

# { bytes in brief }

LAW AND TECHNOLOGY NEWS MONTHLY

EDITORS: Sharon D. Nelson, Esq. and John W. Simek  
ASSOCIATE EDITOR: Jason R. Foltin EDITOR EMERITUS: G. V. Nelson



© 2009 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

## Issue 146 - July 2009

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

---

### SUPREME COURT WILL HEAR MAJOR COPYRIGHT CASE

On February 23rd, 2009, the U.S. Supreme Court granted certiorari to hear an appeal by a group of publishers seeking to reinstall a settlement with freelance writers, effectively reversing the Second Circuit's decision that federal courts lacked jurisdiction in the instant case. Initially, the writers had sued publishers and electronic database services, arguing that their contract did not allow publishers a license for others to electronically produce their work. The settlement was reached in 2005 and was approved by a federal judge. This settlement was subsequently thrown out by a U.S. Appeals Court panel because the panel reasoned that the federal judge lacked jurisdiction over infringement claims arising from unregistered copyrights. In accepting review, the Supreme Court stated the only question it would consider was whether the law restricted federal court jurisdiction over copyright infringement actions. Arguments in the case will take place during the court's upcoming term in October. The brief for the petitioners can be found at [http://www.abanet.org/publiced/preview/briefs/pdfs/07-08/08-103\\_Petitioner.pdf](http://www.abanet.org/publiced/preview/briefs/pdfs/07-08/08-103_Petitioner.pdf)

---

### FIVE LAWYERS INVOLVED IN TEXT MESSAGE SCANDAL FACE ETHICS CHARGES

On May 21st, 2009, The National Law Journal reported that five lawyers who allegedly engaged in a text message scandal involving former Detroit Mayor Kwame Kilpatrick face ethics violation charges. The main thrust of the allegations is that the lawyers either knew about, or took part in a secret lawsuit settlement to hide text messages that demonstrated the mayor had lied under oath about an affair with a former aide, a revelation leading to perjury and obstruction of justice charges as well as the mayor's resignation. The lawyers' conduct has raised serious questions about the attorneys' behavior, specifically whether the lawyers knew perjury had been committed and failed to notify the court as well as whether a newspaper Freedom of Information Act request for the actual text messages was properly handled. Hearings have been set for the second week in July, and if convicted, the lawyers face possible suspension or revocation of their law licenses. For more information, the story may be found at <http://www.law.com/jsp/article.jsp?id=1202430879282>

---

### CLICKJACKING: HIJACKING CLICKS ON THE INTERNET

On May 22nd, 2009, cnet reported a new type of Internet exploitation called clickjacking, a design flaw in the way the Web is supposed to work. In its basic form, a clickjacker superimposes an invisible button over something a user wants to click on, thereby redirecting the unsuspecting victim's click to go anywhere the attacker desires. The story highlighted the serious potential for abuse that could occur through clickjacking; an attacker may be able to turn a user's web cam or microphone on to spy on unsuspecting victims, direct individuals to websites with malicious content, or even make a person click "buy" instead of "cancel" during Internet transactions. Further, another issue compounding the seriousness of clickjacking is that there isn't much available to individuals to protect themselves. The story emphasized that individuals using Windows and Internet Explorer should disable JavaScript to protect against possible clickjacking attempts. Using Firefox is a safer alternative given the NoScript add-on feature that allows users to not only selectively block certain scripts, but also includes a ClearClick feature specifically targeted to protect against clickjacking. Finally, the story noted that when finished using a website, logging out will help prevent attacks as well. The story can be found at [http://news.cnet.com/8301-1009\\_3-10247327-83.html](http://news.cnet.com/8301-1009_3-10247327-83.html)

---

## **HOW TO BECOME AN E-DISCOVERY SPECIAL MASTER**

On May 27th, 2009, Law and Technology News discussed some tips and techniques for tech-savvy lawyers seeking to serve as e-discovery special masters. The article first explained that a special master is a technical expert—ideally a lawyer—appointed by the court to manage and resolve discovery disputes involving electronic evidence. Specifically, a special master may be relied on to sort out search terms, fashion collection protocols, investigate spoliation claims, resolve privilege concerns, arbitrate forms of production, suggest sampling scenarios, apportion costs and make sanctions recommendations. Addressing some useful skills learned throughout the course of his career as a special master, author Craig Ball explained that an individual must be courteous and patient, but also foster efficiency during party meetings and negotiations. Further, Ball explained that a special master must be neutral and keep in mind that he or she stands in the shoes of the court. Additionally, he gave several helpful tips to aid in successful negotiations and discussions. One such tip explained that recording conference calls is a cost-effective alternative to placing all agreements in writing and can also quell many disputes. He also stressed the importance of bringing all IT specialists together, without lawyer intermediaries to reduce friction and arguments—except in instances of substantive legal discussions. Ball concluded by explaining that while being tech-savvy is important, being people-savvy and keeping your ego in check matters more. A discussion of the role of an e-discovery special master may be found at <http://www.cardozolawreview.com/content/30-2/SCHEINDLIN.30.2.pdf>

---

## **WHATEVER YOU DO, DON'T SEARCH THE TERM "SCREENSAVERS"**

On May 27th, 2009 ZDnet discussed a recent report released by McAfee highlighting some of the web's most dangerous search terms. Number one on that list was the term "screensavers" with a maximum risk of 59.1 percent. Additionally, search terms including lyric keywords and anything including the word "free" have the next highest risk of exposing users to malware or fraudulent web sites. The safest were those regarding health related terms or the recent economic crisis. While this research attempts to raise awareness of the potential malicious practices, ZDnet noted that the report may leave many individuals with a false sense of security as cybercriminals have adapted dynamically to the changing environment. Specifically, ZDnet explained that cybercriminals are applying basic mass marketing keyword practices and, additionally, legitimate and compromised web sites serve more exploits and malware than the purely malicious ones. Thus, ZDnet concluded that it may be difficult to quantify the most dangerous keyword search given that cybercriminals are constantly changing their tactics. The McAfee report can be found at [http://us.mcafee.com/en-us/local/docs/most\\_dangerous\\_searchterm\\_us.pdf](http://us.mcafee.com/en-us/local/docs/most_dangerous_searchterm_us.pdf)

---

## **DEFENSE DEPARTMENT AND INDUSTRY JOIN FORCES TO BATTLE CYBER CRIME**

On May 25th, 2009, The Washington Post reported that defense companies and the Pentagon have begun to join forces in an attempt to stem the loss of important defense industry data. For the last two years, the Defense Department has been collaborating with industry and considering ways to share the Pentagon's threat data with other critical companies, such as those that handle vastly larger amounts of data, including phone calls and private e-mails. The goal of this joint-effort is to provide a swift, coordinated response to cyber threats; however, the partnership still faces a myriad of obstacles. For instance, both governmental agencies and private companies have been reluctant to share the requisite information, thereby impeding the promise of the program. Additionally, while the Defense Department's Cyber Crime Center is able to send some alerts out quickly, other reports based on classified data take approximately three weeks to complete. Further, some firms either decline to share information or choose only to share with the Cyber Crime Center technical information that can help the industry broadly. For example, Northrop Grumman reports breaches to the military branch owning the contract and Lockheed Martin prefers to do its own intrusion investigations. The Pentagon concluded by stating cyber threats present a very real problem and that it will soon seek to amend defense acquisition rules to require cybersecurity standards for firms seeking contracts. The Washington Post article can be found at <http://www.washingtonpost.com/wp-dyn/content/article/2009/05/24/AR2009052402140.html?hpid=moreheadlines>

---

## **JUDGE NO-NOS: FRIENDING A LAWYER AND GOOGLING A LITIGANT**

On June 1st, 2009, the ABA Journal reported that a North Carolina judge, B. Carlton Terry Jr., has been reprimanded for using the social website, Facebook, to contact and converse with a lawyer in a pending case as well as accessing the website of a party during the pendency of litigation. According to the opinion, Judge Terry, Jr. “friended” the lawyer, discussed court proceedings on the site, and referenced a poem found on a party’s website during court. At the request of the non-friended counsel, the judge disqualified himself from the trial. During the subsequent judicial standards commission hearing, the commission stated that the ex parte communications and the independent gathering of information indicated a disregard of the principles of judicial conduct. As such, Judge Terry, Jr. was publicly reprimanded and agreed that he would never repeat such conduct in the future. The opinion can be found online at <http://www.aoc.state.nc.us/www/public/coa/jsc/publicreprimands/jsc08-234.pdf>

---

## **TECH GIANTS REPORTEDLY TARGETED IN DOJ RECRUITING PROBE**

On June 2nd, 2009, The Washington Post reported that several tech giants, including Apple, Google, and Yahoo, are being investigated by the Department of Justice for potentially violating antitrust regulations related to negotiations over the recruiting and hiring of one another’s employees. According to the report, companies that agree not to hire away talent could be stifling competition. Generally, fierce battles to maintain top talent are common place in the tech industry. In 2005, Google was sued by Microsoft after hiring Kai-Fu away from Microsoft to run Google’s research operation in China. Last year, IBM sued another former employee to prevent him from joining Apple—claiming that the employee would divulge secrets and violate his employment contract. IBM filed a similar lawsuit to prevent a former employee, David Johnson, from joining Dell on the grounds that it would violate his contract. The Washington Post’s article can be found at <http://www.washingtonpost.com/wp-dyn/content/article/2009/06/02/AR2009060203412.html>

---

## **JUDGE RULES TELECOMS HAVE IMMUNITY UNDER FISA AMENDMENTS ACT**

On June 3rd, 2009, a federal judge ruled that telecommunications companies have immunity from liability under the FISA Amendments Act (FISAAA) and thus dismissed several lawsuits concerning illegal domestic surveillance of American citizens. FISAAA, signed in 2008 by President Bush, permits the dismissal of any lawsuits premised on the participation by any telecom company in any warrantless surveillance programs if the government secretly certifies to the court that the surveillance did not occur, was legal, or was authorized by the President. After the ruling, the Legal Director for the Electronic Frontier Foundation (EFF) contended that FISAAA unconstitutionally takes away claims premised on the Constitution, violates separation of powers, and an individual’s right to due process of law. However, today’s ruling still left open the possibility of governmental accountability. Judge Walker explained that the plaintiffs retained a means of redressing the harms alleged in their complaints by proceeding against governmental actors and entities who were the primary actors in the alleged wiretapping activities. The full opinion can be found at [http://www.eff.org/files/filenode/att/orderhepting6309\\_0.pdf](http://www.eff.org/files/filenode/att/orderhepting6309_0.pdf)

---

## **OOPS! LIST OF U.S. NUCLEAR SITES INADVERTENTLY POSTED ONLINE**

On June 3rd, 2009, the Washington Post provided details about an apparently inadvertent security breach that resulted in a sensitive U.S. document—containing details about country-wide nuclear sites—being posted online. The document was intended as a formal declaration to the International Atomic Energy Agency to satisfy certain U.S. obligations under the nuclear Non-Proliferation Treaty. The draft described sensitive civilian sites, including those facilities that store enriched uranium and materials used in nuclear weapons. Because the information was unclassified, the release was likely more embarrassing than harmful; however, some nuclear experts posited that it was possible that the document could benefit terrorist organizations. The actual draft document may be found at <http://www.scribd.com/doc/16180866/THE-LIST-OF-SITES-LOCATIONS-FACILITIES-AND-ACTIVITIES-DECLARED-TO-THE-INTERNATIONAL-ATOMIC-ENERGY-AGENCY>

---

## **FEDERAL TRADE COMMISSION SHUTS DOWN ROGUE ISP**

On June 4th, 2009, the Federal Trade Commission (FTC) reported that a California District Court had shut down

Pricewart, an Internet service provider that allegedly hosts and participates in the distribution of spam, child pornography, and other harmful electronic content. The case was brought with the assistance of multiple federal agencies and officials seeking to send a message to cybercriminals that corporations and law enforcement are willing to work collaboratively to fight illegal online activities. In its complaint, the FTC contended that Pricewart recruits and colludes with criminals who seek to maliciously initiate cyberattacks over the Internet. Specifically, the FTC estimated that the provider controlled well over 4,500 malicious software programs, programs capable of keystroke logging, password and data stealing, and spam distribution. In response to these allegations, the court responded by issuing a temporary restraining order to quell Pricewart's alleged illegal activities and freezing the service provider's assets. Even though the effects of this decision will take years to manifest and will likely not change the level of spam received, many see this as a step in the right direction. The FTC report can be found at <http://www.ftc.gov/opa/2009/06/3fn.shtm>

---

### **BASEBALL MANAGER SUES TWITTER OVER ALLEGED FAKE PAGE**

On June 4th, 2009, The Associated Press brought to light a lawsuit filed by Tony La Russa, manager of the St. Louis Cardinals, against the social-networking site Twitter claiming that an unauthorized page falsely gave the impression that certain comments were his own, causing emotional distress and damaging his reputation. Specifically, these statements attempted to humorously reference his recent drunken driving charges and the death of two Cardinals pitchers. One tweet posted on April 19th stated: "Lost 2 out of 3, but we made it out of Chicago without one drunk driving incident or dead pitcher." The lawsuit comes during a time when many professional athletes and those affiliated with pro sports have embraced the Twitter phenomena. The article can be found at <http://www.google.com/hostednews/ap/article/ALeqM5gqd0f6CoYrMnmbQdeH0zrqdIVpFgD98JVC4O2>

---

### **LOUISIANA HOUSE APPROVES 15-CENT CHARGE ON INTERNET ACCESS**

On June 5th, 2009, The Associated Press reported that the Louisiana House of Representatives decisively backed a bill that would levy a 15-cent monthly surcharge on Internet access to fight criminal activity despite protests by Governor Bobby Jindal. The bill's sponsor said that the measure would raise approximately 2.4 million dollars a year for the investigation of Internet crime. While proponents have argued that the charge is merely a usage fee and have focused on its primary use—preventing sex crimes against children—to push the bill forward, critics have contended the charge is more of a tax and have questioned whether it violates federal law. If approved by the Senate later in the year, Internet users' bills would begin to reflect the 15-cent charge in 2010 with public libraries and schools receiving exempt status. The report can be found at [http://www.google.com/hostednews/ap/article/ALeqM5hLQq8gon73ewkEC4PwSh\\_7zQgbvQD98KGKS83](http://www.google.com/hostednews/ap/article/ALeqM5hLQq8gon73ewkEC4PwSh_7zQgbvQD98KGKS83)

---

### **A LESSON ON SPOILIATION SANCTIONS**

On May 29th, 2009, the Delaware Chancery Court issued its decision in Beard Research, Inc. v. Kates, effectively demonstrating the various standards necessary to sanction a party for the spoliation of evidence. After first finding that Defendants had breached their duty to preserve evidence, the court explained that a default judgment, an extreme sanction, was justified in instances where a party acted willfully or in bad faith and intended to prevent the other side from examining the evidence sought. Finding that Defendants had not acted in such a manner, the court then concluded that the next highest sanction, an adverse inference instruction, is warranted where a litigant intentionally or recklessly destroys evidence, when the party knows that the item in question is relevant to a legal dispute or it was otherwise under a legal duty to preserve the item. Here, the court found that evidence tended to demonstrate the requisite mind state and thus an adverse inference instruction was appropriate. Finally, the court concluded that a party can be sanctioned monetarily by showing that the duty to preserve evidence was breached. Basically, negligence is sufficient for attorneys' fees. Given Defendant's actions and destruction of evidence, the Court ordered the defendants to pay the attorneys' fees, expenses and expert fees. A more in-depth analysis of the case can be found at <http://bowtielaw.wordpress.com/2009/06/10/reckless-abandon-lost-hard-drives-and-sanctions/>

---

## **INTERNATIONAL TELECOM HACKER GROUP BUSTED**

On June 12th, 2009, a federal grand jury in New Jersey indicted three individuals, and five people were also arrested in Italy, in correlation with a worldwide telecom hacking scheme to gain free access to telephone services. The actual value of the stolen services is unknown; however, the US Attorney's office said that the hackers had routed well over \$55 million dollars worth of telephone calls throughout the United States. Italian officials stated that the proceeds for this particular scam have been used to fund Islamic fundamentalist groups located throughout Southeast Asia. All individuals arrested in Italy were citizens of Pakistan whereas those indicted in the U.S. included one citizen of Jordan and two Philippine nationals. All were charged with wire fraud, unauthorized access to computer systems and possession of unauthorized access devices, including pass codes to U.S. telephone systems. If convicted, each individual faces up to twenty years in prison. The report can be found at <http://news.idg.no/cw/art.cfm?id=D612D77E-1A64-6A71-CE24D74E4E5C30BC>

---

## **IT EMPLOYEES MAY BE READING YOUR E-MAILS AND COPYING FILES**

On June 11th, 2009, The Wall Street Journal reported that a global survey has found that the number of information-technology (IT) employees who admitted to accessing corporate information has risen from 33% to 35% in just a year. Additionally, the survey demonstrated that the number of individuals who stated that they would take company financial reports and merger and acquisition plans has increased over six-times from a year ago, to approximately 47% of IT staff surveyed. Many believe that the recent economic turmoil and layoff fears contribute to some of the behavior revealed in the study. Adding to this problem, 74% of IT workers said they could get past the controls currently in place for protecting confidential information. Also, a downsized company may now employ a smaller staff which makes monitoring access that much harder. The security-software company that administered the survey emphasized that companies must realize that IT administrators have access to anonymous accounts which do not leave footprints showing who is logging in and accessing the information. A copy of the survey results can be found at [http://www.cyber-ark.com/news-events/pr\\_20090610.asp](http://www.cyber-ark.com/news-events/pr_20090610.asp)

---

## **WWIII MAY POTENTIALLY BE FOUGHT IN CYBERSPACE**

On June 11th, 2009, InformationWeek reported that a former Homeland Security IT chief, Steven Cooper, has warned that if it ever occurs, World War III will be fought via computers. Mr. Cooper explained that foreign hackers have been using automated programs to ping networks controlling critical U.S. infrastructure in attempts to gain access to sensitive sites millions of times per day. Noting the changing landscape of warfare, Mr. Cooper espoused that one of the best ways the U.S. can protect itself in these cyberwars is to recruit the best and brightest IT professionals from around the world. However, Mr. Cooper explained that the strict visa restrictions employed after 9/11 make it more difficult for foreign students to remain in the country, thereby depleting the talent pool and giving other foreign governments access to these U.S.-trained experts. While it is likely only a small minority of individuals will use what they learned against the U.S., Mr. Cooper said that a few hackers could do a tremendous amount of damage, especially if they were able to gain control of the systems that run a nuclear power plant or other sensitive infrastructure. A blog post on this story can be found at [http://www.informationweek.com/blog/main/archives/2009/06/exdhs\\_cio\\_hacke.html;jsessionid=MNKDEPHGQ2COYQSNDLPCKHSCJUNN2JVN?cid=nl\\_IW\\_daily\\_html](http://www.informationweek.com/blog/main/archives/2009/06/exdhs_cio_hacke.html;jsessionid=MNKDEPHGQ2COYQSNDLPCKHSCJUNN2JVN?cid=nl_IW_daily_html)

---

## **JUDGE DISMISSES SOFTWARE-LICENSING CASE AGAINST GEORGE MASON UNIVERSITY**

On June 5th, 2009, a Virginia Circuit Court judge dismissed a lawsuit brought against George Mason University's (GMU) Center for History and New Media by Thomson Reuters, Inc. The suit alleged that the university's support of the open source Zotero project was in contravention of the university's license to EndNote. Specifically, Thomson Reuters accused GMU of violating its site license to EndNote software by supporting the development of Zotero, which has the ability to import and use EndNote reference style files. The court has yet to post details as to the grounds for the dismissal; however, some people have suggested it may have been dismissed simply on procedural grounds. While the exact reasoning behind the dismissal of this case is unclear, many have posited that, at the very least, this case proves that educational institutions are not immune from commercial software lawsuits. Thomson Reuters's complaint can be found at <http://www.courthousenews.com/2008/09/17/ReutersvVirginia.pdf>

---

## **NEW NEVADA LAW REQUIRES HARDWARE AND MOBILE DEVICE ENCRYPTION**

On June 10th, 2009, the Association of Corporate Counsel reported that the state of Nevada has changed its data security law to require businesses that transfer personal information outside the controls of the data collector or its data storage contractor to encrypt the information. The law requires data collectors in Nevada to encrypt both electronic communications and any data storage device containing an individual's personal information. The major amendment to the law is a broader definition of the phrase "data storage devices." The amended law now defines data storage devices to include any device that stores information or data, including but not limited to computers, cell phones, and electric and optical computer drives. Additionally, the law promulgates the standard for encryption and requires that the encryption technology used render the data indecipherable without using an associated cryptographic key. Further, the amended law states that businesses accepting credit or debit cards must meet the payment card industry security standards. Finally, the law contains an immunity provision that says data collectors are not liable for damages when they have complied with the terms of the amended law and the breach was not caused by gross negligence or intentional misconduct of the business or its officers, employees, or agents. The amendments will take effect on January 1st, 2010. For more information, the amended law can be found at [https://www.leg.state.nv.us/75th2009/Bills/SB/SB227\\_EN.pdf](https://www.leg.state.nv.us/75th2009/Bills/SB/SB227_EN.pdf)

---

## **IRANIANS FIND WAYS TO BYPASS NET CENSORS**

On June 17th, 2009, cnet reported that Iranian citizens have bypassed the country's censorial Internet restrictions—one of the world's most restrictive Internet blockades—and have leaked information regarding Iran's internal turmoil resulting from the recent election. Many new restrictions popped up right about the time of the election. One way Iranian citizens have been able to circumvent the government's restrictions is to redirect Web browsing through a proxy, thereby making the task of blocking that individual server almost impossible. Additionally, Iranians have employed the use of the Tor anonymizing network. In its simplest form, Tor makes it difficult for government agencies to monitor the connection. In an effort to aid in the dissemination of information, a multitude of Websites have provided information and tips to Iranians seeking ways to bypass the country's strict regulations. Several human rights groups have emphasized that although Iranians may not have reliable Internet connections, their voice is nevertheless important and is being heard. One such website offering information to Iranians regarding ways to bypass Iran's censorial restrictions can be found online at <http://proxyssetupforiran.blogspot.com/>

---

## **FAKE MICROSOFT PATCH-THEMED MALWARE CAMPAIGNS SPREADING**

On June 18th, 2009, cnet reported that up to three new malware campaigns—each using fake Microsoft patch themes—are currently active and are being used as a tactic to spread over e-mail. The first campaign purports to offer Conficker removal tools and is being spread as an Important Windows XP/Vista Security Update. This campaign has been active for approximately a week and is similar to another campaign which took place in April. The second campaign is using an Outlook re-configuration and is serving Outlook\_update.exe through both legitimate and compromised websites. Finally, the last campaign claims to be an Update for Microsoft Outlook/Outlook Express, but in reality it is nothing more than a Trojan. The story can be found at <http://blogs.zdnet.com/security/?p=3648>

---

## **GOOGLE URGED TO ENCRYPT ALL SERVICES**

On June 16th, 2009, The Washington Post reported that several top security experts have written a letter urging Google to improve the privacy and security setting of several of its online services including Gmail, Google Docs, and Calendar. Specifically, these individuals have questioned whether Google is taking adequate measures to prevent hackers from hijacking a user's Webmail account or intercepting important information from certain online documents. While Google protects a customer's name and password from cybertheft, many experts are concerned its default settings put the customer at an unnecessary risk. Services such as AdSense, Adwords or Google Health are protected through encryption technology by the default settings; however, that same technology is used sporadically, if at all, on services such as Gmail and Google Docs. In response, Google has cited slower service

speed as the primary reason behind its decision to decline encrypting all of its services. A copy of the letter sent to Google is available at <http://voices.washingtonpost.com/securityfix/google-letter-final.pdf>

---

## **APPLE ADDRESSES IPHONE AND IPOD SECURITY PROBLEMS**

On June 18th, 2009, Information Week reported that Apple released 45 software patches earlier in the week to tackle security problems in its iPhone and iPod Touch devices. While the number of security patches issued is unusual, analysts have pointed out that they have yet to discover any malicious software targeting the iPhone since its inception about two years ago. The report noted that security vulnerabilities are not unique to the iPhone as almost all technology companies struggle to stay one step ahead of hackers. For instance, Research in Motion, Ltd also issued a security patch for its new BlackBerry device. A spokesman for the security software maker McAfee has noted that security patches for mobile devices, especially the popular iPhone, may become much more common as sales for these devices soar and the PC industry slumps. The spokesman emphasized that mobile devices are no longer used simply for phone calls, but now often contain a plethora of personal information. A letter released by Apple addressing the security updates can be found at <http://support.apple.com/kb/HT3639>

---

## **MICROSOFT LAWSUIT CLAIMS AD SERVICE WAS VIOLATED**

On June 17th, 2009, The Wall Street Journal reported that Microsoft has filed a lawsuit against three individuals for improperly manipulating its online advertising service for profit. Seeking approximately \$750,000 in damages, Microsoft alleged that these individuals conjured up a plan—called competitor click fraud—which allowed them to drive up advertising costs for other businesses while creating an advantageous situation for their own. As articulated in the company's claims, the defendants' scheme is alleged to be a specific form of click fraud, in which large groups of people or automated computers are enticed to click on online advertisements without any interest in the products or services being advertised. Microsoft stated that other advertisers began to experience voluminous fraudulent clicks on their advertisements, which instead of promoting their products, endorsed auto insurance and virtual currency services. As a result, these companies soon exceeded their advertising budgets which allowed defendants' own Website advertisements to replace their competitors. This created higher traffic and revenue for the defendants' companies. For more information, The Wall Street Journal's story can be found at <http://www.webguild.org/2009/06/microsoft-lawsuit-claims-ad-service-was-violated.php?more>

---

## **AMAZON SETTLES DISPUTE WITH TOYS 'R' US**

On June 12th, 2009, The Associated Press reported that Amazon.com has agreed to paid Toys 'R' Us \$51 million dollars to settle a long-standing dispute. In 2004, Toysrus.com sued Amazon for allegedly violating an exclusivity agreement by permitting other retailers to sell their wares on the Amazon Web site. Amazon countersued, arguing that Toys 'R' Us had routinely failed to maintain requisite levels of inventory. Last March, a panel of judges for New Jersey's Appeals Court affirmed the lower court's ruling in favor of Toys 'R' Us and sent the case back to the lower court for reconsideration of damages. As a result, Amazon negotiated a settlement agreement where all claims and counterclaims would be dismissed in exchange for a one time payment of \$51 million to Toys 'R' Us. For more information, the Associated Press article can be found at [http://www.google.com/hostednews/ap/article/ALeqM5ida\\_gGv0zQHehPM51DNBkvrwcnuAD98PEAI00](http://www.google.com/hostednews/ap/article/ALeqM5ida_gGv0zQHehPM51DNBkvrwcnuAD98PEAI00)

---

*Bytes in Brief*<sup>®</sup> is a FREE monthly digest of Internet law and technology news delivered to you by e-mail. For members of the legal and business community interested in Internet law and technology developments, *Bytes in Brief* provides a synopsis of related news and links to sources with more expanded coverage. In the time it takes to drink a cup of coffee, *Bytes in Brief* is designed to make sure you are tracking major developments in this fast moving area.

If staying current in this field is important to you and you find yourself buried under unread magazines, newspapers and journals, *Bytes in Brief* can help you stay in touch without a major outlay of time or expense.

To subscribe, enter your e-mail address into the sign-up box below. It will take you offsite to the *Constant Contact* website, where our opt-in only list is maintained and updated. After you confirm your e-mail address, you will receive an e-mail asking for confirmation that you do wish to become a *Bytes In Brief* subscriber. Once you reply to that e-mail, you will be added to the subscription list.

**Subscribe to *Bytes in Brief***

Email:

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

---

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