

{bytes in brief}

LAW AND TECHNOLOGY NEWS MONTHLY

EDITORS: Sharon D. Nelson, Esq. and John W. Simek
ASSOCIATE EDITOR: Nicole Kolinski EDITOR EMERITUS: G. V. Nelson



© 2009 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

Issue 145 - June 2009

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

ATM HACKERS STEAL \$500,000 FROM NYC RESIDENTS

On May 11th, the New York Daily News reported that “skimmers” were installed on Sovereign Bank ATM machines in Staten Island, allowing identity thieves to steal over \$500,000. “Skimmers” record the personal information on the magnetic strip on the back of ATM cards. The criminals also installed a tiny camera on top of the ATM that videotaped PIN numbers being entered on the machine. After the criminals obtained the information, they then downloaded the captured data and made duplicate ATM cards, which were then used at other banks to withdraw as much money as possible. Bank surveillance cameras recorded the criminals either as they were installing the items or when they were withdrawing cash, but no arrests have occurred. Sovereign Bank reimbursed the victims for their losses. The story may be found at http://www.nydailynews.com/news/ny_crime/2009/05/11/2009-05-11_automated_theft_bandits_steal_500g_by_rigging_atms_with_pinreading_gizmos.html

WHITE PAPER HIGHLIGHTS SECURITY ISSUES WITH CLOUD COMPUTING

On April 22nd, the Cloud Security Alliance released a white paper entitled “Security Guidance for Critical Areas of Cloud Computing.” While there is no single definition of what cloud computing is, the white paper lists five principal characteristics of cloud computing, including: abstraction of infrastructure, resource democratization, services oriented architecture, elasticity/dynamism of resources, and utility model of consumption and allocation. The white paper also covers three cloud delivery models and four cloud service deployment and consumption modalities. In addition to explaining the basics of cloud computing, the paper also includes fifteen different challenges of cloud computing, including legal, electronic discovery, and security issues. With the different modalities and types of cloud computing, security is particularly a problem. The paper may be found at <http://www.cloudsecurityalliance.org/guidance/csaguide.pdf>

CONGRESS INTRODUCES BILL TO PROTECT ELECTRICITY GRID

On April 30th, Senator Joe Lieberman and Representative Bennie Thompson introduced legislation in their respective chambers of Congress to help protect the security of the electricity grid in the United States from outside threats. The bill, entitled the “Critical Electric Infrastructure Protection Act,” will give increased power to the Department of Homeland Security (DHS) and the Federal Energy Regulatory Commission (FERC) to monitor and respond to electrical grid threats. When DHS identifies a threat, it will notify FERC, which will take appropriate measures through rulemaking procedures that can be suspended in case of an emergency. The bill also requires DHS to conduct an investigation to see if the electricity grid has already been compromised, and requires FERC to impose measures to deal with existing known threats. Senator Lieberman’s press release may be found at <http://lieberman.senate.gov/newsroom/release.cfm?id=312322&&>

SOME COLLEGES LOOK AT APPLICANTS’ SOCIAL NETWORKING PROFILES

On April 29th, the National Association for College Admission Counseling released a report indicating about one-

fourth of U.S. colleges reported doing some research about potential applicants on social networking websites such as Facebook or MySpace. The study did not indicate whether admissions or scholarships were revoked based on what was found on the site, but the author of the report explained that “no school wants to give a prestigious scholarship to someone standing on a beer keg and wearing a lampshade.” A good rule of thumb for high school students hoping to avoid this problem: the grandma rule. If you would not want your grandmother to see anything that you are writing or posting on a social networking site, then take it down. The potential losses are too great for one silly photo or comment. The NACAC press release may be found at <http://www.nacacnet.org/AboutNACAC/PressRoom/2009/Pages/SocialNetworking.aspx>

MAN PLEADS GUILTY TO SENDING THREATENING VA TECH E-MAIL

On April 28th, Johnmarlo Balasta Napa pled guilty to one count of transmitting a threat in interstate commerce for an e-mail he sent to two former Virginia Tech students that glorified the Virginia Tech shooting that took place in April two years ago. Napa sent the e-mail on the eve of the one-year anniversary of the shooting from an e-mail address entitled “seunghuichorevenge@yahoo.com.” The e-mail contained photos of the shooter, Sueng Hui Cho depicted as a hero, a picture of Cho holding paper dolls of the two students, and excerpts of Cho’s manifesto he sent to a TV network before the shootings. The two students immediately contacted the authorities after receiving the e-mail. Authorities traced the e-mail to a computer server at Nevada State College, where Napa was a student. Police focused on Napa because he was suspected of planning a shooting at Nevada State. When police searched Napa’s home, they found \$3,000 worth of guns he had purchased in a two-day period, including the same model Cho used. Napa’s lawyer stated that she might appeal the decision, because the e-mails did not constitute intent to harm, however distasteful they were. The story may be found at http://news.yahoo.com/s/ap/20090428/ap_on_re_us/us_virginia_tech_threat

MCAFEE LAUNCHES FREE CYBERCRIME HELP CENTER

On April 28th, security provider McAfee launched the first online help center to assist victims of cybercrime. The Cybercrime Response Unit will help victims of cybercrime find various resources to address the situation, including law enforcement and credit reporting agencies. In serious cases, trained Cybercrime Unit Agents are available by phone to discuss the problem. The service also includes a forensic scanning tool, which identifies whether a computer has been infected by malware or whether a user has visited malicious websites that steal personal information. Some common indicators that a computer is at risk include if the computer runs slower than usual, unexplained charges on bank or credit card accounts, or if a computer was recently lost or stolen. The McAfee press release may be found at http://newsroom.mcafee.com/article_display.cfm?article_id=3511

GOOGLE UNVEILS NEW TOOLS TO FIND PUBLIC DATA

On April 28th, Google launched a new tool called Google Public Data to help people search for public data, such as the unemployment rate, that can be hard to find on government websites. The goal of the tool is to make public data more accessible to citizens. With the tool, users can search for a specific piece of data and a box appears at the top of the search results displaying the available public data. Currently, the tool compiles information from the Bureau of Labor Statistics and the U.S. Census Bureau’s population division, and makes it easier to use in a graphical format. Data from other agencies, such as the Environmental Protection Agency, will be available in the next few months. The Google blog post may be found at <http://googleblog.blogspot.com/2009/04/adding-search-power-to-public-data.html>

FBI ARRESTS MAN AFTER TWITTER THREATS

On April 26th, CNET News reported that Daniel Knight Hayden had been arrested after the FBI identified him as Twitter user CitizenQuasar, who used Twitter to send out threatening messages about starting a “war” against the government at the Oklahoma City Capitol. The posts were in response to a tea party tax protest scheduled to take place on election day. Many of the messages were directed towards an Oklahoma City man, Earl Shaffer, who Hayden erroneously believed organized the protests. Shaffer, who is 68 and retired, stated that he was unnerved

that Hayden knew so much about him and made threats on his life. One of Hayden's other posts included threats of cutting off police officers' heads and throwing them on the state capitol steps. Hayden is charged with making interstate threats, and was arraigned on April 16th and released to an Oklahoma City halfway house. The story may be found at <http://news.cnet.com/fbi-accuses-twitter-user-of-massacre-threats/>

ADVISORY OPINION DISCUSSES FRIENDING WITNESS ON FACEBOOK

A March 2009 advisory opinion of the Philadelphia Bar Association discussed what an attorney should do if he wants to view a potential witness's Facebook or MySpace page. A profile is discoverable information, but there are acceptable and unacceptable ways to go about it. The opinion indicated that if an attorney wants access to the page, then he or she should simply ask for permission. Asking a third party to "friend" the person would be unethical because it is deceptive, since the witness would not know the true purpose of the friend request – to obtain information for use in a lawsuit or to impeach the witness's testimony at trial. Understandably, many witnesses would not grant access to their profiles in that situation. Online profiles are different from open spaces where an attorney could discover information through observing the person because an invitation is required to access the profile. The opinion may be found at http://www.philadelphiabar.org/WebObjects/PBARReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf

MICROSOFT RE-NAMES CONTROVERSIAL ANTI-PIRACY TOOLS

On May 7th, Microsoft announced that it had re-named its Windows Genuine Advantage (WGA) validation system in Windows 7, now calling it Windows Activation Technology (WAT), because it more accurately reflects how the technology works. The WGA/WAT system checks to see if someone is running a genuine copy of Windows, and if not, the software runs a series of pop-up alerts to remind the user that their software is counterfeit. The new activation tool has many improvements, as it includes support for virtualized images and volume activation for multiple operating systems to support new technologies since the time WGA was initially released in 2006. The tool was introduced as part of Microsoft's effort to crack down on piracy, and was initially criticized for its early bugs. The Microsoft press release may be found at <http://www.microsoft.com/presspass/features/2009/May09/05-07Piracy.msp>

REPORT FINDS FAA COMPUTERS HACKED MULTIPLE TIMES

On May 4th, an Inspector General report announced that the Federal Aviation Administration (FAA) computers were broken into multiple times in the past few years. The most recent hacking occurred in February, when hackers compromised a public facing computer and accessed personal information such as Social Security numbers on 48,000 current and former FAA employees. Last year, hackers took over FAA network servers and could have shut them down. The hackers did so by gaining access to an FAA computer in Alaska, stole an administrator's password, and then installed malicious code and compromised the FAA domain controller, giving them control over the network. According to the report, the breaches happened because web applications that support the FAA systems were not properly secured to prevent unauthorized access and network monitoring programs were not used to detect cyberattacks. The FAA stated that it was identifying and fixing weaknesses in its systems. The report may be found at http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/ATC_Web_Report.pdf

VA COURT FINDS BEST EVIDENCE RULE INAPPLICABLE TO VIDEO

On May 12th, the Court of Appeals of Virginia held that allowing the testimony of a witness about events he witnesses on a surveillance video without admitting the video itself did not violate the best evidence rule. The defendant, Maurice Brown, was convicted of grand larceny based on the testimony of a store employee that he watched Brown steal frozen crab legs on the video. The court explained that the best evidence rule stands for the proposition that when one is trying to prove something, he should prove it by the most reliable evidence available. In Virginia, the best evidence rule is a term of art that applies only when trying to prove the contents of a writing. The court explained that a writing was defined by statute to include only letters, words, or numbers. Therefore the

surveillance video was not a writing, was not covered under the best evidence rule, and the testimony was admissible. While the Federal Rules of Evidence include videotapes as “writings” for the purpose of the best evidence rule, the court declined to extend the best evidence rule in Virginia without the approval of the legislature. The decision may be found at <http://www.courts.state.va.us/opinions/opncavwp/1034082.pdf>

FAKE SEARCH ENGINES USED TO SPREAD MALWARE

On May 5th, a PandaLabs blog posting warned that cybercriminals were using fake search engines to link to malicious websites. The fake search engines are showing up in Google search results, and when the user searches for something like “flu statistics” in the fake search engine, the results re-direct the user to porn websites. The porn website then asks the user to download what purports to be the latest version of a video player, but really is malware. Searching for security topics on these fake search engines leads to fake antivirus sites. The clear lesson is to use reputable web search sites. The blog post may be found at

<http://pandalabs.pandasecurity.com/archive/Swin-flu-and-the-Blackhat-SEO-techniques.aspx>

GOOGLE CHANGES ADWORDS TO ALLOW TRADEMARKS IN SOME AD TEXT

On May 14th, Google announced on its AdWords blog that it was modifying its trademark policy to allow some ads to use trademarks in the ad text for U.S. users, even if the advertiser does not actually own the trademark or have explicit permission to use it. To use the trademarks in ad text, advertisers must be using the trademarks for a specific purpose allowed by Google, including those that resell the trademarked goods, sell components or parts of trademarked goods, or are providing information about trademarked goods. To let companies know whether they can advertise certain brands, Google added a function to its Search Based Keyword Tool that lists all of the brands that appear on a company’s website that may be used for ads. Google stated that the change brings its trademark policy in line with industry standards and would improve advertising by allowing advertisers to narrowly target ad text that highlights the specific products sold by the advertiser. The AdWords blog post may be found at

<http://adwords.blogspot.com/2009/05/update-to-us-ad-text-trademark-policy.html>

REPORT FINDS THAT MALWARE GREATER THREAT THAN CONFLICKER WORM

On May 5th, McAfee released its first quarter security report for 2009, which found that 12 million new computers were infected by malware since January, a 50% increase from 2008. The report found that the United States now hosts the largest percentage of infected computers at 18%, with China coming in second at 13.4%. The expansion of botnets used to spread malware has provided cybercriminals with the infrastructure needed to commit cybercrime, according to Jeff Green, senior vice president of McAfee Avert Labs. While threats such as the Conflicker worm are important, other threats may pose a greater risk, such as malware or the Koobface virus going around Facebook. The report also finds that spam levels will probably rise again in 2009, as spammers recover from the shutdown of the McColo server farm in November. Since then, the volume of spam has increased 70%. The report may be found at

http://img.en25.com/Web/McAfee/5395rpt_avert_quarterly-threat_0409_v3.pdf

LEXISNEXIS HIT BY DATA BREACH

On May 1st, online information service LexisNexis notified 32,000 people that their personal information may have been compromised in a credit card fraud scheme. The breach compromised information from both LexisNexis in New York, and another company that conducts background checks, Investigative Professionals, based out of New Mexico. Of the 32,000, about 300 people had personal information used fraudulently to obtain fake credit cards in their name. All of the 300 people had been notified by postal authorities, who are investigating the scheme. No arrests had been made, but authorities were wrapping up the investigation. The story may be found at

http://www.usatoday.com/money/industries/technology/2009-05-01-lexisnexis-warns-of-data-breach_N.htm

MISTRIAL DECLARED WHEN WITNESS TEXTED BOSS FROM WITNESS STAND

On May 13th, Miami-Dade Circuit Judge Scott Silverman declared a mistrial in a civil fraud case after a witness on the stand was text messaging about his testimony to his boss at the counsel table while the judge had a sidebar conference with attorneys. The case arose out of a sale of an apartment complex. The plaintiff, Sky Development, accused the defendant, Vistaview Development, of fraudulently misrepresenting the number of two bedroom units in the apartment complex purchased by Sky. On the stand was Sky chief operating officer Gavin Sussman, who was text messaging Sky chief executive Yizhak Toledano at the plaintiff's table. A courtroom observer passed a note to a defense attorney that Sussman appeared to be text messaging, which the attorney brought to the judge's attention. The defense then moved for a mistrial, which Silverman granted as he described Sussman's conduct as "outrageous." The text messaging violated a basic trial rule that prevents anyone from communicating with a witness about their testimony while on the stand, including during breaks. The situation highlights the current dilemma of whether cell phones should be allowed in courtrooms, as recently judges have also declared mistrials for jurors doing outside research from their smartphones. The story may be found at

<http://www.law.com/jsp/law/careercenter/lawArticleCareerCenter.jsp?id=1202430721257&rss=careercenter>

FACEBOOK TO OFFER VERIFIED APPLICATIONS

On May 14th, Facebook announced a number of new changes that would be taking place, the most notable of them the "Verified Apps" program. The program was announced in November, but will be launching in the next few weeks. For a \$375 fee, Facebook will review apps to ensure that they meet security and transparency standards, and will award a badge to those that meet these standards. Ensuring that applications are trustworthy is particularly important in light of the phishing attacks that have recently hit Facebook. Verified applications will also be ranked higher in the Facebook directory, which is advantageous because there are more than 52,000 applications. The directory also will feature better categories, and update application profile pages so that they look more like public profile pages. The Facebook blog post may be found at

<http://developers.facebook.com/news.php?blog=1&story=244>

UK POLICE HAVE TOO MUCH SURVEILLANCE DATA TO HANDLE

On May 15th, CNET News reported that the police in the United Kingdom are overwhelmed by the amount of surveillance data from four million surveillance cameras. The director of information for the Association of Chief Police Officers Criminal Records Office, Ian Readhead, stated that he was concerned that the police cannot track a car in real time due to the volume of the data. Tracking cars in real time was one of the purposes of the Automatic Number Plate Recognition System, to enable the police to track a car that contained a kidnapped child, for example. But Dominic Grieve, a politician, said that the surveillance cameras are not primarily used to prevent crime, as the police do not have enough resources to look at the footage in real time. Instead the cameras are used to provide evidence of crimes after they occur. The story may be found at http://news.cnet.com/8301-1009_3-10241664-83.html

NYC OFFICIALS STOP INTERNATIONAL IDENTITY THEFT RING

On May 14th, New York City Police Commissioner Kelly and Queens District Attorney Richard Brown announced the breakup of an international credit card and identity theft ring that victimized more than 6,000 customers and caused about \$15 million in losses. More than 35 people were indicted on enterprise corruption charges in New York State Supreme Court, with 22 pleading not guilty. The suspects were mostly Nigerian nationals living in New York. Some of the ringleaders were still at large, with one believed to be in Nigeria. Investigators first discovered the scheme in September 2007, when a Queens real estate office opened a package and found 60 valid credit cards in different names. The police then used a variety of techniques to uncover the schemes, from surveillance and wiretapping to executing search warrants that found large amounts of cash, machines used to make fake IDs and computers. The ring was made up of three different enterprises working together. Legitimate credit cards were re-routed to the criminals who used them to withdraw cash. The scheme also used personal identification information to loot accounts, and ran ID mills that made fraudulent licenses and credit cards. The press release may be found at

http://www.queensda.org/newpressreleases/2009/may/operation%20plastic%20pipeline_05_2009_ind.pdf

MICROSOFT PROVIDES FREE SERVICE TO CHECK THE STRENGTH OF PASSWORDS

On May 22nd, Microsoft announced that it was offering a free password checker to determine the strength of your password, i.e. how easily the password can be cracked by hackers. When it comes to passwords, the best ones have at least 14 characters and include a mix of numbers, symbols, uppercase letters and lowercase letters. The password checker does not record your password information; it generates a response based on the nature of the input. When you type your password into the checker, it immediately gauges whether your password is weak, medium, strong, or best. Creating a strong password is one step in protecting against identity theft. Microsoft's advice on how to create a strong password may be found at

<http://www.microsoft.com/protect/yourself/password/create.mspx>

The password checker may be found at <http://www.microsoft.com/protect/yourself/password/checker.mspx>

WISCONSIN APPELLATE COURT – NO WARRANT REQUIRED FOR GPS TRACKING

On May 7th, the Fourth District Court of Appeals in Wisconsin held that no warrant is required when police attach a GPS device to the outside of a vehicle because no search or seizure occurs. In the case, defendant Michael Sveum was convicted of aggravated stalking based partially on evidence obtained from a GPS tracking system that the police put on his car. The police in his case had a warrant, but Sveum's attorneys argued that the GPS tracked Sveum's movements out of the public view, for instance in his garage. The court disagreed, and found that police could have seen Sveum entering and leaving the garage through visual surveillance. Under the current law, the court explained that it appeared that anyone could track anyone without implicating the Fourth Amendment by attaching a GPS tracking device to his or her car. The court expressed its concern with its conclusion, as some GPS tracking could be used for illegitimate purposes, and urged the legislature to pass laws governing the use of such devices. The decision may be found at <http://www.wisbar.org/res/capp/2009/2008ap000658.htm>

STUDY FINDS SOFTWARE PIRACY GROWING

On May 12th, the Business Software Alliance announced the results of its annual study, which found that software piracy rates rose from 38% in 2007 to 41% in 2008, meaning that 41% of all software installed is pirated. Losses to companies from pirated software were estimated at \$53 billion in 2008. There was progress fighting piracy in some countries in the past year, particularly in China and Russia. While U.S. piracy was only 20% of the total market, lowest in the world, the number is still important because more software is sold in the U.S. than anywhere else. Many losses come from businesses that use unlicensed copies of software programs, e.g. have 50 computers but only pay for rights to the software on 25 computers. The BSA press release may be found at

<http://www.bsa.org/country/News%20and%20Events/News%20Archives/global/05122009-idx-globalstudy.aspx>

CRAIGSLIST SUES SC ATTORNEY GENERAL

On May 20th, Craigslist announced that it was suing South Carolina Attorney General Henry McMaster for threatening Craigslist executives with criminal prosecution for aiding prostitution. The lawsuit stemmed out of Craigslist's recent struggles with its "erotic services" section, which was modified recently due to requests by state Attorneys General. McMaster claimed that the changes made by Craigslist were inadequate, and said that his office had "no alternative but to move forward with criminal investigation and potential prosecution." Craigslist believes that it is protected under the "safe harbor" provisions of the Communication Decency Act, which provides that an Internet company is not responsible for the activities of its users. Craigslist chief executive, Jim Buckmaster, explained that McMaster's threats would force Craigslist to remove the sites in South Carolina, and that the format of Craigslist made it impossible to prevent all solicitation or pornography. McMaster responded to the lawsuit by calling it "good news" and saying that he would continue to monitor the site. The Craigslist blog post may be found at <http://blog.craigslist.org/2009/05/cl-sues-sc-ag-for-declaratory-relief/>

A new story including McMaster's comments may be found at http://news.cnet.com/8301-1023_3-10245380-93.html

NATIONAL ARCHIVES OFFERS REWARD FOR MISSING HARD DRIVE

On May 20th, the National Archives offered a reward of \$50,000 for information relating to a missing hard drive that contains personal information of former Clinton administration staff and visitors. The hard drive was last seen in October 2008, and was discovered missing in late March 2009. The Archives conducted an investigation after it realized the hard drive was missing, but did not know whether the hard drive was lost, stolen, or missing. No original information was lost, as the hard drive was being kept as a backup and contained snapshots of hard drives of employees who left the Executive Office of the President. The individuals affected will be notified and offered a year of free credit monitoring. The National Archives Q&A may be found at <http://www.archives.gov/news/clinton-hard-drive-faq-2009-5-20.pdf>

WHITE HOUSE DOES NOT HAVE TO TURN OVER MISSING E-MAILS

On May 19th, the D.C. Circuit Court found that Bush Administration e-mails did not have to be turned over to the Citizens for Responsibility and Ethics in Washington (CREW) because the White House was not an "agency" under the Freedom of Information Act. CREW requested information about the Bush Administration's electronic record keeping system. The Bush Administration responded that there were nearly 3,500 pages of documents relating to problems with that system, but stated it did not have to turn the documents over. The court unanimously determined that the Office of Administration only performs support tasks for the president, and does not have independent authority like an agency. CREW stated its disappointment in the decision, particularly after the Obama Administration championed a more transparent government, but then sided with the Bush Administration in the dispute. The opinion may be found at <http://www.citizensforethics.org/files/20090519%20-%20OA%20Circuit%20Decision.pdf>

ILLINOIS JUDGE FINDS SHIELD LAW DOES NOT PROTECT BLOGGERS

On May 15th, Madison County, Illinois Circuit Judge Richard Tognarelli ruled that the Alton (IL) Telegraph had to turn over the identities of two people who commented on the newspaper's website. The judge found that the Illinois shield law that protects reporters from revealing their sources does not apply to "online bloggers." The comments on the website had to do with the murder investigation of a five-year old boy. While many people commented, two identities had to be revealed, but three did not because they did not appear to contain relevant information. The judge explained that since the law did not specifically address the issue of bloggers, it was up to the legislature to change the law. The story may be found at <http://www.stltoday.com/stltoday/news/stories.nsf/laworder/story/C00A2A4B72C13760862575B8000C9D3F?OpenDocument>

HACKERS BREAK INTO VA PRESCRIPTION DATABASE, DEMAND RANSOM

On May 6th, the Virginia Department of Health Professions (DHP) announced that an unauthorized message appeared on the DHP's Prescription Monitoring Program (PMP) website. The program helps doctors and pharmacies track the sale of powerful narcotics and painkillers to help reduce the abuse and illegal sale of controlled substances. The system contained 31.6 million prescription records as of January 1st. The message was from hackers who claimed to have broken into the pharmaceutical database and stolen prescription and patient records. The hackers gave the state one-week to provide \$10 million for the records, or they would sell access to the database to the highest bidder. State officials claimed that it was unclear whether the hackers actually had access to the records or not, but that a full investigation was underway to determine who the hackers were. The PMP computer system was shut down since the data breach, but the data was backed up and files were secured. Despite the hacking, on May 19th Virginia Senator Mark Warner held a conference in Richmond explaining the benefits of digitizing patient records. One benefit of digitizing records is that it would eliminate the need to do expensive tests multiple times, because doctors would have access to the first test through the digital record. However, Warner stressed that one of the keys to the electronic records was to ensure security and privacy. Coverage of Senator Warner's conference may be found at http://warner.senate.gov/public/index.cfm?p=Blog&ContentRecord_id=2c4049c7-e87d-42fc-95aa-

ade06fbdbb8f&ContentType_id=ec227f31-cc52-4e56-87db-385a02e2bceb

The DHP press release may be found at http://www.dhp.state.va.us/misc_docs/Statement050609.pdf

The May 14th DHP update may be found at http://www.dhp.state.va.us/misc_docs/PMPQA51409.pdf

GOOGLE EXPERIENCES OUTAGE DUE TO NETWORKING ERROR

On May 14th, Google experienced widespread outages for several of its services, including search, Google docs, and Gmail. A Google blog post explained that the outage was due to a glitch in the system that caused all traffic to be re-routed through Asia, which caused a “traffic jam.” The blog post stated that 14% of Google users experienced slow services or interruptions. Google apologized for the error and said that it was constantly looking for ways to improve its system so situations like this will not happen again. On May 18th, Google experienced another outage that only impacted the Google News service. When some users tried to access Google News, they would receive a “503 Server Error” asking them to try again in 30 seconds. The second outage was not as widespread as the first, but was reported by users in California and Massachusetts. The Google Blog post may be found at <http://googleblog.blogspot.com/2009/05/this-is-your-pilot-speaking-now-about.html>

A news story on the second outage may be found at http://www.pcworld.com/article/165046/google_suffers_another_service_outage.html

FTC FILES SUIT TO STOP ILLEGAL ROBOCALLS

On May 14th, the Federal Trade Commission announced that it had filed suit against two companies engaged in a telemarketing campaign that conducted hundreds of millions of deceptive robocalls. The robocalls purported to sell consumers vehicle service contracts by pretending they were extensions of original vehicle warranties. Consumers who respond to the robocalls are pressured to purchase the extended service contracts for their vehicle, which are not extensions of the original warranty. These calls resulted in 30,000 consumer complaints, and \$10 million in sales. The FTC is seeking a permanent injunction to force defendants to give up their gains to repay consumers. A federal judge granted two temporary restraining orders against the two companies, which ordered the companies to stop making the calls and froze their assets. The FTC press release may be found at <http://www.ftc.gov/opa/2009/05/robocalls.shtm>


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.