

{ 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 147 - August 2009

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

NEW WEB PRIVACY RULES ISSUED BY EUROPEAN UNION

On June 23rd, a panel of European privacy regulators that advises the European Commission issued an opinion describing how European Union privacy laws apply to Facebook, MySpace and other social-networking sites. While these recommendations are considered more expansive than those in the United States, the exact requirements have been viewed as vague and open to broad interpretation. The panel of regulators recommended that the sites should offer privacy-friendly default settings and allow users to limit data disclosed to third parties. Additionally, the panel advised that network operators should not retain personal information after users delete their accounts, and operators should delete accounts that remain inactive for a certain period of time. In response, Facebook and Myspace have explained that they are currently studying the newly issued opinion to assess how to best respond. A spokeswoman for Facebook added that the opinion is an important step in providing an industry standard for the European Union and that the company has recently hired an officer to deal with European public policy issues. The guidelines may be found at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf

9TH CIRCUIT RULING OPENS DOOR FOR LAWSUITS INVOLVING TEXT-MESSAGE SPAM

On June 23rd, Law.com reported that the 9th Circuit has reversed the decision of the federal court in the Northern District of California, effectively opening the door for lawsuits against companies that send spam via cell phone text messages. The initial lawsuit, brought in 2007, alleged that Simon & Schuster violated the Telephone Consumer Protection Act by sending an unsolicited text message through an automated telephone dialing system. Simon & Schuster moved for summary judgment claiming that it did not use an auto-dial system, that no "calls" took place as defined by federal law and that consent had been given by agreeing to the terms and conditions for ringtone downloads. In overturning Judge Claudia Wilken's decision to grant Simon & Schuster's summary judgment motion, the appellate court ruled that a text message could be considered a call under Federal Communications Commission regulations and that, contrary to the company's claim, no permission had been given to receive unsolicited text messages. A trial date has not yet been set for the remaining questions of fact. The decision may be found at <http://amlawdaily.typepad.com/textspam.pdf>

GATES CREATES CYBER-DEFENSE COMMAND

On June 23rd, Defense Secretary Robert M. Gates issued an order establishing a command that will defend military networks against computer attacks and develop offensive cyber-weapons. Gates stated that he would write a memo to senior military leaders recommending that President Obama designate that the director of the National Security Agency (NSA) lead the new command. The command will be set up as part of the U.S. Strategic Command and is expected to be launched this October and be fully operational by October 2010. While the command's mission would be to defend military networks, Deputy Defense Secretary William reasoned that it would be inefficient and irresponsible not to use the technical expertise to protect federal civilian networks as well, as long as it is done in a way that protects civil liberties. The memo written by Gates recommending the creation of the command may be found at <http://online.wsj.com/public/resources/documents/OSD05914.pdf>

ONLINE ELECTRONICS STORES CAUGHT IN FRAUDULENT ACTIVITIES

On June 25th, New York's attorney general Andrew M. Cuomo announced that seven online merchants have agreed to pay \$765,000 after the New York State Attorney General's office found that the companies have been engaging in several forms of consumer fraud. One such fraudulent tactic employed by the merchants was a classic bait-and-switch scheme. The merchants would first "bait" consumers into purchasing products from their websites by offering significantly lower prices. After a consumer orders a particular product, the companies would call the buyer and attempt to "switch" the consumer's original order with additional or upgraded merchandise at inflated prices. If the buyer refused, the companies would either cancel the sale or claim that the item was backordered for months. If the consumer did agree to the additional merchandise, the merchants would send substandard merchandise and either deny any returns requests or levy hefty undisclosed fees to do so. The New York State Better Business Bureau has stated it will permit those individuals who believe they qualify for restitution to submit claims starting in July. The press release from the New York State Attorney General's office may be found at <http://hdguru.com/wp-content/uploads/2009/06/online-scam-etailers-fined.pdf>

NATIVE FORMAT? NOT SO FAST

On June 25th, a Byte and Switch blog posting explained how a recent case, *Kay Beer v. Energy Brands*, demonstrated an important lesson in eDiscovery regarding production and presentation of documents. In this case, Plaintiff demanded that Defendant produce a large number of e-mails in their native Outlook format. Nearly 20 GB of potentially relevant data comprising well over half a million pages was involved. During the Rule 26 conference, Defendant had agreed that if Plaintiff made a good faith request for relevant documents in native format it would do its best to comply. However, when Plaintiff's requests for production poured in, Defendant decided to push back. The judge ruled for the Defendant. The judge had previously ruled in Defendant's favor for all but one claim, so the scope of the case was substantially smaller. As such, the review request was greatly out of proportion to the one remaining claim. Quoting the *Sedona Principles for Electronic Document Production*, the judge explained that unless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court. A recent blog post discussing the court's order may be found at http://blog.ca-ig.com/2009/07/ediscovery_philosophy_2-0/

NO BAIL FOR BLOGGER ACCUSED OF THREATENING JUDGES

On June 25th, U.S. Magistrate Michael Shipp denied bail to Harold "Hal" Turner, the New Jersey blogger accused of threatening three federal judges. This decision came even after attorneys on both sides had reached a tentative agreement permitting Turner's release on \$200,000 bail. In the federal complaint, Turner is accused of threatening to assault or murder the judges, using his blog to proclaim that the judges deserved to be killed and providing a map that pinpointed the courthouse where the judges are located. The blog entries also referenced the 2005 murders of the mother and husband of Judge Joan Humphrey Lefkow. In reference to that event, Turner is accused of posting a comment that stated "apparently, the 7th U.S. Circuit Court didn't get the hint after those killings" and contending that another lesson was needed. In an unrelated matter, Turner also faces charges that he encouraged violence against two state legislators after he urged readers of his blog to take up arms over controversial legislation on Catholic parish finances. A blog post discussing this case may be found at <http://blog.taragana.com/n/judge-denies-bail-for-nj-blogger-accused-of-threatening-3-chicago-federal-judges-92174/>

SURPRISE! WINDOWS UPDATES INSTALL WITHOUT PERMISSION

On June 25th, *Windows Secrets* announced that Windows has been installing updates on computers against the wishes of some individuals. In fact, many readers of *Windows Secrets* have stated that they have watched their computers install updates from the June 9th security patches after rebooting their machines. This occurred even after users set their options to require permission prior to installing patches or updates. Explaining the problem, staff members for the newsletter have stated that if a user has an incomplete update download, Windows won't display the fact that you have updates, and then, on reboot or shut down, those updates start installing even though the user has told Windows not to do so. The problem may have been caused by the record number of updates issued on June 9th—31 individual bug patches—which could have exceeded Microsoft's server capacity and resulted in downloads failing before they were completed. However, this isn't Microsoft's first run-in with

accusations of installing surprise updates without users' permission. In 2007, the company was accused of secretly updating files relating to the Windows Update program. More details about the problem, as well as workarounds may be found at <http://blogs.technet.com/mu/archive/2009/06/26/update-notifications-and-install-at-shutdown.aspx>

UNCLEAR WHAT WILL HAPPEN TO PERSONAL INFO WITH CLEAR

On June 26th, a *Practical Nomad* blog posting explained that the sudden shutdown of the Clear program, which stored personal information to speed airplane passengers through security, has left over a quarter million people concerned with what will happen to that information. While security experts have noted that it is unlikely customers' private data would be handed over to creditors or new owners, the potential headaches that could occur have raised eyebrows by some members of Congress. In a statement posted on the parent company's website earlier in the week, the company assured the public that it was taking the necessary precautions and that all of its Clear airport kiosks had been wiped clean of data. This potential problem is part of the bigger debate on the methods used by the Transportation Security Administration (TSA) to manage passenger data. Some security experts have argued that the TSA keeps too much passenger data for way too long, leaving many vulnerable if a security breach were to occur. The blog post may be found at <http://www.hasbrouck.org/blog/archives/001691.html>

WEB ADVERTISERS PROPOSE SELF-REGULATION PRINCIPLES

On July 2nd, MSNBC.com reported that web advertisers have proposed new self-regulatory principles combining consumer education, disclosures about what information is being collected, and special protections for children and sensitive information in an attempt to prevent tough legislation from being enacted. The principles would require online advertisers to create a specific icon or phrase to point Internet users to a site where they could learn what information was being collected and opt out. These guidelines would be much stricter when it comes to children and sensitive information. No information would be collected about children the advertisers know are under the age of 13 or from sites directed to children under the age of 13 for online behavioral advertising. Further, consent must be given to collect financial account numbers, Social Security numbers, pharmaceutical prescriptions or medical records about a specific individual for online behavioral advertising. On the education side of the principles, the industry would establish a Web site to educate consumers about how the Internet is monetized. Not everyone shares the industry's view on these self-regulation principles. Marc Rotenberg, president of the Electronic Privacy Information Center, called the principles virtually meaningless and predicted that Congress would eventually pass legislation hemming in information collection by advertisers. A blog discussion on this subject may be found at <http://www.webmasterworld.com/foo/3944833.htm>

WOMAN CONVICTED OF COPYRIGHT INFRINGEMENT ASKS FOR NEW TRIAL

On July 6th, CNET News reported that Jammie Thomas-Rasset, the woman recently found liable for willful copyright infringement of 24 songs, has asked the court for either a new trial or a reduction of the \$1.92 million she was ordered to pay. During the initial lawsuit in 2007, the jury rendered a \$220,000 verdict, but that decision was later thrown out after the judge acknowledged he erred in the jury instructions. At her retrial, the jury again decided against her, but this time they awarded damages of \$80,000 for each song for a grand total of \$1.92 million. Thomas-Rasset's attorney explained that not only was this award excessive, but such a judgment runs afoul of the United States Constitution, specifically the Due Process Clause. On appeal, her attorneys plan to argue that the verdict reveals a major flaw with the statutory damages scheme of the Copyright Act. Specifically, they explained that Ms. Thomas should not be subjected to a penalty that no reasonable person could have expected would flow from the noncommercial music sharing of which she stands convicted. Further information may be found at <http://arstechnica.com/tech-policy/news/2009/06/jammie-thomas-retrial-verdict.ars>

NORTH KOREA SUSPECTED IN ATTACKS ON U.S. GOVERNMENT WEB SITES

On July 8th, the Associated Press reported that a massive computer attack, which began on July 4th, knocked out several U.S. government Web sites. The unusually lengthy and sophisticated attack brought down the Transportation Department site for three days, while the Federal Trade Commission site was down from Sunday to

Monday. Government officials acknowledged that the Treasury and Secret Service sites experienced problems as well, but did not disclose the length of time these sites were down. Shortly after the U.S. was attacked, South Korea experienced a similar problem with certain government and banking Web sites as well. An initial investigation by South Korea found that many personal computers were infected with a virus ordering them to visit major official Web sites in South Korea and the U.S. at the same time. While the U.S. refused to publicly discuss the attack, South Korean intelligence officials explained that they believed the culprits behind the attack to be either North Korea or North Korean sympathizers. A detailed discussion of the attacks may be found at <http://www.reuters.com/article/technologyNews/idUSTRE56709E20090709>

SHORTCUT URLS MAY HAVE TWITTER SHAKING IN ITS BOOTS

On July 8th, a *New York Times* blog posting warned that spammers have entered the shortcut URL game made popular by users of Twitter. In fact, a recent *New York Times' Bits* blog post noted that short URL spam has skyrocketed in the past few months and is now present in more than two percent of all spam messages. What's worse, the potential headaches of this type of spam could potentially diminish the power of Twitter. The writer noted that while it is easy to use caution in an e-mail message and simply delete messages by unknown senders, many Twitter users happily follow people that they may not actually know and often click on posted links without giving them a second thought. The *New York Times' Bits* blog post may be found at <http://bits.blogs.nytimes.com/2009/07/07/spammers-shorten-their-urls/>

LESSONS LEARNED FROM TWITTER'S SECURITY BREACH

On July 15th, a Twitter blog posting announced that valuable lessons can be learned from Twitter's latest security breach. Hackers were able, using Yahoo's password recovery system, to get in and gain information from a number of other sites, including the personal accounts of some Twitter staff members. This attack has highlighted the extreme interconnectedness of the social Web and the ability of hackers to access multiple accounts simply by accessing one. While the security of Web applications like Yahoo Mail and Google docs have come under fire as of late, Twitter executives have reasoned that the breach speaks more towards the importance of following good personal security guidelines such as choosing a strong password, different passwords for each site and having a system in place that makes it hard for the wrong people to get in. Further, security experts have reasoned that adding more security layers to these apps may wind up doing more harm than good. Peter "Mudge" Zatko, technical director of national intelligence at BBN Technologies, has explained that these services are about convenience and has been quoted as saying that you can't make something easy to access and terribly secure at the same time. Those are diametrically opposed goals. The blog post may be found at <http://blog.twitter.com/2009/07/twitter-even-more-open-than-we-wanted.html>

MICROSOFT SUES ALLEGED IM SPAMMERS, PHISHERS

On July 16th, CNET News reported on a recent civil lawsuit filed against Funmobile, Mobilefunster, and several other individuals by software giant Microsoft for the alleged intentional misuse of the company's Live Messenger network to gain personal information of its users. In the suit, Microsoft alleged numerous attacks on the service, including IMs disguised to appear to be coming from friends, as well as various phishing attacks that resemble the look of an outside service or official Microsoft page. Using these scams, cyber thieves have been able to obtain users' personal account information and later exploit it by sending mass spam and phishing messages to the friends of users whose accounts have been breached. In bringing out the big guns to combat this problem, Microsoft has stated it hopes to accomplish three things: stop these attacks, recoup monetary damages, and send a message to other would-be scam artists. In the meantime, Microsoft is urging all users of its Live Messenger service to use caution and not give out their log-in information to other people. A blog post by Tim Cranton, Microsoft's associate general counsel of Internet safety enforcement, may be found at <http://microsoftontheissues.com/cs/blogs/mscorp/archive/2009/07/16/saying-no-to-spim.aspx>

A copy of the complaint may also be found at <http://www.scribd.com/doc/17420433/Microsoft-Corporation-v-Funmobile-et-al-case-number-092212473>

PHILLY POLICE DEPARTMENT SUED BY BLACK OFFICERS GROUP OVER WEBSITE

On July 16th, the *Philadelphia Inquirer* reported on a civil rights lawsuit filed by the Guardian Civic League against the Philadelphia Police Department over an Internet discussion forum on which officers have allegedly posted hundreds of derogatory and racist comments. While the police department does not run the Web forum, Domelights.com, the suit alleges that not only do officers post from department computers, but also that the site's founder and moderator is an active sergeant in the department. Several other organizations, including the National Association for the Advancement of Colored People and the National Association of Black Law Enforcement Officers, have joined forces with the league in an attempt to force the department to shut the site down. Explaining that enough is enough already, these groups have argued that they are sick and tired of the officers further dividing the department by their comments. Roosevelt Poplar, a vice president with the city's Fraternal Order of Police chapter has explained that officers could not likely be disciplined solely for making postings on the site; however, if the league's allegations are true and a department computer was used, disciplinary action could be possible. The story may be found at

http://www.philly.com/philly/news/pennsylvania/20090717_Black_police_officers_group_sues_over_Web_site.html

ALARMING DEVELOPMENTS IN MOBILE MALWARE

On July 17th, Computerworld.com reported that the day of mobile botnets has likely arrived. This alarming news comes after analysts at Trend Micro examined a piece of mobile malware know as "Sexy Space," a variant of another piece of mobile malware called Sexy View, which targets devices running the Symbian S60 OS. To consumers, however, there really isn't much sexy about this malware; they might view the term as annoying instead. When infected, phones send text messages (SMS) to everyone in the phone's contact list with a link to a Web site. For some reason, those who wrote Sexy View were able to get the application and the Sexy Space variant approved and signed by Symbian. What's even more alarming is the fact that Sexy Space is capable of downloading new SMS templates from a remote server in order to send out new SMS spam. Sexy Space can also steal subscriber and network information from the device and send it to a remote server. This new development confirmed what many have previously warned: as mobile devices become more like minicomputers, it's likely they will be frequently targeted by malware writers. In an attempt to at least slow down this spreading problem, Symbian announced it has revoked the content certificate and publisher certificate used to sign the malware. An analysis of the malware Sexy Space may be found at http://www.f-secure.com/v-descs/worm_symbos_yxe.shtml

HSBC FINED \$6M IN BRITAIN FOR DATA LOSS

On July 23rd, *Australian IT* reported that HSBC, Europe's biggest bank, has been fined over \$6 million by the Financial Services Authority (FSA) for the careless handling of confidential information of tens of thousands of its customers. The bank sent unencrypted private details via courier to third parties, left information lying on open shelves and unlocked cabinets and lost unencrypted CDs holding thousands of customers' details. These lapses in judgment came even after the bank had received warnings about its security procedures. FSA did state, however, that HSBC had taken a number of remedial actions in an attempt to rectify or at least stifle future problems including contacting customers involved, improving staff training and demanding that all electronic data in transit be encrypted. Some have questioned whether the fine would be enough to act as a deterrent. This does not mark the first time FSA has assessed fines against banks for data security lapses and fraud. In the past four years FSA has fined Capita Financial Administrators, Nationwide, BNP Paribas Private Bank, Norwich Union and Merchant Securities for similar occurrences. The story may be found at

http://www.australianit.news.com.au/story/0,,25823370-15306,00.html?from=public_rss

LA OFFICIALS QUESTION GOOGLE APPS PLAN

On July 21st, CNET News reported that Los Angeles officials have questioned the city's plan to move government e-mail and other records onto Google's hosted Web service Google Apps. Both LA City Councilman Tony Cardenas and Paul Weber, president of the LA Police Protective League, have expressed concern for the safety of these records. Mr. Cardenas went a step further explaining that drug cartels would pay any sum of money to be

aware of our progress on investigations. These concerns come after sensitive Twitter documents were stolen by a hacker who gained access to a Twitter employee's e-mail account and from there got information that allowed access to the company's data on Google Apps. In a public statement, a Google spokesperson explained that security is an important consideration for any organization considering cloud computing and that the company has been working closely with the City of Los Angeles to address any concerns and questions voiced by government officials or citizens alike. The story may be found at http://news.cnet.com/8301-1009_3-10291911-83.html

ESPN REPORTER SECRETLY VIDEOTAPED NUDE IN HOTEL

On July 21st, a *LawInfo* blog posting announced that ESPN reporter Erin Andrews was secretly videotaped in the nude while she was alone in a hotel room, and the video was posted on the Internet. Ms. Andrews has stated that she plans to seek criminal charges and file civil lawsuits against the person who shot the blurry, five-minute video and anyone who publishes the material. Due to her popularity and name recognition, cyber criminals have jumped on this golden opportunity and have used the video as a delivery vehicle for malware and viruses. In fact, several links which claim to send Internet users to the Andrews video actually sent Internet users to sites with malicious software and computer viruses. Some hackers have also included a portion of the video on their sites in hopes that the malware gets passed along as users share the link with friends. The blog post may be found at <http://blog.lawinfo.com/2009/07/21/espn-reporter-secretly-videotaped-nude-in-hotel/>

SPAM SOARS DESPITE BILLIONS SPENT TO PREVENT IT

On July 21st, TRACELabs issued a report which stated that despite billions being spent by corporations on spam filters, spam volumes have reached record levels. The report suggested that spammers have been unimpeded by the efforts of law enforcement and the security community and that recent efforts to shut down spam crime groups have only encouraged spammers to develop more resilient systems. In fact, crime groups running the Waledac, Rustock, Pushdo and Grum spamming botnets continue to be very strong. The report further found that over 30% of all spam last week came from Asian countries, helped out by new spam heavyweight Vietnam. Another interesting tidbit of information is the fact that only three targeted institutions were the focus of 99.5% of all phishing activities last week—eBay, Bank of America and Comerica. Senior TRACELabs researcher Phil Hay commented that a more holistic and well planned approach needs to be adopted by law enforcement and the security community working together worldwide to really have a positive and long-lasting impact on reducing spam. The report may be found at http://www.marshal8e6.com/newsimages/trace/Marshal8e6_TRACE_Report_July_2009.pdf

SHORTAGE OF CYBER EXPERTS MAY HINDER GOVERNMENT

On July 22nd, *The Associated Press* announced that federal agencies are facing a severe shortage of computer specialists, a problem which poses national security risks as cyberattacks against the government become more and more frequent. The study described the federal cyber force as fragmented, where no one is truly in charge and government agencies often work in direct opposition with one another. The study went on to say that the recruiting and retention of cyber workers has been hampered by the cumbersome hiring process, the failure to devise government-wide certification standards, insufficient training and salaries, and lack of an overall strategy. While President Obama has yet to fill the new cyber coordinator position, the study recommends that whoever is chosen should start by laying out a strategy to meet the government's work force needs, setting job classifications, enhancing training and leading a nationwide effort to promote technology skills, including the use of scholarships. The federal government's vulnerabilities have been highlighted by the recent attacks that breached a high-tech fighter jet program and the electrical grid. And while some have described the link between the work force shortages and the increased cyber threats as tenuous at best, one thing is for certain: if the government doesn't have the work force capable of meeting the cyber challenge, all of the cyber czars and organization efforts will be for naught. The story can be found online at http://news.lp.findlaw.com/ap/a/w/1155/07-22-2009/20090722012001_02.html

AMAZON ERASES ORWELL BOOKS FROM KINDLE

On July 17th, in an ironic series of events, Amazon.com remotely deleted some editions of George Orwell's "1984" and "Animal Farm" from the Kindle devices of readers who had bought them. This move not only angered those affected, but generated waves of online pique against the company. In response, Amazon released a statement that explained that the books were added to the Kindle store by a company that did not have the rights to them, and effectively acknowledged that the deletions were a bad idea. The company went on to explain that it is in the process of changing its systems so that in the future it will not remove books from customers' devices in these circumstances. Many have reasoned that this event has highlighted how few rights Kindle owners have when they buy an e-book from Amazon. Bruce Schneier, an expert on computer security and commerce, pointed out that customers can't lend people books or sell books they have already, but now it appears that you can't even count on still having your Kindle books tomorrow. A blog post on the story may be found at <http://poque.blogs.nytimes.com/2009/07/17/some-e-books-are-more-equal-than-others/>

Details of Amazon's CEO Jeff Bezos' apology for the incident may be found at http://www.informationweek.com/news/personal_tech/drm/showArticle.jhtml?articleID=218600600


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.