city had to produce the text messages, but because relevance was related to the content of the messages, a protocol was necessary. In the second order, Judge Rosen described the protocol, which first required the city to turn over the PIN numbers of some phones so the service provider could produce the messages from those phones. After that, two magistrate judges would obtain the messages from the service provider and review the communications to determine whether the messages were discoverable under Federal Rule of Civil Procedure 26(b)(1). A copy of the first order may be found at http://www.klgates.com/files/upload/eDAT_Flagg_Mar_20_2008_Order.pdf

A copy of the protocol order may be found at http://www.klgates.com/files/upload/eDAT_Westlaw_Document_Flagg.doc

STUDY CONCLUDES NO "CSI" EFFECT IN JURY CONVICTION RATES

In an article in the *March National Institute for Justice (NIJ) Journal*, the Honorable Donald E. Shelton explained that he helped conduct a study to determine whether watching crime dramas such as CSI had an impact on juror behavior. The "CSI" effect refers to the belief that jurors would be unwilling to convict a defendant if no scientific evidence was presented as they are used to seeing on television crime dramas. The study found that while jurors who watched CSI were more likely to expect scientific evidence for specific types of crimes (e.g. fingerprints for burglary, DNA for rapes/murders, etc.), the jurors were not inclined to acquit if no scientific evidence was presented. The NIJ article, with a link to the full study, may be found at <http://www.ojp.usdoj.gov/nij/journals/259/csi-effect.htm>

NIH LAPTOP CONTAINING PATIENT DATA STOLEN

On March 24th, the National Institute for Health (NIH) announced that a laptop had been stolen from the trunk of an employee's car in late February. The laptop contained unencrypted patient information from an NIH study, and included health information but no financial information or social security numbers. The NIH investigation revealed that it appeared to be a random theft, and it was unlikely that the confidential information would have been exposed because the computer was password protected and off at the time of the theft. Almost a month after the incident, the NIH sent letters to affected parties informing them of the breach, and assured the public it was taking steps to secure its data for the future. The full NIH press release may be found at <http://public.nhlbi.nih.gov/newsroom/home/GetPressRelease.aspx?id=2559>

COURT RULES NO ADVERSE INFERENCE INSTRUCTION

On December 21st, 2007, in the case of *Toussie v. County of Suffolk*, in the U.S. District Court for the Eastern District of New York, Magistrate Judge Arlene Lindsay refused to impose an adverse inference instruction against a defendant in a discrimination lawsuit. The plaintiff moved for sanctions for failure to produce e-mails in a timely manner. The court stated that a party seeking an adverse inference instruction must satisfy a three part test: 1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed, 2) that the records were destroyed with a culpable state of mind, and 3) that the destroyed evidence was relevant to the parties' claim or defense. Here, the court found that the defendant was grossly negligent, as the defendant failed to implement a litigation hold, continued to put its information on back-up tapes in an inaccessible format, and key employees were free to delete documents because there was no litigation hold. The plaintiff therefore met the first two prongs of the test, but failed to meet the third because he did not show that the e-mails would have been relevant to his claim, because the e-mails had to do with the plaintiff's business practices, not discrimination. For this reason, the court refused to order an adverse inference instruction and instead awarded the plaintiff monetary sanctions. A copy of the full opinion may be found at http://www.klgates.com/files/upload/eDAT_Westlaw_Document_Toussie.doc

STATE DEPARTMENT EMPLOYEES ACCESS OBAMA'S PASSPORT

On March 21st, the State Department announced that three employees had accessed potential Democratic presidential nominee Barack Obama's passport information without authorization. Two of the employees were fired, whereas the third was only disciplined. Undersecretary for Management, Patrick Kennedy, answering questions during a press briefing said that the employees had access to the database for their jobs. Kennedy also explained that the data system security worked, as it had uncovered the unauthorized access so the State Department could act upon it. It was later discovered that the other two presidential hopefuls, Senator John McCain, and Senator Hillary Clinton, had had their passport information accessed as well. Undersecretary Kennedy's press briefing may be found at <http://www.state.gov/m/rls/102460.htm>

COURT SAYS NO ADVISORY OPINION ON DOCUMENT PRESERVATION

On March 27th, in the United States District Court for the Eastern District of Texas, the court refused to give the State of Texas, the plaintiff, relief from a general litigation hold request for electronic documents sent by the defendant, City of Frisco. No complaint had been filed against the state yet, the city had simply asked for a litigation hold pertaining to a highway toll project in the Texas Department of Transportation. The state asked the court to issue a declaratory judgment against the city, stating that the litigation hold did not follow the Federal Rules of Civil Procedure. The court found that the state had the burden to prove why a declaratory judgment was necessary and that the state failed to meet that burden because it did not establish that there was an actual controversy. The court found that the state was seeking judgment as to how rules of discovery applied before a lawsuit was filed. The court stated that it did not rule on discovery processes before a lawsuit was filed. The court said that both parties had to conduct themselves under the good faith requirement of the Federal Rules, but would not go into the specific duties of a party to retain certain documents. A copy of the full opinion in *Texas v. City of Frisco* may be found at

http://www.klgates.com/files/upload/eDAT_Westlaw_Document_Texas.doc

TRACKING SYSTEMS INCREASE IN POPULARITY

On April 4th, the *Washington Post* reported that Internet Service Providers (ISPs) have increased access to users' online activity, from sending e-mail to visiting websites. The purpose of tracking is to sell the information to advertisers, who then place ads on the websites relating to the users' online activity. The article described new technology, called "deep pocket inspection," that allows the ISP to view any website visited, along with e-mails sent and search terms used. The deep pocket method is in contrast with other tracking systems that can only track what websites the user visit. The increasing practice brought up numerous privacy concerns, especially because most consumers do not know whether they are being monitored. Tracking firms declined to release which ISPs they were tracking for. The full report may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html?nav=hcmodule>

ALL STATES REAL ID COMPLIANT THROUGH EXTENSIONS

On April 2nd, the Department of Homeland Security (DHS) announced that all 56 U.S. jurisdictions were compliant with the initial benchmark of May 11th for the first stage of the REAL ID program. The compliance announcement was a bit of a farce however, because all jurisdictions were granted extensions to comply with the program. In effect, nothing changed, as many states simply promised to pass legislation on REAL ID, and others have made it clear that they will oppose the program completely. Maine, one state that was completely opposed, achieved "compliance" through promising to introduce legislation on the issue, though the chance of the legislation passing is negligible. The REAL ID program was implemented as a measure to increase the security of state issued identification, but most states viewed it as an imposition on their authority. The press release from the DHS may be found at http://www.dhs.gov/xnews/releases/pr_1207167055742.shtm

A listing of the "compliant" states and information about extensions may be found at http://www.dhs.gov/xprevprot/programs/gc_1204567770971.shtm

An informative news article about the compliance may be found at http://www.news.com/8301-13578_3-9909928-38.html

9TH CIRCUIT SAYS ROOMMATES.COM CAN BE SUED FOR DISCRIMINATION

On April 3rd, the U.S. Court of Appeals for the Ninth Circuit held that the website Roommates.com is not immune from discrimination lawsuits. The court found that the site is not a typical Internet forum because it required users to answer questions about gender, marital status and sexual orientation. The ruling limited Section 230 of the Communications Decency Act of 1996, which typically protects online forums and Internet Service Providers from what its users say online. According to the court, the immunity did not extend to Roommates.com because the check boxes on the site actively ask for discriminatory content, taking the site beyond a passive forum for user information. The court held that the site did have immunity on the forum part of the site where users could post further comments. The full ruling may be found at [http://www.ca9.uscourts.gov/ca9/newopinions.nsf/F71559D8162BA7EE8825741F00771BC1/\\$file/0456916.pdf?openelement](http://www.ca9.uscourts.gov/ca9/newopinions.nsf/F71559D8162BA7EE8825741F00771BC1/$file/0456916.pdf?openelement)

DATA BREACHES HIT RECORD HIGH FIRST QUARTER

On April 9th, the Identity Theft Resource Center (ITRC) unveiled a new report that found at least 8 million Americans had their personal information exposed by data breaches in the first quarter of 2008. The number of breaches reported was 167, which was a 76 percent increase from the same time period in 2007. A few of the companies reporting data breaches were Hannaford Bros Supermarket Chain, GE Money, and Georgetown University, among others. The ITRC explained that the increase statistically showed the alarming rate at which data breaches are growing, and showed the need for more preventative measures across all industries. The ITRC press release, with links to the full report, may be found at

http://www.idtheftcenter.org/artman2/publish/m_press/Breach_List_2008_Q1.shtml

COURT RULES PARTY NOT ENTITLED TO NATIVE PRODUCTION

On April 2nd, in a trademark infringement case, the defendant wanted to compel the plaintiff to produce a document in its native format with relevant metadata. The United States District Court for the Northern District of Illinois ruled that the plaintiff did not have to produce a document in its native format, because the plaintiff had already produced the document in paper format, PDF format, and had included a nine-page history of all the changes that were made to the document. The court found that under Federal Rule of Civil Procedure 34(b)(2)(E), the paper and PDF formats were readily useable forms. Further, the defendant did not initially request that the metadata be produced, and the metadata was not mentioned in any prior document requests. For these reasons, the court denied the defendant's motion. The decision in *Autotech v. Automationdirect.com* may be found at http://www.klgates.com/files/upload/eDAT_Westlaw_Document_Autotech.doc

FBI REPORTS INTERNET CRIME AT AN ALL TIME HIGH

On April 3rd, the Federal Bureau of Investigation announced the release of its 2007 Internet Crime Report, which found that 206,884 complaints about Internet crime were received by the Internet Crime Complaint Center in 2007. Of the complaints, about 90,000 were referred to law enforcement, and resulted in losses totaling \$240 million, an increase of \$40 million from 2006. Internet auction fraud was the most reported complaint, but others included non-delivery of items, computer intrusions, spam e-mails and child pornography. The full report may be found at http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf

TJX ANNOUNCES SETTLEMENT WITH MASTERCARD

On April 2nd, TJX announced that it had agreed to pay MasterCard \$24 million for losing 29 million MasterCard transactions in its massive data breach last year. Under the settlement, alternative recovery options would be made available to issuers of cards affected by the breach. The settlement will occur if 90 percent of the issuers accept the alternative recovery by May 2nd, 2008. The settlement, among the other settlements TJX entered into because of the data breach, continued to demonstrate the massive cost of data breaches. The TJX press release may be found at <http://tinyurl.com/4xwejb>

COURT SIDES WITH RECORDING INDUSTRY IN KAZAA LAWSUIT

On March 31st, U.S. District Court Judge Kenneth Karas denied a motion to dismiss the complaint in a copyright lawsuit against a Kazaa user who placed her music in a shared folder that allowed others to download the files. Karas found that under copyright law, to determine whether a person "made available" the files, the terms distribution and publications were synonymous, and that offering to distribute copies could result in liability. Further, the recording industry did not properly use the term distribution, and the court gave the industry 30 days to amend the complaint. Because there were other claims in the complaint that could support a copyright infringement action, Karas refused to dismiss the complaint. The full opinion may be found at http://www.ilrweb.com/viewILRPDF.asp?filename=elektra_barker_080331Decision

REPORT FINDS CHILD PORNOGRAPHY ON 20,000 VIRGINIA COMPUTERS

On April 10th, as reported by the *Washington Post*, an expert report by agent Flint Waters found that 20,000 computers in the state of Virginia had sent child pornography files. Waters is a special agent with the Wyoming Attorney General's office, and serves as part of a federal program called the Internet Crimes Against Children Task Force. The Task Force uses tracking software called Operation Fairplay, which allows investigators to download child pornography from a user and then identifies the user's IP address. This process can lead to a search warrant, but there is a lack of resources to investigate each individual user. The full Washington Post report may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2008/04/08/AR2008040803930.html>

POOR IRS SECURITY COULD EXPOSE TAXPAYERS' CONFIDENTIAL INFO

On March 26th, the Treasury Inspector General for Tax Administration issued a report that stated IRS computers had poor controls that could allow a disgruntled employee, agency contractor or hacker to steal taxpayers' personal information. Out of 374 accounts the IRS authorized for systems administration duties, 141 had never been properly authorized or had expired authorizations. The report also found that "audit trail" logs that could help identify questionable activity were not being properly reviewed, which would allow unauthorized access to go undetected. The report recommended improvements such as ensuring that users were properly authorized and ensuring that audit trail information was reviewed. The IRS agreed to implement most of the measures. The full report may be found at <http://www.treas.gov/tigta/auditreports/2008reports/200820071fr.pdf>

LOVESTRUCK TEENAGER NOT GUILTY OF HARASSMENT ON MYSPACE

On April 4th, New York City Criminal Court Judge Michael Gerstein held that a teenager declaring his love for another teenager over MySpace was not a criminal act. The New York prosecutors charged eighteen year-old Isaiah Rodriguez with harassment and endangering the welfare of a child because he sent messages to a fourteen year old girl stating that he loved her, would not stop talking to her, and that they should be together. Gerstein found that there was nothing in the complaint that elevated Rodriguez's messages to harassment, as MySpace allows a person to choose who to communicate with, and there was no indication that Rodriguez had been rebuffed or that his messages had been blocked. The full story, including excerpts from the opinion, may be found at http://www.news.com/8301-13578_3-9914734-38.html

FINJAN REPORTS CRIMEWARE SERVICES ON THE RISE

On April 7th, security supplier Finjan released a report through its Malicious Code Research Center stating that cyber criminals are increasingly using online cybercrime services instead of using their own servers or software. The criminal software providers offer updates for their products and give their users new ways to attack as technology changes. The new crimeware provides more options for criminals and allows them to produce more targeted attacks. The full report may be found at <http://www.finjan.com/Pressrelease.aspx?id=1922&PressLan=1819&lan=3>

COURT REFINES SEARCH PROTOCOL

On April 1st, in the United States District Court for the District of Utah, the court refined the search protocol for parties in a case alleging misappropriation of trade secrets. A previous order called for the mirror imaging of two defendants' computers, and the April order refined the terms to search the mirror images. The court found that a conjunctive search term should be used with a person's name, because almost every document on the computer could be potentially responsive with only a name, and including another term would help narrow the search. Also, five additional terms proposed by the plaintiff were not overly broad, and use of the terms in the disjunctive would probably yield significant evidence. The court further warned that the order was not the final say on discovery or search terms, and that additional orders would be issued as necessary. The case is *Clearone Communications, Inc. v. Chiang*, and the full decision may be found at http://www.klgates.com/files/upload/eDAT_Westlaw_Document_ClearOne_Comm.doc

MICROSOFT AND YAHOO BATTLE THROUGH LETTERS

On April 5th, Microsoft sent a letter to Yahoo! stating that Yahoo! should take Microsoft's previous offer or be prepared for a hostile takeover. Microsoft threatened to go to the shareholders directly, and said this would decrease the value of Yahoo! significantly. Yahoo! replied on April 7th, and stated that the company had already decided that Microsoft's unsolicited bid undervalued the company and was not in Yahoo!'s best interest. Yahoo! also pointed out that Microsoft's stock price had decreased, making its proposal worth less. Microsoft's initial letter may be found at <http://www.microsoft.com/presspass/press/2008/apr08/04-05LetterPR.msp>

Yahoo!'s reply may be found at <http://yhoo.client.shareholder.com/press/releasedetail.cfm?>

[ReleaseID=303369](#)

VIRGINIA FIRST STATE TO REQUIRE INTERNET SAFETY IN SCHOOL

On April 6th, news sources revealed that Virginia was the first state to require Internet safety lessons in school. The rules went into effect this school year, and in accordance with the rule, Assistant Attorney General Gene Fishel did a presentation at James River High school, warning teens not to believe everything they read online and not to meet people they met online in person. Virginia has implemented programs to help integrate Internet safety lessons into regular coursework, along with having guest speakers like Fishel. The full story may be found at <http://www.foxnews.com/story/0,2933,347035,00.html>

NY APPELLATE COURT HOLDS E-MAILS CAN MODIFY CONTRACT

On April 1st, the New York Appellate Division, First Department, held that e-mails were signed writings that could be used to modify an employment agreement. The e-mails satisfied the Statute of Frauds because the name at the end of the e-mails indicated that the parties wanted to authenticate the contents of the e-mail. The Appellate Court upheld the trial court in finding that offer and acceptance through the e-mails were valid. The full decision may be found at http://www.courts.state.ny.us/reporter/3dseries/2008/2008_02880.htm

GOOGLE SUED BY COUPLE CLAIMING STREET VIEW VIOLATES PRIVACY

On April 4th, a Pittsburgh couple filed a complaint against Google, claiming that street view images of their home on Google's website violated their privacy rights, devalued their home and caused them suffering. The couple claimed that Google went down their road, marked "private" and took the photos. Google stated that the claim had no merit, and that there were better methods besides litigation to get a photo removed from the website. An interesting point was that Google was not the only website that had photos of the home, as it was also featured on the Alleghany County, PA website. The full story, with a copy of the complaint at the bottom, may be found at <http://www.thesmokinggun.com/archive/years/2008/0404081google1.html>

WHITE HOUSE SEEKS CLARIFICATION ON E-MAIL PRESERVATION

On April 17th, the White House submitted a clarification request on a previous court order that required the White House to preserve its backup tapes. The clarification asked that the order be amended to state that the tapes could still be used for data recovery when necessary to assist the President. The White House claimed that if the court did not agree to the request, then the daily operations of the Executive Office of the President would be hindered. The suit brought by the National Security Archive and Citizens for Ethics and Responsibility in Washington was awaiting rulings on various motions, including a motion to extend the protective order and conduct depositions, a motion to expedite discovery, and the White House's motion to dismiss. The full press release may be found at <http://www.gwu.edu/%7EEnsarchiv/news/20080417/index.htm>

PUBLISHERS SUE GEORGIA STATE FOR ONLINE REPRODUCTIONS

On April 15th, three publishers filed suit against officials at Georgia State University for copyright infringement because the University reproduced the publishers' works online without permission. The complaint alleged that the University encouraged professors to post materials online for download by students without the requisite authorization and compensation to the publishers. The complaint also stated that the publishers tried numerous times to negotiate with the University about its unauthorized use. The publishers asked for injunctive and declaratory relief, in what is likely the first lawsuit of its kind. The full complaint may be found at <http://www.publishers.org/main/PressCenter/documents/GSULawsuitcomplaint.pdf>

NEW PHISHING SCAM SENDS OUT FAKE SUBPOENAS

On April 16th, the New York Times reported that a new e-mail scam had targeted executives at many companies through an e-mail containing a fake subpoena for the executive to appear before the United States District Court for the Southern District of California. The scam told the viewers to follow a link to view the whole subpoena. When the user clicked on the link, the user was asked to install a Web browser add-on to view the actual subpoena. The "add-on" was a component designed to steal usernames and passwords. A copy of the fake e-mail may be found at <http://www.casd.uscourts.gov/uploads/emailscam-pdf.pdf>

The New York Times Story may be found at <http://www.nytimes.com/2008/04/16/technology/16whale.html>

FLORIDA COURT REJECTS JURISDICTION OVER BLOGGER

On April 8th, United States District Judge Ann Conway ruled that Florida courts had no personal jurisdiction over a blogger in a defamation lawsuit. Plaintiff Internet Solutions Corp. (ISC), sued the defendant, Tabitha Marshall, of Washington state, for allegedly defamatory statements Marshall made on her blog. The plaintiff alleged that jurisdiction was proper because Marshall's comments had caused injury in Florida. Without more than just an injury, the court found that jurisdiction over Marshall would not satisfy the minimum contacts test for personal jurisdiction in Florida. That Marshall's website was accessible in every state did not equal purposeful availment, and the court dismissed the case for lack of personal jurisdiction. A full copy of the decision may be found at <http://www.citmedialaw.org/sites/citmedialaw.org/files/2008-04-08-Order%20Dismissing%20the%20Case.pdf>

GOOGLE USES TECHNOLOGIES TO FIGHT CHILD PORNOGRAPHY

On April 14th, Google announced that it was working with the National Center for Missing and Exploited Children (NCMEC), building software to help workers go through the millions of child pornographic images on the Internet. Google Research Scientist Shumeet Baluja described the work with NCMEC in a blog post, and stated that Google helped create software tools that would allow NCMEC workers to go through images more quickly and reference historical material more easily. The video tool streamlines the review of the clips, and the automation and streamline techniques helps make the review process much faster. The full blog post may be found at <http://googleblog.blogspot.com/2008/04/building-software-tools-to-find-child.html>

ATTORNEYS SANCTIONED FOR OBSTRUCTING COMPUTER INSPECTION

On April 9th, the United States District Court for the District of Connecticut issued sanctions against defense attorneys in the case of Sterle v. Elizabeth Arden, Inc., a wrongful termination case. The plaintiff was seeking discovery of sales reports that he knew existed but the defendant would not produce. The court ordered a forensic examiner to search the defendant's computers under an agreed upon protocol. But when the examiner went to do the search, he was at first given some access and then had it taken away after the defendant consulted with his attorneys, waited for help to get access from an IT professional that never came, and was unable to access the necessary folders. The court found that the defense attorneys did not act in good faith during the investigation. The court awarded sanctions for reasonable expenses the plaintiff incurred in his effort to compel discovery. The full decision may be found at http://www.klgates.com/files/upload/eDAT_Westlaw_Document_Sterle.doc

"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.