

# { 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 149 - October 2009

**PLEASE NOTE:** The URLs referenced in Bytes frequently link to newspapers and other current news sources. These links may fail over time. [Click here to visit Sensei's home page at www.senseient.com](http://www.senseient.com)

---

### MICROSOFT FILES APPEAL IN WORD INJUNCTION CASE

On August 25th, Microsoft filed its formal appeal of a patent infringement ruling that had threatened to halt sales of its popular Word program. Recently, a federal judge increased the monetary judgment against Microsoft and issued an injunction barring any sales of Word that included the custom XML code at the crux of the dispute. In its appeal, Microsoft has argued that the judge made several procedural errors and failed to live up to his role as a "gatekeeper." In Microsoft's view, this case stands as a stark example of what can happen in a patent case when a judge abdicates his or her gatekeeping functions. Conversely, i4i has done nothing but praise the ruling and has repeatedly explained that it is not trying to sink Word; it simply wants the infringing code removed. The company has explained that, while it may lack the gargantuan resources of Microsoft, it is counting on the protection of fairness under the U.S. judicial system to help prove that Microsoft is not above the law. Microsoft has already succeeded in securing a minor victory by having the appeals court set a September 23rd hearing to weigh an appeal of the case and potentially hold off the injunction, which is scheduled to go into effect in October. Microsoft could have avoided appealing the matter if it patched the problem, removed the XML function, or reached a settlement agreement with i4i. Dell's brief in support of Microsoft may be found <http://blog.seattlepi.com/microsoft/library/20090828dellbrief.pdf>

---

### SNOW LEOPARD'S MALWARE PROTECTION ONLY SCANS FOR TWO TROJANS

On August 28th, an Intego blog posting explained that Apple's much hyped malware protection, incorporated in its Snow Leopard upgrade, might not provide as much protection as originally thought. In a comparative review, Intego reported that Apple's anti-malware only scans files downloaded with a handful of applications such as Safari, Mail, iChat, Firefox, Entourage, and a few other browsers. According to the review, it is therefore possible that the modest signature bases would be undermined if the user were to download the malware from a BitTorrent application. What's worse, the report noted that Apple's anti-malware function appears to be nothing more than an XProtect.plist file containing five signatures for two of the most popular Mac OS X trojans - OSX.RSPlug and OSX.Iservice. The review concluded by emphasizing that Apple's anti-malware receives only occasional updates via Apple's Software Update, which is troubling because this reliance on the Apple Software Updates can increase the life cycle of a known piece of malware. A copy of the story may be found at <http://blogs.zdnet.com/security/?p=4139>

---

### FACEBOOK KNOWS TOO MUCH, ACLU SAYS IN WARNING OF QUIZZES

On August 26th, MercuryNews.com reported that the ACLU has launched a cautionary Facebook quiz titled "What Do Facebook Quizzes Know About You?" to illustrate how quizzes which seem perfectly harmless can actually release an array of personal data including the user's religion, sexual orientation, political affiliation, photos, events, notes, wall posts, and groups. Since its release, over 8000 participants have taken the quiz, which delivers its answers by opening a window that scrolls biographical data, attributed comments and photos. The group has explained that it hopes the quiz will prompt Facebook to upgrade its privacy default settings for its users; perhaps by changing its default privacy settings so that quizzes and other third-party applications run by a user's friends do not have access to the information on a user's profile without the user's opt-in consent. The ACLU has noted that many Facebook users ignore the generic warnings provided by the applications or don't fully comprehend the

potential risks. Further, a technology fellow with the ACLU warned that private investigators and political entities have been known to create dossiers using technology that automatically scours the web. Thus, an individual bombarded by spam may be targeted simply because of an affiliation posted on Facebook. In response, Facebook announced that it has been actively policing its service and has disabled hundreds of applications, including a few quiz apps, found to be inconsistent with Facebook policies. Further, the social networking giant pointed out that it recently simplified user privacy settings and that more changes are under way. The ACLU quiz may be found at [http://apps.facebook.com/aclunc\\_privacy\\_quiz/](http://apps.facebook.com/aclunc_privacy_quiz/) (registration required)

---

## **SOCIAL NETWORKERS RISK MORE THAN PRIVACY**

On August 27th, a U.K. study reported that personal information on social networks could be used by professional home burglars looking for potential targets. The report explained that close to 40% of individuals using sites such as Facebook and Twitter have posted specifics concerning holiday plans and over 30% have offered status updates during a weekend getaway. Couple these alarming numbers with the fact that a high proportion of people agree to be online friends with strangers and it's a recipe for increased home break-ins. According to Michael Fraser, a reformed burglar and star of the BBC's Beat the Burglar series, there is absolutely no doubt that burglars are using social networks to develop relationships with people to identify likely targets. He believes that burglars gain confidence by learning more about their potential victims, what they are likely to own and when they are likely to be out of the house. Further, Fraser explained that burglars can then use this information in conjunction with other Web sites, like Google Street View, to gain more information on the targeted homes. Those most targeted? Fraser stated that new users of Facebook are prime targets because they are keen to build up their number of "friends" or "followers." Pet owners are also considered good targets because they are often lax in their security measures and generally do not use security systems, such as alarms and motion detectors because of their furry companions. The Digital Criminal Report may be found at <http://files.shareholder.com/downloads/LGEN/734255841x0x314247/f6b2ccd3-9b53-485d-8558-2c65923767d9/DigitalCriminal.pdf>

---

## **TEENAGE GIRL IS FIRST TO BE JAILED FOR BULLYING ON FACEBOOK**

On August 21st, Keeley Houghton, an eighteen-year-old teen from Malvern, Worcestershire, became the first person in Britain to be jailed for bullying on a social networking site. Houghton's conviction came after she updated her status with an extremely disturbing message in which she threatened to kill another teen, Emily Moore. The Facebook threat came after the victim, also eighteen, was approached at a local pub by Houghton who sat next to her and asked if she could "have a huggle [sic]?" After Moore told Houghton to leave her alone or she would call the police, Houghton told her she would give Moore something to "ring the police about." Houghton had told police that she wrote the threats while she was drunk; however, an examination of the Internet records showed that the comments were written around 4 p.m. and then kept on her Facebook page for 24 hours. At trial, Moore explained how she had been victimized by Houghton for four years, suffering not only damage to her home, but also a physical assault. While Houghton wept, the district judge told her that "bullies are by their nature cowards...on this day you did an act of gratuitous nastiness to satisfy your own twisted nature." After entering her guilty plea for harassment, Houghton was sentenced to three months in a young offenders' institution and was also issued with a restraining order banning her from contacting Moore. A copy of the story may be found at <http://www.mirror.co.uk/news/top-stories/2009/08/22/teenager-becomes-first-girl-in-britain-to-be-jailed-for-bullying-on-facebook-115875-21615194/>

---

## **APPLE SHIPS VULNERABLE FLASH VERSION WITH NEW MAC OS**

On September 2nd, an Adobe blog post explained that upgrading to Apple's latest operating system, Snow Leopard, will actually downgrade the latest Adobe System Flash Player to 10.0.23.1, which is not patched against several security problems. This is problematic, as Adobe's programs are an attractive target for hackers who use vulnerabilities in the company's applications to gain control over a PC. In fact, hackers have found ways to create malicious PDF documents that infect an unsuspecting victim's computer when opened. The problems have become so severe and so frequent that Adobe introduced a quarterly patching schedule for two of its popular programs, Acrobat and Reader, timed to coincide with Microsoft's patch releases. Flash Player is unique in that its Settings Manager, which controls the programs security settings, must be accessed through the company's Web site. Once

in the Settings Manager, users can then set how frequently Flash checks for an update â€” 7, 14, 30, or 60-day intervals â€” with the default interval being every 30 days. A blog post on the story may be found at <http://www.sophos.com/blogs/gc/g/2009/09/02/apple-ships-vulnerable-version-flash-snow-leopard/>

---

## **NFL BANS TWEETING BEFORE, DURING, AFTER GAMES**

On August 31st, the NFL announced that players, coaches, and other team personnel were prohibited from using Twitter and updating profiles on Facebook and other social-networking sites during games. Further, the league explained that these individuals were not allowed to tweet or update their profiles 90 minutes before and until post-game interviews are completed. The NFL also prohibited all media attending games from providing game updates through social networks. The organization explained that while a game is in progress, any forms of accounts of the game must be sufficiently time-delayed and limited in amount (e.g., score updates with detail given only in quarterly game updates) so that the accredited organization's game coverage cannot be used as a substitute for, or otherwise approximate, authorized play-by-play accounts. The changes might have been in response to comments made by Bengals wide receiver Chad Ochocinco, who proclaimed that he was going to circumvent the rules and tweet while he played. They might also have been prompted when Donte Stallworth posted several tweets to his Twitter account discussing his suspension and incarceration after he was charged with DUI manslaughter. Whatever the reason, many have agreed that the new rules will be difficult for the NFL to enforce. To do so, the NFL would likely have to monitor each and every social networking site on the Internet. A blog post highlighting the NFL's new social media policy may be found at <http://mashable.com/2009/08/31/nfl-social-media-policy/>

---

## **JUDGE EXTENDS DEADLINE TO DEBATE GOOGLE BOOK DEAL**

On September 3rd, The Associated Press reported that U.S. District Judge Denny Chin has extended the deadline for either protesting or supporting Google's book deal, which would allow the Internet search leader to convert millions of copyrighted books into digital formats so they can be read on computers and other electronic devices. Judge Chin's decision gives the growing number of opponents more time to hone their attack against the settlement agreement. The non-exclusive arrangement has many fearing that the company could emerge as the ringleader of a literary cartel that could effectively control the prices of digital books. These worries even prompted the U.S. Justice Department to open an inquiry into whether Google's book deal would violate any U.S. laws designed to promote competition. Additionally, the Federal Trade Commission has inquired into how much data the company intends to collect about what people are reading and what the company intends to do with the information. In response, Google announced that it will work to ensure that the privacy of online readers is fact not fiction. The settlement agreement hasn't only drawn criticism - many researchers and librarians have supported the idea of having a library accessible around the clock from anywhere with an Internet connection. Google's new draft privacy policy for online books may be found online at <http://books.google.com/googlebooks/privacy.html>

---

## **APPLE PATCHES 10 IPHONE BUGS, 4 QUICKTIME FLAWS**

On September 10th, Apple issued a pair of updates that patched ten vulnerabilities in its iPhone software and four in its QuickTime player program. The iPhone patches cured numerous bugs, from a vulnerability in the iPhone's telephone service that attackers could exploit to disrupt SMS text messaging to a bug which would allow hackers to silently operate smartphone features such as its camera or microphone. Only 2 of the 10 vulnerabilities Apple patched were classified as critical; albeit the company doesn't rank or score flaws, but rather uses the phrasing "arbitrary code execution" to denote vulnerabilities that could be used by attackers to gain complete control of the iPhone. Users can either wait for their iPhone to update automatically, or they can retrieve the update manually to obtain the patches. Be aware that your iPhone may not be able to synchronize if you use Exchange 2007. This is because Exchange 2007 enforces on-device data encryption, a real issue for the iPhone. Additionally, Apple also updated QuickTime for both the Mac and Windows to version 7.6.4, fixing four flaws, all critical. All of the QuickTime vulnerabilities involved the program's handling of file formats. Two related to improper parsing of H.264 movie files, while the remaining pair were due to issues in handling MPEG-4 video files and FlashPix image files. Apple was quick to point out that updating to QuickTime 7.6.4 will disable the QuickTime Pro functionality of versions earlier than version 7. The company acknowledged that QuickTime 6 Pro users, for example, will need to buy the \$29.99 QuickTime 7 Pro activation code to restore the lost features if they upgrade to 7.6.4. Apple's

explanation about the security content of iPhone OS 3.1 and iPhone OS 3.1.1 for iPod Touch may be found at <http://support.apple.com/kb/HT3860>

---

## **MICROSOFT, YAHOO SEARCH DEAL FACES DOJ SCRUTINY**

On September 11th, Microsoft confirmed that the U.S. Department of Justice will conduct an in-depth anti-trust review into its search deal with Yahoo. Under the 10-year agreement, Microsoft's Bing search engine will power Yahoo's search site, and Yahoo will sell premium search advertising services for both companies. Additionally, Microsoft will have an exclusive license to Yahoo's core search technologies as well as the ability to integrate them into Bing. The goal of the deal, according to Microsoft and Yahoo, is to provide the companies with more search competition to market-leader Google, who holds a search market share of over 70% in the U.S. Before the deal can take effect, it must clear regulatory approval in both the U.S. and in Europe; however, it's still unclear whether the European Union will undertake a formal review of the agreement. Further information may be found at <http://www.infoworld.com/t/mergers-and-acquisitions/microsoft-yahoo-search-deal-faces-doj-scrutiny-407>

---

## **BILL WOULD GIVE PRESIDENT EMERGENCY CONTROL OF INTERNET**

On August 28th, CNET News reported that aides to Sen. Jay Rockefeller have been working on a revised Senate bill, which appears to permit the President the ability to seize temporary control of private-sector networks during a so-called cybersecurity emergency. The new version grants the President the authority to declare an emergency relating to non-governmental computer networks and then to do what is necessary to respond to the threat. A Senate source familiar with the bill compared the President's power to what President Bush had when he grounded all aircraft on September 11, 2009. Additionally, Rockefeller's revised legislation seeks to reshuffle the way the federal government addresses cybersecurity. It requires a "cybersecurity workforce plan" from every federal agency, a "dashboard" pilot project, measurements of hiring effectiveness, and the implementation of a "comprehensive national cybersecurity strategy" in six months--even though its mandatory legal review will take a year to complete. Other sections would allow a federal certification program for cybersecurity professionals and require that certain computer systems and networks in the private sector be managed by people who have been awarded that license. This bill, like its predecessor, has troubled some, in large part because it is very vague. In fact, Larry Clinton, president of the Internet Security Alliance, has noted that it appears unclear what authority Sen. Rockefeller thinks is necessary over the private sector and emphasized that, until clarified, members of the Alliance would not back the proposed bill. Others are worried about the privacy implications of the bill. An excerpt of the proposed bill may be found at <http://www.politechbot.com/docs/rockefeller.revised.cybersecurity.draft.082709.pdf>

---

## **FIRST U.S. INTERNET ADDICTION CENTER OPENS**

On September 4th, USA Today reported on what has been claimed to be the first residential treatment center for Internet addiction in the United States. The center, called ReStart, is located in Seattle and for \$14,000 offers a 45-day program intended to help people wean themselves from pathological computer use. While Internet addiction is not recognized as a separate disorder by the American Psychiatric Association and treatment is not generally covered by insurance, there are many treatment centers in China, South Korea, and Taiwan. In these countries, Internet addiction is taken very seriously and many psychiatric experts have argued that Internet addiction is very real and very harmful. Addiction warning signs vary, but some include being preoccupied with thoughts of the Internet; using it longer than intended, and for increasing amounts of time; repeatedly making unsuccessful efforts to control use; and jeopardizing relationships, school or work to spend time online. And the effects of addiction are no joke. They can range from loss of a job or marriage to even death from playing video games for days without a break, generally stemming from a blood clot associated with being sedentary. To combat these problems, ReStart uses the cold turkey approach. A patient's days are spent in counseling and psychotherapy sessions, doing household chores, working on the grounds, going on outings, exercising and performing other common household tasks. Some have questioned whether this is the appropriate way to respond to this problem. Some experts have argued that Internet addiction is merely a symptom of other mental illness and that unless we treat a patient's underlying problems, new forms of addiction will pop up down the road. Whether Internet addiction is simply a symptom of an underlying problem or its own separate mental illness, it is clear that the Internet is here to stay and the problems associated with it are too. A copy of the story may be found at [http://www.usatoday.com/tech/news/2009-09-03-internet-addiction\\_N.htm](http://www.usatoday.com/tech/news/2009-09-03-internet-addiction_N.htm)

---

## **PASSWORD HACKERS ARE SLIPPERY TO COLLAR**

On September 7th, The Washington Post reported on the thriving underground business of password hacking. In fact, Web sites such as YourHackerz.com, piratecrackers.com, and hackmail.net are still active and all boast of having little trouble hacking into such Web-based e-mail systems as AOL, Yahoo, Gmail, Facebook and Hotmail. And, according to most experts, there doesn't appear to be much anyone can do about it. If a hacker is competent and spends the time and targets an individual, the hacker is likely to be successful. In fact, experts explained that there are numerous ways to steal someone's e-mail password, from simply guessing at family names or pet names to high-tech infiltration. The most common method is to send the target a link to a greeting card or anything else that they might specifically be interested in. When the target opens the link, software is installed on his or her computer that snatches the password the next time it's typed in and sends it to the hacker. Web-based e-mail can also be attacked through bugs in the Web browser. Further, while Federal law prohibits hacking into e-mail, without further illegal activity it's only a misdemeanor. A law professor at George Washington University explained that the feds usually don't have the resources to investigate and prosecute misdemeanors and it is hard to know when an account has been compromised, because e-mail snooping doesn't usually leave a trace. Moreover, a spokesman for the FBI explained that the organization cannot police the Internet and that it cannot investigate an online service without evidence of a particular crime in the United States. There are however, a few tips to help prevent hackers from obtaining your passwords. Beware of malware, such as viruses, worms and keystroke loggers, choose the least risky communication channels, use encryption or use different passwords for everything. A copy of the story may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2009/09/06/AR2009090602238.html>

---

## **HACKERS TARGETING WEB 2.0 SITES AT ALARMING RATE**

On September 16th, an Acunetix Security Blog post reported that social networking and user-generated sites have become the new hotspot for spam, spyware and phishers. Alarming, the number of malicious sites between January and June grew 233 percent over the second half of 2008, and 671 percent compared to the same period last year. According to a report published by the security software maker Websense, 95 percent of the user-generated comments on blogs, message boards and chatrooms are either spam or malicious. One Websense researcher explained that the very aspects of Web 2.0 sites which have made them so revolutionary—the dynamic nature of content on the sites, the ability for anyone to easily create and post content, and the trust that users have for others in their online networks—are the same characteristics that radically raise the potential for abuse. Further compounding the problem, these open and largely unsupervised forums typically lack the security applications and processes needed to weed out the bad guys. In fact, Websense security experts said that community-driven security tools, which enable users to report inappropriate content, on sites including YouTube and BlogSpot are 65 percent to 75 percent ineffective in protecting Web users from objectionable content and security risks. The report went on to explain that sites that allow user-generated content make up the majority of the top 50 most active distributors of malware. In addition, 61 percent of the top 100 sites either hosted malicious content or redirected users to malicious sites without their knowledge. Perhaps Sam Masiello, director of threat management at McAfee's MX Logic security team, put it best: spammers know where to go to get the most bang for their buck. And right now, that place is social networking and user-generated sites. The report issued by Websense may be found at [http://www.websense.com/site/docs/whitepapers/en/WSL\\_Q1\\_Q2\\_2009\\_FNL.PDF](http://www.websense.com/site/docs/whitepapers/en/WSL_Q1_Q2_2009_FNL.PDF)

---

## **GOOGLE TO REINCARNATE DIGITAL BOOKS AS PAPERBACKS**

On September 17th, Google announced that it would be opening up part of its digital library to the maker of a high-speed publishing machine that can manufacture a paperback-bound book in under five minutes. The service has been seen as an acknowledgment by the Internet search leader that not everyone wants their books in digitized form. While the machine itself is not new and has been used worldwide, the Harvard Book Store will be among the first already equipped with an instant-publishing machine to access Google's digital library. Books published by the machine will have a recommended sales price of around \$8 per copy, with On Demand Books, the machine's maker, receiving \$1 of each sale and another \$1 going to Google, although the Internet search leader explained that it will donate its commission to charities and other nonprofit causes. The deal does come with some limits though. For starters, Google is only permitting publications from the section of its digital library that consists of two million books no longer protected by copyright—including those classics like "Moby Dick" and the "Adventures of Huckleberry Finn." However, if Google gets federal court approval of a class-action settlement that would grant it

the right to sell copyrighted books no longer being published, millions of other titles could be added to On Demand's virtual inventory. Even if the settlement is denied the CEO of On Demand Books stated he is thrilled just to have the rights to publish selections from Google's digital library of public domain books. Further information may be found at

[http://www.google.com/hostednews/ap/article/ALeqM5hmkCQJVoiANDaVf5tsxOw\\_4fvi\\_AD9AORBBG3](http://www.google.com/hostednews/ap/article/ALeqM5hmkCQJVoiANDaVf5tsxOw_4fvi_AD9AORBBG3)

---

## **SECURITY PROS ARE FOCUSED ON THE WRONG THREATS**

On September 15th, a biannual report from the SANS Institute, a training organization for computer security professionals, explained that corporate information technology departments are focusing on the wrong threats to their computer systems. The report noted that IT departments are prioritizing old problems and leaving their companies open to a multitude of new cyberattacks, which seek to steal private customer and corporate information. The report weighed two sets of data in coming to its conclusion: data on the most common attacks hitting corporate networks and data on which vulnerabilities are most prevalent on company networks. In so doing, the data revealed that IT professionals are choosing to invest in mitigating less critical risks—flaws in the Windows operating system—rather than combating the new quiet attacks on desktop programs such as Microsoft's Office, Adobe's Flash Player, Adobe Acrobat programs, Java applications, and Apple's QuickTime program. These attacks have quickly accounted for approximately 10% of the attack volume and are likely to be far more successful, since more than 90% of corporate computers are using old, unsecured versions of these programs. Attackers are very opportunistic and will work the easiest-to-use vulnerability that will give them the biggest return; a fact that explains in part why attacks on company Web sites have skyrocketed. So far, cybercriminals have been very successful in stealing proprietary information, like trade secrets and customer data, through the implementation of these kinds of attacks. McAfee estimated that in 2008 alone, companies around the world lost more than \$1 trillion because of this sort of intellectual-property and data theft. Making matters worse, hackers often turn these victimized sites into tools for distributing malicious software to the computers of site visitors, turning their machines into zombies that are networked into botnets. The report issued by the SANS institute may be found at <http://www.sans.org/top-cyber-security-risks/>

---

## **FACEBOOK FIGHTS VIRGINIA'S DEMAND FOR USER DATA, PHOTOS**

On September 14th, Virginia's Workers Compensation Commission said it was no longer going to levy a \$200-a-day fine on the social-networking site Facebook for refusing to comply with a subpoena from an airline company that previously employed a flight attendant named Shana Hensley. On June 4th, the airline's lawyer issued a subpoena demanding all documents, electronic or otherwise, related directly or indirectly, to all activities, writings, photos, comments, e-mails, and/or postings on Hensley's Facebook account. The subpoena was issued in an attempt to prove that Hensley's back injury was not as severe as she alleged. Facebook initially objected on privacy grounds, reasoning that federal law prohibits divulging user data in response to a subpoena and promising to further litigate this issue by seeking, among other things, an injunction from the federal courts. Specifically, Facebook stated that the request must come from a California court, and that it was overly broad because the federal Electronic Communications Privacy Act (ECPA) protects the privacy of user accounts. Randolph Tabb, a deputy worker's compensation commissioner, granted the airline's request for contempt citations against the social-networking site, ordering the \$200-a-day fine until Facebook complied and produced the requested documents. But, after Facebook refused to budge, the commission retracted the fine. Privacy advocates have applauded Facebook's steadfast approach, likening it to Google's mostly successful effort to fend off a similar subpoena from the Justice Department three years ago. Kevin Bankston, a senior staff attorney at the Electronic Frontier Foundation, explained that the Foundation was glad to see that the rule of law established in O'Grady v. Superior Court is being used to ensure that Facebook content is not being disclosed in violation of federal privacy statutes. However, in a somewhat ironic turn of events, it appears that the subpoena won't be necessary after all—Hensley's lawyer has explained that Hensley has agreed to sign a release authorizing Facebook to disclose the contents of her account to her former employer. Further information is available at [http://news.cnet.com/8301-13578\\_3-10352587-38.html](http://news.cnet.com/8301-13578_3-10352587-38.html)

---

## **ONCE AGAIN, DMCA PROTECTS ONLINE VIDEO SITES**

On September 14th, Wired.com reported that the Digital Millennium Copyright Act (DMCA) has once again

immunized another Web host, the web-video host Veoh. Under the DMCA, Web hosts are given immunity from liability if they remove infringing content at the owners' request via a takedown notice. In Universal Music Group's suit against Veoh, the company claimed that the website was a copyright scofflaw, allowing its users to post material that repeatedly infringed its copyrights; however, the Los Angeles federal judge ruled that Universal failed to establish that the DMCA imposed an obligation on a service provider to implement filtering technology at all, let alone technology from a copyright holder's preferred vendor or on the copyright holder's desired timeline. One interesting line from the court's decision stated that Web hosts do not have to enable copyright-filtering technology, even though many do. Universal has vowed to appeal the court's latest order, explaining that it believed the ruling was wrong because it runs counter to established precedent and legislative intent, and to the express language of the DMCA. A copy of the summary judgment order may be found at <http://www.scribd.com/doc/19740660/UMG-v-Veoh-summary-judgment-order>

---

*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.**