



Issue 129 February 2008

The URLs referenced in Bytes frequently link to newspapers and other current news sources. Be aware that these links may fail over time.

CONVICTED HACKER SAYS BREAKING INTO SYSTEMS WAS EASY

Convicted hacker Robert Moore, now in federal prison serving a two-year sentence after pleading guilty to conspiracy to commit computer fraud, said breaking into systems was “so easy a caveman could do it.” Moore was involved in a scheme that hacked into telecommunications companies to steal VoIP (voice-over IP) services and sell them through a separate company. Moore was not the mastermind behind the operation, but he was the one hacking into the computers. The biggest insecurity Moore found in most systems was insecure passwords due to companies not changing the defaults. Once he got in through the default passwords, the whole database was usually up for grabs. Moore also explained that companies easily could have detected him on their system, if they had tried. See the original interview at: <http://www.informationweek.com/story/showArticle.jhtml?articleID=202101781>

ONLINE FRAUD MORE SOPHISTICATED IN 2007

A year-end report by the *Washington Post* described the different types of online fraud for 2007. Hackers tried to get people to go to certain websites, where unbeknownst to them, spyware would be installed on their computers. Particular incidents of this happened before the Superbowl on the Dolphins stadium website, where the Superbowl was held, and on “Cyber Monday” after Thanksgiving, when there is a surge in online shopping. Also, an increase in spam e-mails by 100 percent can partially be attributed to the so-called “Storm worm,” an e-mailed Trojan horse program that infected computers after users went to footage of storms on the European coast. The Trojan gave the creators access to the infected computer allowing them to send the user and many others spam. The number of spam e-mails is up to 120 billion spam messages daily, or about 20 spam e-mails per day for every person on the planet. Another alarming development was the use of “phishing” attacks to try to trick users into entering their personal bank account data at fake e-commerce and banking sites. Other attacks involved e-mails appearing to come from the Better Business Bureau and asking users to view a complaint. When the user opened the “complaint,” spyware was installed on the computer. These are just a few of the methods used by hackers in 2007. The full report may be found at: <http://www.washingtonpost.com/wp-dyn/content/article/2007/12/20/AR2007122001266.html>

NY COURT RULES NO ATTORNEY-CLIENT PRIVILEGE FOR E-MAIL SENT ON EMPLOYER'S SERVER

On October 17th, 2007, the Supreme Court of New York County ruled that a doctor's e-mails, sent on his employer hospital's system, were not privileged. The hospital located the e-mails during discovery, did not read them, and notified the doctor of their existence. The doctor moved to suppress the e-mails, claiming they were privileged. The hospital claimed the doctor waived his right to privilege because hospital policy prohibited personal e-mailing while on the job, and the policy included the right to access the e-mails without notice. The doctor argued that he was protected by New York Civil Practice Law 4548, which states that no communication shall lose its privileged character just because it is transmitted electronically. The court applied a four-part test used in a bankruptcy case with similar issues to determine whether the attorney-client privilege would apply to personal e-mails exchanged by an employee with an attorney over a company-controlled communications system. The test states the privilege would not apply where (1) the company maintains a policy that bans personal or other objectionable use; (2) the company monitors employee use of computers or e-mail; (3) third parties other than the employee have a right to access the computer and the employee's e-mail; and (4) the company notifies the employee of its use and monitoring policies. The court concluded that the hospital had met all four

requirements in this case, and denied the doctor's motion to suppress. The full opinion can be found at http://www.nycourts.gov/reporter/3dseries/2007/2007_27429.htm

FTC PROPOSES ONLINE BEHAVIORAL AD GUIDELINES

On December 20th, the Federal Trade Commission announced new guidelines for online behavioral advertising. Behavioral advertising is advertising based on information collected about one's preferences, and then receiving ads based on the preferences. The guidelines promote notifying consumers that their information is going to be used for behavioral advertising, allowing consumers to choose whether their information is gathered, gaining consumer consent before changing privacy policies, securing the gathered information, and keeping the gathered information for a limited time. To see the full press release from the FTC on the guidelines, go to <http://www.ftc.gov/opa/2007/12/principles.shtm>

GOOGLE HANDED SETBACK IN PATENT CASE

On December 26th, the United States Court of Appeals for the Federal Circuit handed down a decision that overturned part of a District Court ruling for summary judgment in favor of Google. Initially, Plaintiff Hyperphrase Technologies filed suit against Google for patent infringement involving their AdSense and AutoLink programs. Google then moved for summary judgment, and the District Court ruled in favor of Google, saying that the programs did not violate Hyperphrase's patents. The ruling by the Federal Circuit affirmed in part and vacated and remanded in part the District Court ruling. The District Court defined a data reference as including only one possible record. The Federal Circuit held that the District Court erred in its definition, and therefore overturned the motion for summary judgment in regard to two of the patents at issue regarding AutoLink. The court affirmed the summary judgment saying the AdSense program did not infringe on any patent claims. The ruling of the Federal Circuit can be found here <http://www.cafc.uscourts.gov/opinions/07-1125.pdf>

CIA NOT A ROLE MODEL FOR EVIDENCE PRESERVATION

On December 6th, the CIA admitted that it had destroyed videotaped evidence of detainee interrogations. The taped interrogations occurred in 2002, and the tapes were destroyed in 2005, allegedly after they were of no value to the CIA and were not needed for investigations. PC World writes that though the CIA is a government agency and not subject to the Federal Rules of Civil Procedure, private companies engaging in the same actions could be subject to severe sanctions for destruction of evidence. The Federal Rules require companies to keep electronic records when faced with a lawsuit or the possibility of a lawsuit. There also can be punishment for failure to keep required electronic records. The CIA press release can be found at <https://www.cia.gov/news-information/press-releases-statements/press-release-arc-hive-2007/taping-of-early-detainee-interrogations.html> and the PC World article at http://www.pcworld.com/businesscenter/article/140594/cia_not_a_role_model_for_corporate_cios.html

APPLE AND THINK SECRET REACH SETTLEMENT

In December 2007, Apple and website ThinkSecret.com reportedly reached a settlement that calls for the website to shut down. Apple filed suit in 2005, after Think Secret revealed details about Mac products before they were formally released. No other details about the settlement were disclosed. The press release on the Think Secret site can be found at <http://www.thinksecret.com/news/settlement.html>

DEPARTMENT OF HOMELAND SECURITY PASSES REAL ID REGULATIONS

On January 11th, the Department of Homeland Security (DHS) released new regulations for government issued identification cards. The regulations establish minimum security standards for drivers licenses and identification cards, with the goal of preventing identity theft. The program requirements are (1) information and security features that must be incorporated into each card; (2) proof of the identity and U.S. citizenship or legal status of an applicant; (3) verification of the source documents provided by an applicant; and (4) security standards for the offices that issue licenses

and identification cards. The program will be implemented over the next ten years, with the initial stages beginning in 2009. To see the full DHS press release, go to http://www.dhs.gov/xnews/releases/pr_1200065427422.shtm. Remarks on the program from the DHS Secretary are available at http://www.dhs.gov/xnews/speeches/sp_1200320940276.shtm

INTEL FACES ANTITRUST INVESTIGATION

New York Attorney General Cuomo announced on January 10th that he would be launching an antitrust investigation against Intel. Intel was served with a subpoena concerning its pricing practices and whether it tried to exclude competitors, specifically its main competitor, AMD. Similar allegations against Intel have been pursued in Europe and Asia. Cuomo wants to determine whether Intel has abused its market power and engaged in monopolistic practices. The full press release from the Attorney General can be found at http://www.oag.state.ny.us/press/2008/jan/jan10a_08.html

PA SUPERIOR COURT REISSUES OPINION REGARDING SEIZURE OF COMPUTER FROM CIRCUIT CITY

On December 5th, the Pennsylvania Superior Court reissued an opinion in a case involving a defendant whose computer was seized at a Circuit City store after an employee found alleged child pornography while installing a DVD burner on the computer. The Superior Court reissued the opinion because the Pennsylvania Supreme Court overturned a case relied on in the initial decision. The court reached the same conclusion and overturned the Berks County Common Plea's judge that granted the defendant's motion to suppress evidence. The decision was made under the rule that when an individual abandons control over personal property, no objection can be made to an ensuing search by police. The court said that by dropping off his computer at the Circuit City store, he intentionally abandoned control of the computer. The court further held that the evidence cannot be suppressed because of the plain view exception to the ban on warrantless searches by the police. The full court opinion can be found at http://origin-www.courts.state.pa.us/OpPosting/Superior/out/a02023_07.pdf

SEARS FACING CLASS ACTION LAWSUIT FOR DATA BREACH

On January 4th, a complaint was filed against Sears, Roebuck and Co. for posting customers' data online in violation of its privacy policy. On the website, Manage My Home, there was a feature that allowed shoppers to look up past purchases, which could be used to look up the purchase history for any customer, in violation of Sears's privacy policy. The lawsuit was filed in Illinois on a class action basis for all of the customers damaged. To remedy the breach, the lawsuit is asking for damages along with an accounting by Sears to determine whether the website was misused by criminals. One rumored threat would be a criminal using the information to pretend to be a Sears repair person to get into someone's house. A copy of the full complaint may be found at <http://blog.washingtonpost.com/securityfix/sears%20complaint.pdf>

APPLE SUED FOR ALLEGED ANTITRUST ABUSES

On December 31st, in a complaint filed in United States District Court for the Northern District of California, Apple was accused of anti-trust violations because of a program that makes iPods unable to play music files in WMA format. The iPod has a program that disables the WMA ability because Apple does not pay Microsoft Windows's media licensing fees. The complaint alleges that Apple is engaging in monopolistic behavior with the disabler, because allowing the iPod to play only one format restricts consumer purchase options. The Plaintiff is not the first person to make these allegations against Apple, as other anti-trust lawsuits have been filed dealing with the same topic. The full complaint can be viewed at http://docs.justia.com/cases/federal/district-courts/california/candce/5:2007cv0_6507/198939/1/

NATIONAL LABOR RELATIONS BOARD: EMPLOYERS CAN RESTRICT USING COMPANY E-MAIL TO SEND UNION MESSAGES

On December 21st, the National Labor Relations Board voted 3-2 in favor of allowing employers to prohibit the use of work e-mail systems to send out union related messages. The board qualified the

ruling by saying this only applies if employers have policies in place that prohibit non-work related e-mails. The ruling states that employers have a property right to employees' e-mail on their system, and have the right to regulate and restrict usage. The ruling is a blow for unions, who say that they have been using e-mail more than ever to communicate with their members. The two dissents state that the property interest held by the employer is not absolute, and here the employee's interest in communication with the union outweighs that property right. The full opinion of the board can be found at http://www.nlr.gov/shared_files/Board%20Decisions/351/V35170.htm

ELEVEN INDICTED OVER STOCK SPAM

On January 3rd, the United States Department of Justice unsealed an indictment for eleven people accused of sending illegal spam e-mails. The indictment included "Spam King" Alan Ralsky and others from the United States, Hong Kong, and Canada. The indictment says that the spammers sent e-mails urging people to buy stocks at a low price. Once the price of the stock increased, the defendants sold at the inflated price, known as a "pump and dump" scam. The defendants reportedly made about \$3 million from the scam. The full Department of Justice press release is available at http://www.usdoj.gov/opa/pr/2008/January/08_crm_003.html

DATA BREACHES AND THEFTS ON THE RISE

On January 2nd, the Associated Press reported that companies and public agencies are spending more to prevent security breaches, but most of the protection comes too late. Most companies enact the measures when faced with a security breach, instead of enacting preventative measures, and identifying vulnerabilities. Attrition.org reported that more than 162 million records were compromised in 2007, up from 49 million in 2006. Most of the difference is accounted for by the massive security breach at TJX, where an estimated 94million records were compromised. Other breaches are entirely due to human error, like leaving personal data on computers that are subsequently lost or stolen. Attrition.org and the Identity Theft Resource Center are the only places keeping track of data breaches over the past few years. Check out their websites at <http://attrition.org> and <http://www.idtheftcenter.org>. See the original Associated Press article at <http://www.washingtonpost.com/wp-dyn/content/article/2008/01/01/AR2008010101714.html>

GOVERNMENT WEBSITES POST PERSONAL DATA

On January 2nd, the Washington Post reported that Social Security numbers are available on numerous government websites, despite warnings about identity theft from the government. The report also states that Social Security numbers are available on many government documents, including court documents. Starting in 2001, federal courts banned personal information from appearing on government documents, and some states, including Virginia, have passed either legislation or regulations regarding what kind of personal information are filed in government records. Before these precautions were taken, there were many documents filed that are not subject to the restrictions. Court clerks stated the impossibility of going back and taking out all the personal information on these records. The original article can be found at <http://www.washingtonpost.com/wp-dyn/content/story/2008/01/01/ST2008010102368.html>

GRAND JURY ISSUES SUBPOENAS IN MYSPACE SUICIDE CASE

On January 9th, the LA Times reported that a federal grand jury has issued subpoenas in the case of a Missouri teenager who committed suicide after being rejected by a person she thought was a 16 year old boy she met on MySpace. The case took a weird twist when it was discovered that the boy was not a boy at all, but the mother of one of the girl's former friends. Prosecutors in Missouri were unable to find a statute to prosecute the case, but the U.S. Attorney's office in Los Angeles is trying to charge the mother with defrauding MySpace through creating a false account. Because MySpace is based out of California, the subpoenas were issued in Los Angeles. The approach to convict the mother is novel, but could encroach on freedom of speech concerns. See the *LA Times* article at http://www.latimes.com/news/print/edition/california/la-me-myspace9jan09_0,993796_story?coll=la-headlines-pe-california

ISPS DEBATE ON PLAYING TRAFFIC COP, AT&T ON BOARD

On January 10th, at a panel discussion at the Consumer Electronics show, AT&T admitted it is looking into policing copyrighted material and preventing its distribution. AT&T endorsed the idea because peer-to-peer sharing uses up network bandwidth, which slows down its network for other users. The slope could be a slippery one for AT&T, as it could lead to user concerns about privacy, leading them to switch networks. Another concern of AT&T should be the expense of figuring out what constitutes a copyright violation. In 1998, AT&T and Verizon lobbied Congress for a safeguard against being held liable for its users' illegal activity, as the illegal content only passes through the network and it would be unreasonable to ask ISP providers to search for copyright infringers. Now, AT&T seems to be on the other side. Unsurprisingly, the entertainment industry supports the monitoring. The industry justification is that it is easy to figure out where copyright infringement is coming from on YouTube, but with peer-to-peer file sharing, it is more difficult, because there is not one place that the content comes from. Some feel that ISP monitoring seems to be the only solution to the problem. The future of ISP monitoring is uncertain, but watching how the battle of privacy concerns vs. copyright concerns plays out will be interesting. Check out the full article at http://www.news.com/Should-ATT-police-the-Internet/2100-1034_3-6226523.html and the *New York Times* article at <http://bits.blogs.nytimes.com/2008/01/08/att-and-other-isps-may-be-getting-ready-to-filter>

TIME WARNER TESTS NEW PRICING STRUCTURE BASED ON INTERNET USE

A new plan announced by a Time Warner spokesperson on January 16th stated that the company will offer different pricing guidelines based on how much data a user is transferring. The plan is intended to curb peer-to-peer sharing on its network because it uses up bandwidth. The new plan theoretically will increase the network efficiency, but could also scare away customers. Time Warner said it is going to do a test run in Texas, and the new pricing would only affect new customers. See the original story at http://www.news.com/8301-10784_3-9852800-7.html

LAWSUIT REVEALS THAT WHITE HOUSE RECYCLED BACKUP TAPES

In a court filing on January 15th, the White House admitted that until October 2003 they recycled backup tapes that contained e-mails. The backup tapes served two important purposes: to preserve records in case of a disaster, and to comply with federal record keeping laws. The initial lawsuit was filed by an advocacy group, Citizens for Responsibility and Ethics in Washington (CREW), in January last year. The suit alleges that millions of e-mails are missing from the White House archives. According to CREW, the filing also stated that the White House had inadequate methods for backing up e-mails, along with recycling the tapes. The chances for recovering the e-mails are slim, considering the overwriting and recycling practices. See the full *CREW* article at <http://www.citizensforethics.org/node/30771>

FORMER SYSTEMS ADMINISTRATOR GETS RECORD COMPUTER SABOTAGE SENTENCE

On January 8th, the United States Attorney for New Jersey announced that a former systems administrator for Medco Health Solutions, Inc. had been sentenced to 30 months in prison, the longest sentence on record for computer sabotage. The administrator, Yung-Hsun Lin, tried and failed to release a "logic bomb" that would have wiped out data on the server. First, the bomb did not detonate at its scheduled time, and then when Lin reinstated it, another systems administrator discovered it. Lin pleaded guilty and was sentenced to pay \$81,200 in retribution to Medco, along with his prison sentence. The full press release from the U.S. Attorney can be found at <http://www.usdoj.gov/usao/nj/press/press/files/pdf/files/lin1208%20rel.pdf>

OVER 10,000 U.S. WEBSITES POISONED BY NEW CRIMEWARE IN DECEMBER

On January 14th, security company Finjan announced its discovery of a malware attack that infected an estimated 10,000 websites in December. The company says the Trojan, dubbed "random js toolkit" infects a machine after visiting an infected website and the information is sent back to the "master" of the program over the Internet. The code that it encrypts onto the computer is not easily detected because the code randomly changes every time it is accessed. Finjan explains how to deal with the malware in its "Malicious Page of the Month" report. You can find the press release with a link to the report at <http://www.finjan.com/Pressrelease.aspx?id=1820&PressLan=1819&lan=3>

MYSFACE ENTERS INTO AGREEMENT TO PROTECT MINORS SAFETY

On January 14th, MySpace and 50 Attorneys General entered into an agreement to help protect minors on MySpace, to limit sexual predators' use of the site, and to prevent other misuses of the site. Some features of the agreement include: allowing parents to give MySpace their children's e-mail addresses to prevent anyone from setting up fake profiles using that e-mail, making it the default setting for 16 and 17 year olds' pages to be "private," responding within 72 hours to complaints about inappropriate content, employing more staff to check out pictures and groups, using better software to find underage users, and creating a high school section for users under 18. The full agreement can be found at http://www.ag.state.oh.us/press/08/01/pr080114_b.pdf and the announcement is available at http://www.naag.org/nations_attorneys_general_announce_nationwide_agreement_with_myspace_regarding_social_networking_saf.php

HOUSE OVERSIGHT COMMITTEE EXPOSES TSA SECURITY BREACH

On January 11th, the House Oversight Committee released a report about the Transportation Security Administration's (TSA) website explaining that the website opened up users to potential identity theft. TSA launched the website to help people who were erroneously placed on travel watch lists. The website contained an application where innocent travelers could apply to be taken off the list. The application required applicants to submit personal information, which was exposed to potential identity theft. Some problems included the fact that the website was not hosted on a government domain and that the website was not encrypted. The report investigated these problems and discovered that TSA granted the website contract without competition, the TSA manager in charge of the website was a former employee of the company awarded the website contract, and TSA did not provide sufficient oversight of the website, especially considering that these insecurities existed for months without discovery. The full press release from the House committee is at <http://oversight.house.gov/story.asp?ID=1680>

NEW REPORT FINDS MAJORITY OF MALICIOUS WEBSITES ARE LEGITIMATE SITES COMPROMISED BY HACKERS

In a report released on January 22nd, security company Websense, Inc. revealed that over half of malicious websites are legitimate websites infiltrated by hackers. The report found that there are about 2 million hacked websites online at any given time, and it can be any sort of website, ranging from small businesses to high powered firms. Even your favorite trusted websites could be infected, because infections result from complicated techniques that are not always easy to catch. There also are websites that keep track of what websites would be vulnerable to infection, because some vulnerabilities are in the website code itself. Information about these types of risks and more can be found in the full report at: http://www.websense.com/securitylabs/docs/SecurityLabsReport_Q4_011808.pdf

FEDERAL JUDGE RULES DATA HACKING NOT INSIDER TRADING

On January 8th, a federal judge in the Southern District of New York ruled that a man who hacked into the computer system of the Thompson Financial Network, and subsequently used the information to trade stocks, could not be held liable for insider trading under section 10(b) of the Securities and Exchange Act of 1934. The judge refused a request by the Securities and Exchange Commission (SEC) to prevent the defendant from gaining access to his profits. The judge ruled that though the defendant may have broken a criminal law, he had not violated section 10(b) because he did not owe a fiduciary duty to the source of his information or the people he transacted with in the market. In making the decision, the judge relied on a 1980 Supreme Court ruling saying "that a person who fails to disclose material information prior to a transaction commits fraud only when he is under a duty to do so." The SEC has appealed the ruling, arguing that a breach of a fiduciary duty is not required for deception under section 10(b). The full opinion can be found at http://pub.bna.com/eclr/07cv9606_010708.pdf

WARNER MUSIC GROUP SUES MUSIC SEARCH SITE

On January 18th, in the District Court for the Central District of California, Warner Music Group (WGM) filed a complaint against music search site Seeqpod. The complaint alleges Seeqpod infringed on WGM's copyrighted music, by making available unauthorized digital public performances. Further, the complaint alleges Seeqpod is getting paid for advertisements without compensating WGM. Seeqpod is a search engine and music player, on which people can search for songs hosted in other locations and stream those they like. Seeqpod claims the streaming is protected by the Digital Millennium Copyright Act, because it does not directly provide files to users. The full complaint can be found at <http://www.eff.org/files/Warner%20v%20SeeqPod%20complaint.pdf>

PUBLISHERS ANNOUNCE AGREEMENT WITH UNIVERSITIES ON COPYRIGHT GUIDELINES

On January 17th, the Association for American Publishers (AAP) announced an agreement with three universities (Hofstra, Syracuse, and Marquette) on new copyright guidelines for educational materials in digital format. The guidelines affirm that educational materials in digital content should be treated under the same copyright principles as those in printed format. Each university developed guidelines separately, tailoring the guidelines to the needs of the university. The AAP is hopeful the guidelines will serve as a model for other universities across the country. Negotiations for the guidelines began when teachers began posting copyrighted materials online for multiple students without getting permission from the publishers, though the teachers knew they should get permission for the printed materials.

The guidelines for Hofstra can be found at http://www.hofstra.edu/pdf/about/Policy/policy_ereserves.pdf

The guidelines for Syracuse can be found at <http://sunews.syr.edu/copyright.cfm>

The guidelines for Marquette can be found at http://www.marquette.edu/library/reserve/ereserve_copyright_guidelines.pdf

FTC SETTLES WITH 'LIFE IS GOOD' OVER FAILURE TO PROTECT CONSUMER INFORMATION

On January 17th, the Federal Trade Commission (FTC) announced that it had settled claims against online clothing retailer Life Is Good over failure to protect sensitive consumer information. The FTC claimed Life Is Good stored consumer information like names, addresses and credit card information without properly securing it on its website. The website had a security policy misrepresenting that consumer information was secure when it was not. Because of this lack of security, a hacker was able to get into the website and access consumer credit card information. The settlement said that Life Is Good cannot make any more deceptive claims about its security policies, and has to institute a comprehensive security plan to keep its users' data safe. The settlement also requires an independent auditor to ensure the company is keeping up with its requirements every other year for the next 20 years. The FTC press release on the agreement can be found at <http://www.ftc.gov/opa/2008/01/lig.shtm>

ATTORNEY SEARCHING ON EBAY HELPS CATCH ARTIFACT THIEF

On January 28th, the New York Attorney General's Office announced the arrest of an education department employee who stole artifacts from the New York State Library and sold them on eBay. A Richmond, VA lawyer noticed a John Calhoun artifact up for sale on eBay and was alarmed because he had seen the document before in a book on Calhoun. The lawyer notified the New York authorities, which led to the arrest of Daniel Lorello, an archivist with the state. Lorello was charged with grand larceny, among other things, and is reported to have made tens of thousands of dollars from other online sales. The press release of the Attorney General can be found here http://www.oag.state.ny.us/press/2008/jan/jan28a_08.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, [click here](#) and enter your real name, company name, and e-mail address.

Copyright © 2008 Sensei Enterprises, Inc. All rights reserved.