



ISSUE 156 - MAY 2010

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 home page at www.senseient.com](http://www.senseient.com)

NEW SOFTWARE LETS BUSINESSES TRACK EMPLOYEES' FACEBOOK, TWITTER ACTIVITY

On March 24th, a New York Times blog posting reported that tracking an employee's social networking activity just got a whole lot easier. The news comes after a company called Teneros demonstrated a software-as-a-service product called Social Sentry at the recent DEMO conference. Social Sentry automates the process of examining employee activity on social networking sites. The software isn't simply focused on the amount of time employees spend on these sites while they're supposed to be working, but rather it monitors all public social networking activity in case employees reveal confidential information or make statements that could be damaging to the company. DEMO conference chief Matt Marshall said Social Sentry might seem kind of spooky, but emphasized that the software only tracks public activity, which people could do anyway by manually searching the Web. Companies using the program can get a variety of alerts about employee activity on Facebook, Twitter, LinkedIn, MySpace or YouTube. These alerts can be based on keywords related to products or financial results, or simply to identify foul language. Aside from its ability to identify and monitor employee public communication happening from any location, within the corporate network or on the Internet from other locations, Social Sentry also allows companies to monitor selected users or the entire employee base to eliminate corporate exposure related to communication. Yet, for all its potential, it remains to be seen whether Social Sentry will be effective in preventing loss of confidential information. Once a post is on Twitter, it can go viral in a matter of minutes. More information may be found at <http://bits.blogs.nytimes.com/2010/03/26/keeping-a-closer-eye-on-workers-social-networking/>.

SYMANTEC NAMES RISKIEST U.S. CITIES FOR CYBER CRIME

On March 23rd, Symantec released its list of riskiest U.S. cities when it comes to cyber crime and congratulations Seattle, you're number one! In fact, the Northwest region sports two of the top ten cities, with Portland, Oregon, ranked No. 10 in the list of the nation's 50 largest metro areas. Rounding out the first five spots were Boston, Washington D.C., San Francisco, and Raleigh, N.C. The least dangerous cities were Detroit (No. 50); El Paso, Texas (No. 49); and Memphis, Tenn. (No. 48). Symantec partnered with Sperling's BestPlaces to come up with the rankings, which relied on data from Sperling's security response team for factors including the number of malicious attacks, infected machines, and spam-spewing zombies per capita. Sperling's BestPlaces contributed data on the prevalence of computer ownership, Internet use and potentially risky online activities, including online banking and online shopping. Also factored into the rankings was the number of free Wi-Fi hotspots per capita. Scores were calculated by adding the point totals for each criteria, which were based on their relation to other cities' scores. A city with the total for each factor was scored as 100, while the city with the lowest total was given 0. Seattle received the riskiest city award because it scored in the top 10 in every criteria, and took the No. 2 spots for both Wi-Fi availability and risky behavior. But, like every scoring system, the Symantec ranking doesn't portray the experiences of everyone who lives there. Instead, the report should serve as a cautionary tale: if you spend much of your time online, you need to be more cautious. A copy of the study may be found at http://norton.newslinevine.com/Cybercrime_Exec_Summary.pdf.

WIESENTHAL STUDY DETAILS ONLINE HATE, TERROR GROUPS

On March 22nd, CNET News reported on a recent report by the Simon Wiesenthal Center that highlights the growing number of websites and social networks used by people propagating hateful, racist, or terrorist ideas and activities. The report, which combed through the Web, found more than 11,500 different sites, networks, and forums that it categorized as hateful or terrorist, a number that represented a 20% increase from last year's study. And while the 11,500 sites may just be the tip of the iceberg, the Wiesenthal study notes that it's not just the quantity of sites that alarms the center, it's the trends found among them. The report noted that social networking and online video sites have become popular tools to spread hate and fear. For instance, Facebook is home to a variety of people and groups that urge violence against minorities and certain religions. And sites like YouTube and LiveLink display videos that purportedly show you how to create a binary explosive, such as the type used by "shoe bomber" Richard Reid in 2001 and "underwear bomber" Umar Farouk Abdulmutallab in December 2009. Moreover, the report also found that the Internet is a growing factor among the new "lone wolf" terrorist. The report calls for a consortium approach, noting that laws and protocols are not the answer. Instead, companies need to be directly involved, from their business model and their communities - they have to take these issues into account. While the report itself is not available to the general public because of the sensitive material it contains, more information including an interview with Rabbi Abraham Cooper, associate dean at the Wiesenthal Center, may be found at http://news.cnet.com/8301-1023_3-10469814-93.html.

COURT SAYS BUSH ILLEGALLY WIRETAPPED TWO AMERICANS

On March 31st, a federal judge announced that the George W. Bush administration illegally eavesdropped on the telephone conversations of two American lawyers who represented a now-defunct Saudi charity. The lawyers had argued that some of their 2004 telephone conversations to Saudi Arabia were siphoned to the National Security Agency without warrants; allegations backed by a classified document the government accidentally mailed to the lawyers. However, the document was later declared a state secret and removed from the lawsuit. Because of the evocation of the state secrets privilege, Walker had ruled the lawyers must make their case without the classified document. So their counsel, Jon Eisenberg, amended the case and cited a bevy of circumstantial evidence. It worked. U.S. District Judge Vaughn Walker ruled that the Plaintiffs had put forward enough evidence to establish a prima facie case that they were subjected to warrantless electronic surveillance. More specifically, Judge Walker found that the evidence did in fact demonstrate that the government illegally wiretapped the two lawyers as they spoke on U.S. soil to Saudi Arabia. As a result of the decision, Judge Walker noted that the attorneys are free to ask for monetary damages. But, according to their lawyer, this case is not about recovering money. Instead Eisenberg believes that Judge Walker's decision tells the president, or the next president, that you don't have the power to disregard an act of Congress in the name of national security. The victory, however, might be short-lived should the Justice Department decide to appeal. In 2006, for example, a Detroit federal judge declared Bush's spy program unconstitutional. But a federal appeals court quickly reversed, ruling that the plaintiffs did not have legal standing to bring a case, because they had no evidence to show that their telephone calls specifically were intercepted. The Supreme Court declined to review that ruling. A copy of the decision may be found at http://www.wired.com/images_blogs/threatlevel/2010/03/walker.pdf.

FACEBOOK MULLS PRIVACY CHANGES, CAUSES MORE OUTRAGE

On March 29th, PCWorld.com reported that recent proposed privacy changes by the social networking giant Facebook has left many users crying foul. Under Facebook's current rules, you're asked first if you want to share information (your name, photos and friends list) with third-party sites. The new policy bypasses asking you for approval when visiting some sites and applications Facebook has had business relationships with, sharing limited personal information automatically. While users are able to opt-out of the information sharing, many will not, and may not know of the change. Users have been quite vocal in articulating their distress. There are more than 900 comments on the blog post in which Facebook Deputy General Counsel Michael Richter announced the proposed changes. Most of them are negative, especially concerning the fact that the third-party is opt-out, meaning users will take part by default, rather than opt-in, meaning that a user must expressly choose to take part in the program. Facebook users are understandably sensitive about what the site does with their personal data. In 2007, the site got into hot water over its Beacon program, which logged user activity on third-party sites even when they weren't logged into Facebook, and optionally published that activity to users' profiles. That resulted in a \$9.5 million lawsuit settlement last December. Facebook also retooled user privacy settings in December in hopes that people would make parts of their profiles public. That effort backfired when users realized their friends' lists were

made public even when the rest of their profiles were not, causing Facebook to relent and tweak its settings. A copy of the story may be found at http://www.pcworld.com/article/192816/facebook_mulls_privacy_changes_causes_more_outrage.html.

JUDGE FILES \$50 MILLION DOLLAR SUIT AGAINST NEWSPAPER AND WEBSITE

On April 7th, Judge Shirley Strickland Saffold and her daughter, Sydney Saffold, filed a \$50 million lawsuit against the Cleveland Plain Dealer and Advance Internet after the newspaper alleged the judge may have made anonymous comments on the newspaper's website about cases before the court. The newspaper maintained that a user named "lawmiss," who was connected to an e-mail account registered to Judge Staffold, made several comments regarding cases over which the Judge was presiding. However, according to her attorney, any comments from "lawmiss" were most likely left by the judge's 23-year-old daughter Sydney, an aspiring law student. However, one troubling question remains unanswered. Why did a public records request reveal that a computer in the judge's office was on the website at the time three of the comments were left? E-discovery can surely shed some light on the answer. A copy of the complaint may be found at <http://www.scribd.com/doc/29598727/Saffold-Complaint>.

SON SUES MOTHER OVER FACEBOOK INTERFERENCE

On April 7th, CNET News reported that the 16-year-old son of Denise New has sued his mother for harassment after she allegedly hacked into his Facebook account, changed his password, and posted things about him that he claims were slanderous. But, as Ms. New told a local news station, she believes that she was acting within her legal rights to monitor her child and to have a conversation with her child. What apparently brought this problem to fruition was a Facebook post by the son claiming that he had driven home one night at 95 mph because he was upset with a girl. This appears to have prompted the aforementioned Facebook intervention. Ms. New does not have custody of her son. She says she did not hack into his account, that instead he left his Facebook page open when using his laptop at her home. From the looks of things, Ms. New clearly intends to fight for her right to interject herself into her son's Facebook. As she said herself: "I'm not gonna let this rest. I think this could be a precedent-setting moment for parents." A copy of the story may be found at http://news.cnet.com/8301-17852_3-20001917-71.html.

WHOLE FOODS WORKING TO CURB FACEBOOK-BASED SCAM

On April 2nd, the upscale grocery conglomerate Whole Foods Market announced that it will continue to clamp down on a series of Facebook-based scams that entice users with a purported \$500 gift card from the Austin, Texas-based supermarket chain. The scam has been spreading virally through Facebook via "fan pages" with names like "Whole Foods Market Free \$500 Gift Card Limited - first 12,000 fans only" and "Whole Foods FREE \$500 Gift Card! Only Available for 36 hours!" The fan page asks Facebook users to add it as a fan, thus pushing awareness of the page through those users' Facebook networks, and then asks them to fill out a credit assessment and other forms that request personal information. The scam then uses a form of malware to crash users' computers and the information they have entered is left vulnerable. While Whole Foods has stated that it has been working with Facebook to pull down all the scams, new ones keep popping up. In addition, Whole Foods has also been using its Twitter account to reply to people who have tweeted about the scam or expressed concerns with it, providing answers like, "It's a scam, unaffiliated and unauthorized by us! Please help us report these pages so Facebook can shut them." A copy of the story may be found at http://news.cnet.com/8301-13577_3-20001665-36.html.

COMCAST RULING RAISES QUESTIONS ON FCC REGULATION

On April 6th, a federal court ruled that Comcast could regulate high-speed Internet traffic over its own system and that a company that wanted to push its content through Comcast's pipelines could not. In 2008, the FCC told Comcast and other big high-speed Internet companies that they must treat content that flows through their pipelines equally, whether it's digitally lightweight e-mail or hefty movie files, by pushing it all through at the same speed. Comcast complained that certain kinds of Internet traffic are so heavy that they slow down the entire system and argued that it should be permitted to enforce speed limits on its information highway. In siding with Comcast, the court effectively said that the FCC does not have the authority to regulate net neutrality. As a result

of the decision, the agency is now forced to reconsider the cybersecurity, privacy and consumer-protection policies it had wanted to pursue. But, the FCC could work around the Tuesday ruling with a vote of the five FCC commissioners. Currently, Internet service providers fall under a lightly regulated area of the FCC. It would take only a 3-to-2 vote to move high-speed Internet into one of the FCC's more heavily regulated areas, where the agency could set tough rules on companies such as Comcast. The FCC has yet to declare whether it will appeal the ruling or attempt to work around the court's decision. A copy of the story may be found at http://www.washingtonpost.com/wp-dyn/content/article/2010/04/06/AR2010040600742_2.html.

AFTER GOOGLE-CHINA DUST-UP, CYBER WAR EMERGES AS A THREAT

InfoWorld.com has reported that the recent attacks against Google and more than 30 other tech firms by China-based hackers has stoked long-standing fears over the ability of cyber adversaries to penetrate commercial and government networks in the U.S. Many see the recent attacks as evidence that the U.S. is already in the midst of an undeclared cyber war, with attacks against government targets estimated to have more than doubled in the past two years. And many see the relentless probing and attacks on U.S agencies and commercial interests as a precursor to something more devastating. The concern has prompted all sorts of action in the political sphere, including two new proposed cyber security bills and the possible creation of a cyber security ambassador for the U.N. However, the first step to formulating an organized response is to define cyber war correctly. As Robert Rodriguez, a former Secret Service special agent and founder of the Security Innovation Network, explained, war connotes huge conflict at a grand level between nations and societies and also involves the use of military force to essentially destroy another nation's capabilities and will to resist. Thus, the cyber equivalent of such a conflict would involve a nation using cyber means to attain political ends in another country. Thus, many believe that pronouncements that we are in a cyber war or face cyber terror conflate problems and make effective response more difficult. Whatever the case, as incidents involving cyber espionage and cyber crime grow at an almost exponential rate, many believe that the time has come for the government to formalize a national policy for dealing with cyber threats. Such a policy should clearly define the thresholds at which cyber attacks will be considered an act of war, establish who would be in charge among the different federal agencies that would respond to a cyber crisis, and when they would be allowed to use their authority. In addition, the Department of Defense and the NSA need to have a policy framework in place in case they need to launch crippling cyber offensives of their own in response to a cyber attack. Whether that retaliation means a cyber-counteroffensive or a more conventional military one needs to be figured out as part of U.S. cyber policy before a crisis. More information may be found at <http://www.macworld.com/article/150462/2010/04/cyberwar.html>.

FACEBOOK BEEFS UP SITE AGAINST HACKERS

On April 14th, InfoWorld.com reported that Facebook is employing aggressive legal means in combination with technical measures in order to stop hackers from abusing its social-networking site. For starters, Facebook's security team was formed with just a few people, but now as many as 10 percent of Facebook's 1,200 employees are involved in security-related functions. In addition, Facebook has integrated its security incident response team with its law enforcement team, which allows both groups to use some of the same tools in order to respond to a security incident. On the technical side, Facebook has automated systems that detect when someone is using the site in a way that is different from the normal user. Those systems can then employ countermeasures, such as limiting the number of messages a user can send, employing CAPTCHAs (Completely Automated Public Turing tests to tell Computers and Humans Apart) and disabling accounts. The site has also rewarded individuals who responsibly disclose security problems by giving them credit on its security page, and, if it's a really good hack, the social networking giant will probably end up hiring you. Legally, Facebook has pursued a variety of criminal and civil penalties against those who abuse the site, using laws such as the U.S. CAN-SPAM act, which levies penalties of as much as \$100 per spam message. The company has had some notable successes with this strategy. In November 2008, it was awarded one of the largest judgments ever, winning statutory damages of US\$1.3 billion (later reduced to \$873 million) after successfully arguing that Adam Guerbuez of Canada, Atlantis Blue Capital, and 25 other unnamed people falsely obtained login information for Facebook users and then sent spam to those users' friends. Although the individuals charged are in Canada, Facebook could still pursue the money. Even if it doesn't, the court's ruling makes the cost of doing business as a hacker in the U.S. much more prohibitive. More information may be found at http://www.infoworld.com/d/security-central/facebook-beefs-site-against-hackers-631?source=rss_security_central.

TEEN SUICIDE PUTS SPOTLIGHT ON HIGH-TECH BULLYING

On April 9th, Reuters reported that six students face felony charges in the death of Phoebe Prince, 15, who hanged herself in January after being subjected to verbal assault and threats of physical harm. Some of the messages utilized new, contemporary avenues, such as Facebook and text messaging. Those accused of harassing the young girl have come under an online attack themselves with fake websites set up under their names linked to media accounts of the case. The sites have attracted reams of anonymous comments and threats. Three girls involved were recently arraigned and pleaded not guilty in Prince's case to a variety of civil rights violations and stalking charges. A fourth girl and two boys face similar charges. The boys, both of whom briefly dated Prince, also are charged with statutory rape. Massachusetts lawmakers in March approved a bill that would ban bullying, including cyber-bullying, but versions of the bill must be reconciled by lawmakers before it can become law. The legislation came in response to the Prince case and the suicide of an 11-year-old boy in Springfield, Massachusetts, last year. Carl Joseph Walker-Hoover had been subject to relentless anti-gay taunts before killing himself. However, having a statute may do little to stop bullying and could make children more wary of reporting incidents and setting themselves up for retribution. One thing is certain - the new online venues have made a bad problem worse and have strengthened the belief that something must be done to fix this dangerous and sometimes deadly crisis. A copy of the story may be found at <http://www.reuters.com/article/idUSTRE63847420100409>.

FLAWED MCAFEE UPDATE PARALYZES CORPORATE PCS

On April 22nd, ComputerWorld.com reported that a flawed antivirus update sent enterprise administrators scrambling as the new signatures quarantined a crucial Windows system file, crippling an unknown number of Windows XP computers. According to the company, the problem occurred with the 5958 virus definition file (DAT) that was released on April 21 at 2:00 P.M. GMT+1 (6:00 A.M. Pacific). More specifically, users on McAfee's support forum stated that the update flagged Windows' "svchost.exe" file, a generic host process for services that run from other DLLs (dynamic link libraries). Both users and McAfee said that the flawed update had crippled Windows XP Service Pack 3 (SP3) machines, but not PCs running Vista or Windows 7. Once affected, PCs displayed a shutdown error or blue error screen and then went into an endless cycle of rebooting. McAfee pulled the update and posted recovery instructions. While irritating, flawed signature updates are nothing new. A month ago, a BitDefender update clobbered 64-bit Windows machines. In 2005, Trend Micro released a flawed signature update that slowed PCs to a crawl, and McAfee is far from the first anti-virus vendor to ship a flawed signature update. In May 2007, a Symantec definition file crippled thousands of Chinese computers when the software mistook two critical Windows .dll files for malware. Solutions to the problem may be found at <https://kc.mcafee.com/corporate/index?page=content&id=KB68780>.

BANKING VIRUS IS BACK WARNS FIRM

On April 22nd, Web security company Trusteer noted that it has spotted a new, more-powerful version of the Zeus Trojan, a virus that steals online banking details from infected computer users in one of every 3,000 of the 5.5 million computers it monitors in the US and UK. The malware steals login information by recording keystrokes when the infected user is on a list of target websites. The user's data is then sent to a remote server to be used and sold by cyber-criminals. According to Trusteer, this new version of Zeus has the ability to increase fraud losses, since many people have turned to online banking and the infection is growing faster than the company has ever seen before. Trusteer warned computer users to make sure their anti-virus software and operating systems are kept up to date. A copy of the story may be found at <http://news.bbc.co.uk/2/hi/technology/8634356.stm>.

GOOGLE TO DISCLOSE STATS ON GOVERNMENT INQUIRIES

On April 20th, The Washington Post reported that Google plans to publish data on the number of requests it receives from governments to either remove content or identify specific users. More specifically, Google announced that it will host a page on its site that reveals the number of times a government has requested data on a specific user or asked Google to remove a piece of content from its network of sites, such as search, YouTube, or Blogger. The page will be updated every six months and the initial data covers requests sent to Google between July 2009 and December 2009. During that period, Brazilian government agencies and officials filed the most requests, 3,663 requests for data on individuals and 291 requests for removal of content, perhaps underscoring how popular Google's Orkut social-networking service is in that country. Parties acting on behalf of

the U.S. government made 3,580 requests for data on individuals and 123 requests for the removal of content. Google has explained that it hopes this disclosure will lead to greater transparency and in turn, less censorship; however, Google's numbers are not nearly as transparent as they could be. The numbers include how often - in general - it complies with takedown requests, but does not provide specifics. Additionally, the numbers don't include requests made as part of civil court proceedings, such as any requests for content removal made as part of Google's ongoing trial with Viacom over YouTube. And China is absent from the list entirely, except for a red question mark in the content removal category. Google has said that it would like to share more information, but it's not an easy matter. Google has noted that it hasn't yet figured out how to categorize and quantify these requests in a way that adds meaningful transparency. More information may be found at

<http://www.washingtonpost.com/wp-dyn/content/story/2010/04/20/ST2010042005926.html?sid=ST2010042005926>.

GOOGLE HACKERS DUPED SYSTEM ADMINISTRATORS TO PENETRATE NETWORKS, EXPERTS SAY

On April 21st, The Washington Post reported that the hackers who penetrated the computer networks of Google and more than 30 other large companies used an increasingly common means of attack: duping system administrators and other executives who have access to passwords, intellectual property and other information. And once a hacker is able to social engineer a system administrator or a senior executive, it becomes difficult to identify the attackers. In fact, many of these companies don't know if source code has been stolen because the hackers have assumed the identities of people whose passwords have been stolen. The targeting of personnel is only one aspect of a larger, more sophisticated operation that involves planning the mode of attack, reconnaissance inside a company's network, deciding what type of data to go after, and harvesting and analyzing the data. With respect to these most recent attacks, Google has asserted that the attacks originated in China; Chinese officials say they are investigating. Assuming China was to blame, the hackers' goal was likely to obtain information that benefits China in strategic industries and in areas where the country seeks an advantage over U.S. firms. According to Rob Lee, a director with Mandiant, a security firm that is working with some of the targeted companies, the bottom line is, if your company has any business dealings with China or has extremely valuable technology or intellectual property, you have a high likelihood of being a target. And even if China isn't implicated, the fact that these new types of attacks involve many steps, both with human intelligence and electronic intelligence in order to penetrate these organizations, demonstrates that this is the work of a highly organized group or groups that has specific targets in mind. More information may be found at

<http://www.washingtonpost.com/wp-dyn/content/article/2010/04/20/AR2010042005300.html>.

LEGAL SPYING VIA THE CELL PHONE SYSTEM

On April 21st, CNET News reported that two researchers have found a way to exploit weaknesses in the mobile telecom system to legally spy on people by figuring out the private cell phone number of anyone they want, tracking their whereabouts, and listening to their voice mail. Independent security researcher Nick DePetrillo and Don Bailey, a security consultant with iSec Partners, began the sneaky operation by getting a target's cell phone number from a public database that links names to numbers for caller ID purposes. DePetrillo used open-source PBX software to spoof the outgoing caller ID and then automated phone calls to himself, triggering the system to force a name lookup. And according to Bailey, what they did was not illegal, nor is it a breach of terms of service. Next up for the researchers is matching the phone number with a geographic location. The SS7 (Signaling System) public switched network routes calls around the world and uses what's called the Home Location Register to log the whereabouts of numbers so networks can hand calls off to one another. As DePetrillo pointed out, individual phones are registered to mobile switching centers within specific geographic regions and they are logged in to that main register. Although telecom providers are supposed to have access to the location register, small telcos in the EU are offering online access to it for a fee, mostly to companies using it for marketing data and cost projections. It's also relatively easy to access other people's voice mail, a service that's been around for years from providers like SlyDial. They operate by making two nearly simultaneous calls to a target number, one of which disconnects before it is picked up and another that goes straight into voice mail because of the earlier call. This enables the caller to go directly to voice mail without the phone ringing. Because the attacks are based on the assumption of how the networks work, there is not much telecom providers can do. Rather, people are just going to have to be made aware of the threat. Corporations specifically should start to take a look at their security policies for executives as this can impact a business in profound ways involving insider trading, tracking of executives, etc. A copy of the story may be found at http://news.cnet.com/8301-27080_3-20002986-245.html.

LOWER MERION SCOOOL REPORT: WEB CAMS SNAPPED 56,000 IMAGES

On April 19th, The Philadelphia Inquirer reported that Lower Merion School District employees activated the web cameras and tracking software on laptops they gave to high school students about 80 times in the past two school years, snapping nearly 56,000 images that included photos of students, pictures inside their homes and copies of the programs or files running on their screens. In most cases, technicians turned on the system after a student or staffer reported a laptop missing and turned it off when the machine was found; however, in at least five instances, school employees let the Web cams keep clicking for days or weeks after students found their missing laptops. Those computers - programmed to snap a photo and capture a screen shot every 15 minutes when the machine was on - fired nearly 13,000 images back to the school district servers. According to Harriton High School sophomore Blake Robbines, these results confirm his allegation that the program invaded his privacy. The district attorney, Henry Hockeimer, said that attorneys from his firm, Ballard Spahr, and specialists from L3, a computer forensics firm, have used e-mails, voice mails and network data to piece together how often, when and why school officials used the technology. He stated that the vast majority of instances represent cases in which the technology appeared to be used for the reasons the district first implemented it in 2008: to find a lost or stolen laptop or, in a few cases, when a student took the computer without paying a required insurance fee. The next biggest chunk of images stem from the five or so laptops where employees failed or forgot to turn off the tracking software even after the student recovered the computer. And in about 15 activations, investigators have been unable to identify exactly why a student's laptop was being monitored. Further, about 10 employees at the district and its two high schools had the authority to request the computer administrators to activate the tracking system on a student's laptop. But only two employees (Mike Perbix and Carol Cafiero) have the ability to actually turn on and off the tracking. Hockeimer said the district investigators have no evidence to suggest either Perbix or Cafiero activated the system without being asked. In the end, Hockeimer said that the whole situation was riddled with the problem of not having any written policies and procedures in place. Some have argued that it might have been best for the school district to come clean earlier, as soon as they had this information rather than waiting until something was filed in court revealing the extent of the spying. More information may be found at http://www.philly.com/philly/news/breaking/20100419_Lower_Merion_details_Web_cam_scope.html.

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 <i>Bytes in Brief</i>	
Email: <input type="text"/>	Go

Privacy by  **SafeSubscribe**SM
For Email Marketing you can trust