

{ 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 150 - November 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)

REPORT: ONLINE SOCIAL NETWORKING CRITICAL TO THE LEGAL INDUSTRY

In its 2009 Networks for Counsel Study, Leader Networks reported that a global study regarding online social networking by lawyers over the past year revealed that networking remains critical to the legal industry. In fact, the survey showed that the top three most effective means to get business involved networking of some sort. However, despite its importance, lawyers responding to the survey explained that resource constraints make networking more difficult than ever. Still, the use of social networking sites has grown significantly over the past year, with three-quarters of all counsel now reporting that they are members of a social or professional network. The most popular social networking sites have been professional online communities such as LinkedIn and Martindale-Hubbell Connected whereas very few attorneys participate in social bookmarking, microblogging (i.e., Twitter) or online collaboration tools. In fact, the Martindale-Hubbell Connected online community remains the social network that most lawyers feel is likely to deliver on the value proposition of a legal-only network. Additionally, the survey revealed that when attorneys engage in social and professional networking, microblogging, social bookmarking and commenting on content, they are likely to do so at least on a weekly basis. The report also highlighted the different views of corporate and private practice lawyers regarding the benefits of online networking. While corporate counsel identified ease of exchanging information and experiences between peers as the top advantage of an online legal professional network, private practice lawyers most valued the ability to increase visibility among peers. The survey concluded by noting that lawyers and private counsel agree that online networking will likely change the practice of law over the next five years. The survey may be found at http://www.leadernetworks.com/documents/Networks_for_Counsel_2009.pdf

ICANN FREED FROM US GOVERNMENT OVERSIGHT

On September 30th, *PCWorld.com* reported that ICANN and the U.S. Department of Commerce have agreed to set up international oversight of the DNS organization, which allows the nonprofit greater independence while giving more countries oversight of the organization. The new agreement sets up reviews of ICANN's performance every three years with members of ICANN, the Department of Commerce, independent experts and others serving on the review teams. The new agreement commits ICANN to a multi-stakeholder, private sector led, bottom-up policy development model for DNS technical coordination and requires the organization to adhere to transparent and accountable budgeting processes, fact-based policy development, cross-community deliberations, and responsive consultation procedures that provide detailed explanations of the basis for decisions. Paul Levins, the vice president at ICANN, explained that the new agreement was a huge moment, not for just ICANN but for the Internet. Additionally, ICANN's CEO stated that this agreement announced that ICANN was now a global organization. He noted that while the U.S. government will have one seat at the table for the three year reviews, all the reviews and all the work done will be submitted for public comment to the world. Proponents of the agreement have long argued that the U.S. had too much control over ICANN and are pleased that this new agreement ends unilateral review of ICANN by the Department of Commerce and sets up independent review panels. Viviane Reding, the European Union's commissioner for information society and media, announced that she believes that this reform can find broad acceptance among civil society, businesses and governments alike if it is effectively and transparently implemented. However, the agreement doesn't change the Department of Commerce's contract with ICANN to perform the functions of the Internet Assigned Numbers Authority (IANA), which is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources. Additionally, the Department of Commerce explained that it does not endorse ICANN's efforts to allow an unlimited number of new generic top-level domains such as .food or .basketball. A copy of the agreement between ICANN and the U.S. Department of Commerce may be found at <http://icann.org/en/announcements/announcement-30sep09-en.htm>

VIRTUAL TOWN NOT COMPANY TOWN FOR PURPOSES OF FIRST AMENDMENT

On September 2nd, a federal district court held that a virtual world that includes homes, offices, and shops is simply an entertainment space, not a company town that would liken the operator to the government for purposes of the First Amendment. In so holding, the court dismissed a claim brought against Sony, finding that Sony was not acting as the government in its virtual world and was thus not obligated to allow participants the free speech guaranteed by the Constitution. The suit was brought after Sony barred Erik Estavillo from commenting in a public forum after he purportedly violated the Sony terms of use. Estavillo sued, claiming that Sony had violated his First Amendment right to free speech. However, as explained by Judge Ronald M. White, the First Amendment guarantee of free speech is only a guarantee against abridgment by state and federal governments. While exceptions exist for company towns that operate as governmental entities and private actors with a functional or structural nexus to the government, the court found that Sony qualified as neither. The court first noted that the company town exception arose from *Marsh v. Alabama*; however, unlike the corporation in *Marsh*, Sony was merely providing a robust commercial product and was not performing the full spectrum of municipal powers and standing in the shoes of the State. Thus, the court held that Sony's network is not similar to a company town. Additionally, the court ruled that Sony lacked a significant nexus to the government, so was ineligible for the governmental nexus exception as well. Here, the court noted that the Ninth Circuit has explained in *Hall v. American National Red Cross* that First Amendment obligations should attach to companies displaying either a structural or functional nexus to the government. The court said that the Sony network lacked either nexus. According to the court, the network was not created to further government objectives. The government retained no permanent authority to appoint any directors of Sony or the Network, or any other private body associated with the Network. Moreover, there was no indication that Sony had assumed functions traditionally reserved to the government, or that the government had any part in encouraging Sony to create the network. As such, the court dismissed the First Amendment complaint and, in declining to extend its supplemental jurisdiction to the plaintiff's remaining state law claims, the court dismissed those claims as well. The court's order granting Sony's motion to dismiss may be found at http://pub.bna.com/eclr/09cv3007_092209.pdf

SMART GRID VULNERABILITIES COULD CAUSE WIDESPREAD DISRUPTIONS

On September 30th, *InfoWorld.com* reported that a cybersecurity coordination task force has released a report assessing various security and privacy requirements for the U.S. Smart Grid, as well as strategies needed to address them. Opponents are concerned that the software, wireless sensor networks, and the Advanced Metering Infrastructure (AMI) networks that go into a smart grid present too many points of vulnerability into the network. These concerns do not appear to be unfounded. In June, security consultancy IOActive explained that its researchers had discovered several vulnerabilities that could allow attackers to access the network and cut off power. IOActive researchers showed how attackers could spread malware through the network and remotely shut down power to consumers by taking advantage of flaws in the metering devices. However, this report has been viewed as an attempt to assess such threats, highlighting the need for planners to address everything from deliberate attacks to inadvertent compromises. The report looked at vulnerabilities that can arise during the operation of a smart grid as well as problems such as authenticating and authorizing users to substations, key management for meters, and intrusion detection for power equipment. The report also considered vulnerabilities arising from inadequate patching; configuration and change management processes; weak access controls; and lack of risk assessment, audit, management, and incident response plans. Additionally, the report noted that vulnerabilities associated with bad software coding practices, including input validation errors and user authentication errors, can also pose a risk to the integrity of a smart grid. Apart from the threat of cyber attacks, the real-time, two-way communication between consumers and suppliers in a smart grid also raises several privacy concerns. The report explained that there needs to be more of an understanding of how that collected data will be distributed throughout the smart grid system. A copy of the NIST report may be found at http://www.nist.gov/public_affairs/releases/smartgrid_interoperability.pdf

SURVEY: U.S. DRIVERS SAY TEXTING WHILE DRIVING SHOULD BE BANNED; VOICE TECHNOLOGY SEEN AS SAFER

On September 25th, a national survey conducted by Penn, Schoen & Berland Associates on behalf of the Ford Motor Company showed that 86 percent of U.S. drivers described handheld texting while driving as very dangerous, with 93 percent supporting a nationwide ban on texting. However, only 42 percent of those questioned believed drivers would stop texting behind the wheel if the practice was banned. This number increased dramatically—to 75 percent—if hands-free or voice-activated technologies were widely available. In fact, the survey showed that 67 percent of drivers

believed voice-activated technology is a safe alternative to texting, and 76 percent said such a feature would be an appealing feature in a car. According to Jim Vondale, the director of Ford's Automotive Safety Office, research demonstrates that any activity that draws drivers' eyes away from the road for an extended period while driving substantially increases the risk of accidents. Ford has stated it supports a nationwide ban on handheld texting while driving; explaining that the safety concerns associated with texting while driving prompted the company's hands-free and voice-activated technologies to allow drivers to remain connected, but to do so while keeping their hands on the wheel and their eyes on the road. Currently, 18 states have enacted bans on handheld cell phone use and/or texting while driving; however, close to 40 percent of drivers in these states indicated that they were unaware of the ban in their own state. An article on reducing driving distractions may be found at http://media.ford.com/images/10031/Reducing_Driver_Distraction.pdf

HOMELAND SECURITY TO HIRE UP TO 1K CYBER EXPERTS

On October 1st, the *Associated Press* reported that the Homeland Security Department has been approved to be more competitive and selective in hiring up to 1,000 new cyber experts; a move designed to fulfill its promise to bolster security of the nation's computer networks and improve cyber security as a whole. The Obama administration's approval of the hiring plan gives Department of Homeland Security (DHS) officials far greater flexibility to hire whomever they want and pay what they want compared to other federal organizations. Homeland Security Secretary Janet Napolitano explained that her department does not anticipate filling all 1,000 positions, which include a wide range of positions—from cyber analysts to developers and engineers who can detect, investigate and deter cyber attacks. But regardless, the hiring push underscores the administration's struggle to better organize and manage the country's vulnerable digital defenses. In fact, the President has yet to fill the difficult position of cyber coordinator. More information may be found at <http://www.physorg.com/news173639118.html>

EMPLOYERS GRAPPLING WITH SOCIAL NETWORK USE

On September 23rd, the Society of Corporate Compliance and Ethics and the Health Care Compliance Association released a survey which reported that over 50 percent of the companies questioned have no policy to address the use of social networking outside the workplace. While, in general, companies have shied away from restricting an employee's actions off the job, businesses still have reasons to be concerned about employees who use social networking—including revealing proprietary information or posting inappropriate pictures that could embarrass the organization. Of the companies questioned, more than half have no active system to monitor an employee's use of social-networking sites. Thirty four percent have implemented a general employee policy that addresses all online activity, including the use of social networking, both on and off the employer's clock; however, around 32 percent explained that the company acts only when an issue is discovered. The survey reported that 24 percent of all those surveyed said that an employee in their company had been disciplined for inappropriate conduct, while 37 percent admitted that they did not know. The number of reported incidents was slightly skewed towards the nonprofit sector, with 33 percent reporting an employee incident compared to only 13 percent in the for-profit sector. According to the CEO of the Society of Corporate Compliance and Ethics, the report shows that business clearly hasn't caught up with what its employees are doing online. As such, businesses run the risk of employees doing things online that may reflect badly on the company. Additionally, once policies and procedures are developed in this area, employees are going to find that what they have done in the past is no longer acceptable. A copy of the survey may be found at http://www.corporatecompliance.org/staticcontent/09SocialNetworksSurvey_report.pdf

SURVEY: HALF OF BUSINESSES DON'T SECURE PERSONAL DATA

On September 23rd, a survey released by Imperva and Ponemon Institute reported that the personal information given to businesses may not be as secure as one would hope. The survey was conducted to ascertain how many companies are complying with the Payment Card Industry's Data Security Standard (PCIDSS). The standard was established to ensure that businesses take certain steps to secure their Web sites, databases, and other systems that process and store credit card information. According to the survey, approximately 55 percent of all businesses admit that they secure credit card information but not Social Security numbers, bank account details, and other personal data. Further, 71 percent acknowledge that, despite previously being hit by one or more data breaches, data security is not a top priority. Many of the companies explained that cost and lack of resources were the biggest reasons for not focusing more on PCIDSS compliance. In fact, Imperva's chief technology officer explained that, typically, companies devote 35 percent of their IT security budget to PCI compliance, making cost a significant problem, especially for smaller

businesses. The priorities of the organization itself can further compound the problems of PCI compliance. Of those surveyed, 55 percent believed that their CEO did not strongly support PCIDSS compliance, while 52 percent noted that their company is not proactive in managing privacy or security risks. The survey wasn't all bad news as approximately 75 percent of those surveyed stated that their company achieved some level of compliance, with 28 percent compliant for most of their applications and databases and 25 percent compliant for some apps and databases. Still, only 22 percent reported being fully compliant meaning that business still has a long way to go. The survey can be downloaded at <https://www.imperva.com/ld/ponemon.asp> (registration required)

SECURITY RESEARCHER SHOWS HOW HACKERS SPY ON BLACKBERRY AND OTHER SMARTPHONES

On October 7th, a security researcher showed ways to spy on a BlackBerry user, including listening to phone conversations, stealing contact lists, reading text messages, taking and viewing photos, and figuring out the handset's location via GPS—even after stating that the BlackBerry is one of the most secure smartphones available. Because hacking into a BlackBerry is impossible, hackers have relied on social engineering to gain control of a user's device. Social engineering involves tricking someone into loading spyware onto a device or finding some other way to install malware onto the victim's device, such as inserting a compromised MicroSD card. One way hackers have enticed BlackBerry users to download spyware onto their smartphones is by offering a free application that appears harmless, but, in reality, contains a small piece of software that can allow a hacker to do all kinds of things on the device. While people tend to put a lot of personal data on their smartphone, the risk of data theft isn't the only problem. Once installed, spyware could be used to intercept a phone call and let the hacker listen in to the conversation. It could also forward incoming and outgoing text messages to the hacker or even run up the victim's phone bill by making international calls. In one recent example of a massive installation of spyware on BlackBerry phones, the United Arab Emirates mobile phone service provider Etisalat told its users to download a software upgrade that turned out to be spyware. The spyware then forwarded the phone's e-mails to a central server. Luckily, the ploy was discovered shortly thereafter because the software drained the phone's battery at an excessive rate. Users can protect themselves from spyware by not installing random pieces of software and making sure they know what they are actually installing. Further, while it isn't a good idea to let anyone else use your smartphone, if you do hand over your phone, keep an eye on it. Finally, always enable a device password in case your device is lost or stolen. A copy of the story may be found at http://www.infoworld.com/d/security-central/security-researcher-shows-how-hackers-spy-blackberry-and-other-smartphones-895?page=0,1&source=rss_security_central

PHISHING SCAM ARRESTS HIGHLIGHT MASSIVE PROBLEM ON THE WEB

On October 7th, authorities in the U.S. and Egypt indicted 100 people on various charges related to a massive phishing scam that victimized thousands of customers of two major U.S. banks. The FBI has described the bust, called Operation Phish Phry, as the largest cyber-crime investigation and has held it up as a shining example of international cooperation against cyber-criminals; however, many have said that the arrests barely scratch the surface of the phishing problem. According to Dave Jevans, chairman of the Anti-Phishing Working Group (APWG), while the arrests send a message to criminals that they are not immune and that they can be tracked down and jailed, these arrests were not going to materially impact the problem. In fact, as of June, the APWG had detected over 49,000 unique phishing Web sites and as Jevans noted, the problem just continues to grow and get worse. A former cyber-crime prosecutor explained that phishing is so hard to combat because attacks can be launched from anywhere in the world by individuals with little to no technical skills. Tracking down the source of an attack might require communicating with numerous ISPs in different countries, different time zones and using different languages. Further, many phishing attacks use fast-flux networks, which allow an attacker to move counterfeit Web sites to new servers in rapid succession, to make tracking them down even harder. And, according to Jevans, a large majority of the servers hosting a phishing Web site have themselves been compromised and belong to legitimate companies. Making matters worse, tools are available that allow attackers to create authentic user sites that can trick even the most aware users. Moreover, certain malware programs are capable of stealing an individual's account names and passwords directly from an online session, and can even redirect the browser to a fake Web site—all without requiring the user's knowledge or participation. A report on the phishing activity trends for the first half of 2009 may be found at http://www.antiphishing.org/reports/apwg_report_h1_2009.pdf

JUDGE TOSSES DART'S SUIT VS. CRAIGSLIST

On October 22nd, the *Chicago Sun-Times* reported that a federal judge has dismissed Cook County Sheriff Tom Dart's lawsuit against Craigslist. Dart filed his suit earlier this year, seeking to force the Web site to eliminate the erotic services section that he said his officers have monitored to make hundreds of arrests for prostitution, juvenile pimping and human trafficking. In the court's ruling, Judge John F. Grady held that the ads offering "adult services" were not explicitly offering sex, and that Craigslist is simply an intermediary and is not culpable for aiding and abetting customers who misuse their services to commit unlawful acts. The judge ruled, however, that Cook County was permitted to use Craigslist's Web site to identify and pursue individuals who post allegedly unlawful content, but Sheriff Dart was not permitted to sue Craigslist for their conduct. A copy of the complaint filed by Mr. Dart may be found at <http://docs.justia.com/cases/federal/district-courts/illinois/ilndce/1:2009cv01385/229200/1/>

NOKIA SUES APPLE OVER IPHONE

On October 22nd, an Apple blog posting reported that Nokia has sued Apple for allegedly infringing patents on technology used in the iPhone. Nokia has claimed that the ten alleged patent infringements apply to all iPhones sold thus far. Specifically, the allegations relate to three areas of wireless technology: (1) GSM, (2) 3G (UMTS or W-CDMA), and (3) an unnamed wireless local area network (LAN) technology, most likely WiFi. If true, some have speculated that Nokia could grab as much as \$12 per iPhone sold. Once news of the suit broke, Apple's shares declined sharply. A copy of the complaint may be found at <http://www.scribd.com/doc/21458614/Nokia-vs-Apple-Complaint>

DANGER/MICROSOFT BEGINS RESTORING SIDEKICK DATA

On October 20th, Danger/Microsoft announced that it had begun the process of restoring data to Sidekick owners who had been without any of their personal data since a massive outage occurred in early October. Although, initially, many feared that the data might be lost for good, Microsoft explained that it expected to be able to recover most, if not all, of the information; albeit it noted that the process will take some time. In implementing the first phase of the content restoration process, Microsoft posted a tool to T-Mobile's Web site that allows Sidekick owners to restore their address book. In a statement released by the company, Microsoft explained that the tool will enable a customer to view the contacts contained on his or her Sidekick as of October 1. Microsoft went on to state that it is making progress on the next phase in this restoration process, including photographs, notes, to-do lists, marketplace data and high scores. A statement released by Microsoft on the issue may be found at <http://www.microsoft.com/presspass/press/2009/oct09/10-20sidekick.mspx>

CRYPTOGRAPHIC KEYS CAN BE STOLEN FROM MOBILE DEVICES

On Oct 21st, *CNET News* reported that security researchers have discovered a way to steal cryptographic keys that are used encrypt communications and authenticate users on mobile devices by measuring the amount of electricity consumed or the radio frequency emissions. The attack, known as differential power analysis (DPA), can be used to target the victim by using either special equipment that measures electromagnetic signals emitted by chips inside the device or by attaching a sensor to the device's power supply. The cyber criminal can then use an oscilloscope to capture the electrical signals or radio frequency emissions and the data can be analyzed so the spikes and bumps correlate to specific activity around the cryptography. More information may be found at http://news.cnet.com/8301-27080_3-10379115-245.html

BLUE CROSS WARNS DOCTORS ABOUT STOLEN IDENTIFICATION DATA

On October 14th, the *Chicago Tribune* reported that nearly every practicing physician in the country is being warned that business and personal information may be susceptible to a possible breach after an employee of Blue Cross and Blue Shield Association broke protocol and transferred information to an unencrypted personal laptop, which was later stolen in late August. The Blue Cross and Blue Shield Association reported that no patient information was in the database and that no doctors have reported any security breaches to date; however, between 16 to 20 percent of the doctors listed in the database have their Social Security numbers as their medical-care provider identification, putting these health professionals at a potential risk for identity theft. A spokesman for the Blue Cross and Blue Shield stated that the company believes that the incident was a random criminal act, but noted that the company takes any breach seriously and has been taking precautionary actions. Dr. Jame Rohack, the president of the American Medical

Association, solidified the spokesman remarks, explaining that the data set was stored on a laptop that was stolen from a car, which was one of several cars in the immediate vicinity that were vandalized. In his opinion, there is no reason to believe that the thief intended to use the data to commit identity theft. Even so, the Blue Cross and Blue Shield Association is offering credit monitoring services to those providers whose Social Security number was exposed as an added precaution. More information may be found at <http://www.chicagotribune.com/business/chi-biz-doctors-identification-stolen-,0,7997066.story>

YAHOO SETTLES PAY-PER-CLICK FRAUD SUIT

On October 13th, *CNET News* reported that Yahoo has settled its long-standing lawsuit regarding pay-per-click ads sold by the Internet service provider that ended up in some shady corners of the Web. In 2006, a group of advertisers sued Yahoo, alleging that Yahoo sold them ads that were promised to appear on highly targeted sites and instead wound up on Web sites filed with spyware or run by typo squatters. In reaching an agreement with the advertisers, Yahoo was not forced to admit any wrongdoing, but has agreed to change the way it sells certain ads across its sites. In particular, Yahoo will create an "Ad Placement Option" for advertisers to guarantee their ads will appear only on sites owned by Yahoo or sites designated as "premium" partners. Additionally, advertisers will get better tools for measuring traffic quality and potentially troubling sites bearing their ads. Yahoo has explained that the deal will still be effective even assuming it obtains regulatory approval to outsource its search business to Microsoft. The settlement agreement may be found at <https://secureweb.rustconsulting.com/inreyahoosettlement/settlementnotice.htm>

GROWTH OF FACEBOOK LEAVES MYSPACE IN DUST

On October 13th, *CNET News* reported that Facebook and Twitter have become increasingly popular while MySpace has slowly gone by the wayside. According to the Internet monitoring company Experian Hitwise, Facebook, the No. 1 social network in the U.S., increased its share of all reported visits to social-networking sites from 19 percent in September 2008 to 58.6 percent just one year later. Over the same period, Twitter's share jumped from .15 percent to 1.84 percent, placing it squarely as the fourth largest social network site. While MySpace is still in second place behind Facebook and boasts 30 percent of the social-networking market, last year at this time, the company captured over 66 percent of the market. To quell the freefall, MySpace has explained that it is attempting to remake itself into an entertainment portal and has stated that it is in the process of developing more compelling music and video services. Overall, Experian Hitwise, which tracks 155 social networking sites, noted that U.S. visits to such sites rose 62 percent from September 2008 to September 2009. More information may be found at http://news.cnet.com/8301-31001_3-10374324-261.html?part=rss&subj=news&tag=2547-1_3-0-20

FCC LAUNCHES PROBE OF GOOGLE VOICE SERVICE

On October 9th, the Federal Communications Commission (FCC) sent a letter to Google requesting information about its Voice service after AT&T complained that Google's free messaging and calling service, Google Voice, blocks calls to rural communities where local phone companies charge high connection fees. This is allegedly to reduce access charges Google must pay; a practice larger phone companies are prohibited from employing due to common carrier regulations. Richard Whitt, Google's Washington telecom and media counsel, explained in a blog post that Google Voice only restricts calls to phone numbers held by companies that charge exorbitant termination rates for calls and partner with adult sex chat lines and free conference calling centers to drive high volumes of traffic. He further noted that Google would be forced to drop the service if the company was required to pay these ludicrously high charges. Moreover, Google has maintained that its Voice service should not be subject to common carrier laws because it is a free, Web-based software application and not a replacement for traditional phone service. With the complaint coming as the FCC prepares to vote on the network neutrality rules, some have posited that the AT&T complaint was an attempt to turn the tables on Google, with AT&T claiming that Google Voice flouts net neutrality principles by blocking certain calling traffic. However, Whitt said that despite AT&T's lobbying efforts, this issue has nothing to do with network neutrality or rural America. The FCC is requesting that Google explain how its Voice service works, whether it blocks calls to certain numbers and whether it informs users that it does so. A copy of the letter sent to Google may be found at http://www.wired.com/images_blogs/epicenter/2009/10/letter-to-google.pdf

HP CEO SAYS EXTERNAL CLOUDS NOT SECURE

On October 21st, *InfoWorld* reported that while Hewlett-Packard's CEO Mark Hurd has explained that there is much to like about the cloud computing environment, more work is needed before cloud services, specifically those located outside the firewall, can offer enough security. Hurd cited the 1,000 plus hack attacks fended off daily to support his position that it was unlikely that anyone could put anything of material importance outside the firewall and keep it 100% secure. While he acknowledged that many external cloud services do work, credit card companies, with their vast banks of personal information, are most at risk. More information may be found at <http://www.infoworld.com/d/cloud-computing/hp-ceo-says-external-clouds-not-secure-806>


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, 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  SafeSubscribeSM
For Email Marketing you can trust

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