

{ 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



© 2008 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

Issue 138 - November 2008

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

SENATE UNANIMOUSLY PASSES COPYRIGHT BILL

On September 26th, the Senate unanimously passed a bill that would increase intellectual property protection. Senators Patrick Leahy and Arlen Specter introduced the bi-partisan bill in July. The final version of the bill got rid of a controversial measure that allowed federal prosecutors to file civil lawsuits against peer-to-peer users that violate copyright laws. The bill still includes measures for coordination between federal and state efforts to fight piracy, increased resources for the Justice Department to fight intellectual property theft, and increased penalties for infringements. The bill also would replace the current enforcement body with a White House Intellectual Property Enforcement Coordinator, which the Bush Administration opposed on constitutional grounds. The Recording Industry of America and the Motion Picture Association of America supported the bill, while other groups opposed it for going too far.

Senator Leahy's press release, with links to the full legislation and the changes, may be found at <http://leahy.senate.gov/press/200809/092608b.html>

JUDGE ORDERS NEW TRIAL IN COPYRIGHT INFRINGEMENT CASE

On September 25th, U.S. District Judge Michael Davis threw out the verdict against Jammie Thomas, who was convicted of illegal file sharing last year with \$222,000 ordered as damages. Judge Davis rejected the RIAA's main theory of liability for Thomas, which was that she violated the copyright laws by making the files available for download. Instead, the court held that there needed to be proof of distribution to show that Thomas violated the copyright laws. Since Judge Davis ordered a new trial, he did not have to determine whether the damages were excessive, but he hinted that they were. Thomas was convicted of sharing twenty-four songs, or about three CDs worth \$54, but the cost to the record companies was 4,000 times that cost. Judge David encouraged Congress to reconsider these fines and to set damages high enough to deter file sharing without being excessive.

The decision may be found at http://beckermanlegal.com/Lawyer_Copyright_Internet_Law/virgin_thomas_080924Decision.pdf

VERIZON, AT&T, PLEDGE TO GET PERMISSION TO TRACK INTERNET USERS

On September 25th, at a Senate committee hearing, Internet Service Provider giants Verizon and AT&T pledged their support for consumer privacy practices, including getting permission before tracking Internet use. Behavioral advertising, which collects user Internet data and then produces ads based on that data, has been a recent privacy concern, as the practice is usually done without users knowledge or consent. Verizon laid out three practices for the basis of its program, which were transparency, meaningful consent, and consumer control. With these principles, the user would know about the tracking, be able to consent to it or not, and be able to retract consent at any time. AT&T laid out similar principles, and also included that the users' identity would be protected at all time. Dorothy Atwood, the AT&T chief privacy officer, also attacked Google for its privacy practices. Currently, Google has an "opt

out” option for consumers instead of an “opt in” option. The new proposals present a challenge to the other companies about which option they should use.

The Verizon press release may be found at <http://newscenter.verizon.com/press-releases/verizon/2008/verizon-calls-for-industry.html>

The AT&T press release may be found at <http://www.att.com/gen/press-room?pid=4800&cdvn=news&newsarticleid=26121>

FAKE FACEBOOK FRIEND REQUEST E-MAIL ADDS MALWARE

On September 22nd, security firm Websense alerted people to a new e-mail threat from a fake Facebook “friend request” e-mail. This e-mail is another example of cyber criminals capitalizing on the popularity of social networking sites with their scams. Facebook sends out alert e-mails when one user adds another user as a friend. The fake e-mail purports to be one of those, but it contains an attachment to a picture to try to get the recipient to click on it. When clicked, the attached file is really a Trojan horse. Real Facebook friend requests do not contain attachments. The e-mail also contained a link to the login form for the Facebook page, but this page was real, probably to make the e-mail seem more legitimate. The scam shows that users should be careful when looking at e-mails from social networking sites.

The Websense alert may be found at <http://securitylabs.websense.com/content/Alerts/3185.aspx>

U.S. COMPUTERS MAY HAVE BEEN RESPONSIBLE FOR GEORGIA CYBERATTACK

On September 22nd, SecureWorks released a list of the countries with the most computers infected by botnets. The United States ranked first on the list, which could explain where the cyberattacks in Georgia came from. While Russia may have been the real culprit, the Russians did not attack through Russian IP addresses. Instead, the Russians used computers and servers in Turkey, while the botnets came from the United States. Since Georgia could not cut off traffic from Turkey because the Turkish telecom network is Georgia’s main provider, it could not stop the attacks. Georgia also was not prepared to cut off traffic from the United States. The United States is number one on the botnet list because of the number of computers per capita, and because many of these computers are unsecured and not patched. The rest of the botnet list, in order, included China, Brazil, South Korea, Poland, Japan, and Russia.

The SecureWorks press release may be found at http://www.secureworks.com/media/press_releases/20080922-attacks/

A CNET news article about the Georgia attacks may be found at http://news.cnet.com/8301-1009_3-10049008-83.html

COURT DISMISSES STUBHUB LAWSUIT UNDER COMMUNICATIONS DECENCY ACT

On September 9th, the U.S. District Court in Oregon dismissed a lawsuit against Stubhub and eBay because the websites were protected under the Communications Decency Act. Bruce Springsteen fan Sharon Fehrs filed a lawsuit against the companies after tickets for the Springsteen concert at the Rose Garden Arena in Portland, Oregon were sold on the websites for a much higher price than the official box office. Fehrs claimed the resale violated the Portland City Code, which prohibits the sale of tickets over retail price for events in municipally owned arenas like the Rose Garden. StubHub and eBay moved to dismiss under the Communications Decency Act, which provides a “safe harbor” for interactive computer services so they may not be held liable for content provided by third parties. StubHub and eBay argued that since they are online marketplaces, and do not own or sell the tickets listed, they were not liable for the actions of the ticket sellers on their websites. The court accepted that argument and dismissed the lawsuit.

The motions may be found at

<http://cyberlaw.stanford.edu/system/files/Fehrs-StubHub-Defns-Rule21-Motions-2-13-08.pdf>

MICROSOFT CAVES, GIVES XP EXTENSION YET AGAIN

On October 3rd, CNET news reported that Microsoft was giving users another chance to get XP. Microsoft technically stopped selling XP on June 30th. But major computer manufacturers are allowed to use XP for low-cost computers, and now can sell the upgraded versions of Vista (Ultimate and Business) with XP discs. Another option is to sell "factory downgraded" Vista computers with XP instead. Microsoft was supposed to stop providing XP discs at the beginning of 2009, but extended the deadline six months until July 31st, 2009. Microsoft told CNET the move was only to make a smooth transition to Vista. A more likely explanation is that all of the complaints about Vista make users reluctant to switch.

The story may be found at

http://news.cnet.com/8301-13860_3-10057617-56.html

CONGRESS ASKS FCC TO EXPLORE CONTENT BLOCKING TECHNOLOGY

On October 1st and 3rd, the Senate and House passed the Child Safe Viewing Act. Both houses passed the bill unanimously, but the House made changes that required the bill to go back to the Senate for re-consideration. The bill requires the Federal Communications Commission to examine what content blocking avenues are available for different types of electronic devices. The bill also requires the FCC to consider how to implement the new technology without detrimentally affecting prices. The House altered the Senate bill by eliminating a Senate finding that blamed TV for the need to discover content blocking technology. The House version still requires the FCC to report on the technology, and is one step towards making new technologies safer for children.

The text of the legislation may be found at

<http://thomas.loc.gov/cgi-bin/query/z?c110:S.602:>

MICROSOFT, WASHINGTON STATE SUE FAKE SECURITY PROGRAMS

On September 29th, Microsoft and the state of Washington filed suit against vendors of fake security programs that send notices to users saying the computer is at risk. The tactic is known as "Scareware," and the threats are sent to try to get the user to buy anti-virus software. Both the threats to the computer and the supposed protection are fake. One example of a "Scareware" company is Branch Software, which tries to facilitate sales of its "Registry Cleaner XP" software through popup ads containing false information. Washington Attorney General Rob McKenna stated that these types of programs would not be tolerated. Microsoft has filed a series of similar lawsuits against a wide array of fake software vendors.

McKenna's press release, with a link to the complaint, may be found at

<http://www.atg.wa.gov/pressrelease.aspx?&id=21026>

VERIZON RELEASES DATA BREACH REPORT

On October 2nd, Verizon released a report on data breaches that indicated a number of industry specific challenges. The report emphasizes particular challenges to each industry, showing that security needs are not "one size fits all." For the financial services market, data breach problems tended to come from insiders and took longer to detect. For high technology firms, the biggest threats were malicious insiders and hackers, whose behavior was difficult to control because the employees had unlimited access to many different systems. The retail industry recorded the largest number of data breaches, with most coming from remote access connections and Internet applications. For the food and beverage industry, poor security configurations were a major point of concern. The

report also warns against companies outsourcing to third-party vendors, as many of the third party companies have caused breaches due to a lack of oversight.

The Verizon press release with a link to the report may be found at <http://newscenter.verizon.com/press-releases/verizon/2008/verizon-business-data-breach.html>

SKYPE MONITORS MESSAGES IN CHINA

On October 1st, Internet research group Citizen Lab released a report announcing that the text messages of Skype users in China are being monitored for politically sensitive keywords. When the keywords were found, the messages were logged onto a publicly accessible server. The log files revealed information such as the IP addresses and usernames used to place the calls, along with the message content. Skype President Josh Silverman tried to downplay the finding in a blog post explaining that the Chinese service provider, TOM, had to comply with Chinese laws to operate. It is clear that China has been monitoring communications for years, implying that TOM would not be able to operate if it did not monitor communications. Silverman also made vague reassurances that the problem was being worked on.

The Citizen Lab report may be found at <http://deibert.citizenlab.org/breachingtrust.pdf>

The Skype blog post may be found at http://share.skype.com/sites/en/2008/10/skype_president_addresses_chin.html

MORE AMERICANS PREFER MOBILE PHONES OVER LANDLINES

On October 2nd, J.D. Power and Associates announced the results of its 2008 Wireless Regional Customer Satisfaction Index Study. The study found that 25% of wireless phone users were not using a wired landline phone anymore. The move away from landlines was largest among wireless users between age 18 and 24, as nearly 30% of these users disconnected landline phones. Landlines are still used by older people, as only 9% of those over 65 had disconnected their landlines. The study also asked about the most important wireless factors, which were, in order: call quality, brand image, cost of service, service plan options, billing, and customer service. Of wireless service providers, Verizon ranked at the top in five of the six regions, with T-Mobile at the top in the remaining region.

The story may be found at <http://www.jdpower.com/telecom/articles/2008-U.S.-Wireless-Contract-Regional-Satisfaction-Study>

MITNICK WARNS OF BRINGING COMPUTERS ABROAD AFTER DETENTION

On October 1st, CNET news reported that Kevin Mitnick, a former hacker who served five years in prison, was detained on a trip back from Columbia to visit his girlfriend. Mitnick landed in Atlanta on September 16th to speak at a security conference, and was detained for four hours while customs officials questioned him and went through his electronic equipment, including laptops, external hard drives, and cell phones. When agents asked for proof that he was in Atlanta to attend a conference, Mitnick turned on his laptop to access his e-mail. When he replied to a default Firefox security question concerning the automatic deletion of personal information, the agents snatched his laptop, thinking he was trying to delete evidence. Mitnick quickly reached over and turned off his computer so the agents would not have access. After corroborating his story with an FBI agent at the conference, Mitnick was finally let go. Mitnick described the situation as nerve-wracking because he did not know what was going on. Even worse, officials in Columbia suspected that a package Mitnick mailed to a U.S. address contained cocaine. The officials opened the package, and destroyed the hard drive inside by drilling a hole in it to ensure it did not contain drugs. The two incidents were unrelated, but raise red flags for those traveling abroad.

The story may be found at
http://news.cnet.com/8301-1009_3-10054569-83.html

GOOGLE HELPS PEOPLE NAVIGATE NYC

On September 23rd, Google announced a new feature to help people navigate New York City's public transit system. The Google Transit tool incorporates subway stops, bus routes and commuter trains to outlying areas such as New Jersey and Long Island. The Google Transit system operates like Google Maps, as the user may type in a departure point and destination, and get written directions and a map of how to get there. With Google Transit, users may choose their mode of transportation, which gives information on when and where to change trains and how long until the next train arrives. Users may also access Google Transit from the New York Metropolitan Transit Authority's website, which also includes Google Translate, to translate the information into 23 different languages. Besides New York City, Google Transit also covers 170 other cities across the globe.

The Google Blog post about Google Transit may be found at
<http://googleblog.blogspot.com/2008/09/nyc-transit-directions-have-arrived.html>

PALIN KEPT PRIVATE E-MAIL ACCOUNT TO CONDUCT STATE BUSINESS

On September 30th, the *Washington Post* announced that Vice Presidential candidate Sarah Palin had another e-mail account that she used for government business, besides the Yahoo account that was hacked on September 17th. Wasilla company ITS Alaska verified that Palin had this separate e-mail account that was only accessible to close confidants and her husband. The e-mail system was created from an old campaign account, and was limited to only 10-15 e-mail addresses on an independently maintained server. The existence of these separate e-mail accounts has an important impact on the so-called "Troopergate" scandal that indicates Palin may have ensured the demotion of a state trooper who divorced her sister. The alternative e-mail accounts raised questions about Palin's ability to keep private affairs and work separate.

The story may be found at
<http://www.washingtonpost.com/wp-dyn/content/article/2008/09/30/AR2008093002699.html>

SENATE AND HOUSE PASS BILLS TO PROTECT CHILDREN ONLINE

On September 25th, the Senate passed the Protect Our Children Act, legislation introduced by Senator Joe Biden (D-DE) intended to help catch and prosecute child predators across the country. The legislation provides for a national strategy to prevent child exploitation, including making sure there is an Internet Crimes Against Children Task Force in each state. The legislation gives \$320.5 million over the next five years to implement the national strategy and task forces, along with increasing forensic capacity at forensic computer labs across the country. On September 23rd, the House of Representatives passed the Ryan Haight Online Pharmacy Consumer Protection Act, a bill that would ban the sale of prescription drugs online without a valid prescription. The bill was named after Ryan Haight, a teen who died of an accidental overdose on prescription drugs he got online. Under the bill, online pharmacies would have to register with their state Attorney General and would have to comply with the pharmacy licensing laws in their particular state. A related bill passed the Senate in April.

The text of the Ryan Haight Act may be found at
<http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.6353:>

The Protect Our Children Act may be found at
<http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.1738:>

RIAA SEEKS SANCTIONS AGAINST ATTORNEY DEFENDING FILE SHARERS

On September 12th, the Recording Industry Association of America filed a motion for sanctions against attorney Ray Beckerman for his alleged misconduct in defending a file sharer in an RIAA lawsuit. The RIAA claimed that Beckerman engaged in obstructionist tactics including making baseless discovery objections and frivolous motions, and then posting all the motions on his blog. The blog allegedly contains misleading statements about the case. The motion further calls Beckerman a “vexatious” litigator who demeans the integrity of the court proceedings. Beckerman is one of a very few attorneys who defends file sharers, and has successfully gotten some cases dismissed.

The motion may be found at

<http://blog.wired.com/27bstroke6/files/vexatious.pdf>

JUDGE AWARDS IOWA ISP \$236 MILLION IN SPAM LAWSUIT

On September 30th, a federal judge in Iowa awarded \$236 million to ISP CIS Internet Services and its owner, Robert Kramer III in its lawsuit against spammers Henry Perez and his wife Suzanne Bartok. The damages were equal to about \$10 per bulk e-mail, which were sent by the couple using a program called “Bulk Mailing 4 Dummies” over a four-month period in 2003. CIS had to undertake an expensive server upgrade and dedicate three servers to blocking spam, a costly venture for a small company. The court found that Kramer proved that the e-mails originated from the couple’s business in Arizona, and were unsolicited advertisements. The ruling was unique because it held the owners of a spam company directly liable for the spam, even though the couple was not hitting the send button themselves. The judgment is the most recent in a series of judgments CIS has won against spammers.

The story from the Iowa newspaper Clinton Herald may be found at

http://www.clintonherald.com/local/local_story_278021410.html

PRESIDENT BUSH SIGNS RULE 502 INTO LAW, WITH EFFECTS ON E-DISCOVERY

On September 19th, President Bush signed Senate Bill 2450 into law, which modified Federal Rule of Evidence 502 on the waiver of attorney-client privilege and work product. A Law.com article sought to point out the key provisions of the new rule and explain the implications for e-discovery. The first key provision limits the scope of waiver of privilege to the amount of information disclosed, as opposed to the prior rule, which also waived undisclosed material on the same subject as the disclosed material. The second key provision protects against inadvertent disclosures, clearing up confusion over when an inadvertent disclosure constituted a waiver. The new rule provides that an inadvertent disclosure is not a waiver if the party took “reasonable steps” to prevent disclosure and correct the error. The Advisory Committee notes explain that the reasonableness requirement is flexible and takes into account the realities of e-discovery, as properly using keywords to search for privileged materials may be considered a reasonable step under the rule.

The Law.com article may be found at

<http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202425101980>

S. 2450 may be found at

<http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.2450:>

SENATE LAUNCHES INVESTIGATION OF BUSH WIRETAPPING

On October 9th, the Senate Select Committee on Intelligence announced that it will look into allegations that the Bush Administration illegally listened to Americans’ telephone conversations. The announcement came after two ex-National Security Agency (NSA) employees came forward and spoke to ABC News. The two former employees, Adrienne Kinne and David Murfee Faulk, announced that as military linguists, they intercepted phone calls of U.S. military officers, U.S. journalists, aid workers, and other people calling the U.S. from overseas. Kinne and Faulk

also indicated that the conversations were recorded even after it was determined they were private. The allegations were given to the NSA with no response. Senator Jay Rockefeller, head of the Senate Intelligence Committee called these allegations “very disturbing” and said it would be looked into.

The ABC News story may be found at
<http://www.abcnews.go.com/print?id=6022108>

CLICKJACKING ATTACKS GIVE HACKERS SURVEILLANCE TOOL

On October 7th, founder and Chief Technology Officer of White Hat Security, Jeremiah Grossman, reported a new type of attack for hackers in his blog. The attack has been named “clickjacking,” and it allows hackers to watch or listen to people who have microphones or webcams on their computers. Clickjacking affects all browsers except something like lynx. It is a fundamental flaw in the way browsers work and actually allows an attacker to take “control” of the links your browser visits when you have landed on a malicious website that has implemented the exploit. Clickjacking makes your browser click on any link, button or other redirection without your knowledge. To prevent the surveillance that could come with clickjacking attacks, Grossman recommended putting tape over a webcam, and disabling microphones and plug ins.

The blog post may be found at
<http://jeremiahgrossman.blogspot.com/2008/10/clickjacking-web-pages-can-see-and-hear.html>

REPORT FINDS THAT DATA MINING TO ID TERRORISTS DOESN'T WORK

On October 7th, the National Research Council released a report indicating that government data mining techniques to identify terrorist suspects do not work. Data mining is the collection of personal information, including phone, medical, travel, and Internet records, to try to establish a pattern of information linked to terrorist activity. The report distinguishes between subject based data mining, which starts with one person and looks for connections, and pattern based data mining, which looks for a pattern that could show illegal activities. According to the report, pattern based data mining has limited usefulness, and should only be used to identify individuals who may warrant a second look. Data mining generally also implicates privacy concerns, so the report recommends that policymakers formulate adequate safeguards, including restrictions on the use of the data and independent oversight. As a solution, the report calls for Congress to look at the effectiveness of the programs and assess the likely privacy concerns.

The NRC press release may be found at
<http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=10072008A>

PALIN E-MAIL HACKER INDICTED

On October 8th, the Department of Justice announced that it had indicted 20-year-old student David Kernell for intentionally accessing Governor Sarah Palin’s e-mail account without authorization. The indictment stated that Kernell accessed Palin’s account by changing the password after answering security questions correctly through Internet research. Kernell then read the contents of the account, made screenshots and posted the screenshots online. Kernell also posted the changed password so others could access the e-mail account. If convicted, Kernell faces up to five years in prison, a \$250,000 fine and three-years of supervised release.

The DOJ press release, with a link to the indictment, may be found at
<http://www.justice.gov/opa/pr/2008/October/08-crm-910.html>

NEW JUDGE GRIMM OPINION ENCOURAGES COOPERATIVE E-DISCOVERY

On October 15th, Chief Magistrate Judge for the District of Maryland Paul Grimm issued his decision in *Mancia v. Mayflower Textile Services*, which encourages collaborative e-discovery between parties through Federal Rule of Civil Procedure 26(g). The rule requires that an attorney of record sign every discovery disclosure, request, response or objection. The signature certifies that the request is reasonable and the disclosure is correct to the best of the attorney's knowledge and was formed after a reasonable inquiry. The case dealt with an employment dispute, and the plaintiffs moved to compel the defendants to respond to their discovery requests. Judge Grimm explained that Rule 26(g) was intended to impose an affirmative duty on counsel to act in a way consistent with the Federal Rules concerning e-discovery. Toward that end, attorneys should conduct discovery that achieves the ends of the litigation but is not unduly burdensome or costly. The rule intended to get rid of discovery requests issued without consideration of costs and objections to discovery without a factual basis. The court determined that the aforementioned requests would be eliminated if attorneys met to discuss these issues in advance, and in the meantime narrowly tailored discovery requests. The court concluded that since defendants did not give any reason for their objection to the discovery, the defendants waived any objection they might have had. Any problems between the parties were to be addressed in a meet and confer order as the court described.

The opinion may be found at

http://www.mdd.uscourts.gov/Opinions/Opinions/Mancia%20v.%20Mayflower_Opinion_10.15.08.pdf

ICANN RELEASES MORE INFORMATION ON NEW DOMAIN NAMES

On October 23rd, the Internet Corporations for Assigned Names and Numbers (ICANN) released a draft applicant guidebook for alternative domain names to “.com.” New domain names could be locations, such as “.nyc” or company brand names like “.disney.” The new system allows domain names to be in other languages, as the currently available 21 domain names are all in English. The new domain names come with a hefty price tag of \$185,000 – used to cover the costs of implementing the new domain name program. The new program also laid out guidelines to protect trademark and copyright owners, and dispute resolution proceedings. There will be two comment periods for the public of 45 days each, so further revision to the guidebook is possible.

The ICANN press release may be found at

<http://www.icann.org/en/announcements/announcement-2-23oct08-en.htm>

COURT ORDERS PROPRIETARY DATA PRODUCED TO COMPETITOR

On March 21st, U.S. Bankruptcy Court for the Middle District of Tennessee ordered a creditor to turn over copies of its billing data containing proprietary information in native format. In the case, the debtor requested copies of the billing data in native format and the creditor filed a motion for a protective order, claiming that it already turned over the information in an alternative format, and turning it over in native format would compromise proprietary data. The court looked at Federal Rule of Civil Procedure 34, which provides that a requesting party may request data compilations and may specify the form of how electronically stored information is produced. The court also relied on Rule 34 because it requires documents to be produced in a readily searchable format if that was how they were normally stored. Here, the debtor requested the information in native format, and the creditor turned over the documents in useless formats that were not searchable. For that reason, the court denied the creditor's motion for a protective order and ordered the billing information produced in native format.

The decision may be found at

http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_NVMS.doc

YAHOO SUES AMERICAN AIRLINES OVER SEARCH TERMS

On October 21st, the Associated Press reported that American Airlines had filed a trademark infringement suit in the Northern District of Texas against Yahoo. The complaint claims that when a person enters the search term “AAdvantage” for American's frequent flier program, the person is directed to competitors who pay Yahoo for the

traffic. American stated that it sued to protect its intellectual property and prevent consumer confusion. American asked for damages, legal costs and fees, and money for a corrective advertising program. This summer, American filed a similar lawsuit against Google and settled out of court. American did not get any damages but Google did correct the problem.

The story may be found at

http://ap.google.com/article/ALeqM5jNnwYhG3yjOMdh9pHB9v151pRu_AD93V3HE00

RESEARCHERS DISCOVER HOW TO RECOVER KEYSTROKES REMOTELY

On October 20th, researchers Martin Vuagnoux and Sylvain Pasini of the Swiss Security and Cryptography Laboratory discovered how to intercept electromagnetic waves emitted by wired keyboards. The researchers recovered the keystrokes from reading the electromagnetic emanation from a test site. The interception worked from about 65 feet away, including through walls. The researchers posted two videos of the attacks. The first video shows how only the keyboard was monitored in the attack. The second video shows the interception through a wall. The researchers concluded that wired keyboards are not safe for transmitting sensitive information.

The explanation and videos may be found at

<http://lasecwww.epfl.ch/keyboard/>

BRITISH MOTORCYCLIST JAILED AFTER POSTING VIDEO ON YOUTUBE

On October 20th, Reuters UK reported that Sandor Ferenci was given twelve weeks in jail for speeding at up to 130 m.p.h. Ferenci performed stunts on his motorcycle including wheelies and skids, and raced on the opposite side of the road around Banbury, Oxfordshire. A friend was videotaping him and the video was put on YouTube. The prosecutor stated that a motorist took down Ferenci's information and turned him in, and that Ferenci asked if the officers were referring to the YouTube video when called at home. The judge found that the maneuvers were "lunatic and grossly irresponsible." Ferenci pled guilty to two counts of dangerous driving, and stated that he was sorry for what he did.

The story may be found at

<http://uk.reuters.com/article/lifestyleMolt/idUKTRE49J4Q620081020>

PUBLIC INTEREST GROUPS ASK YOUTUBE TO ALTER TAKEDOWN PROTOCOL

On October 20th, the Electronic Frontier Foundation (EFF) and other interest groups asked YouTube and broadcast networks to alter their copyright infringement policies for political content. The groups sent a letter asking the networks to stop sending YouTube Digital Millennium Copyright Act (DMCA) notices over clips of news footage in election related videos. The letter claimed that the DMCA notices were stifling a new form of political expression that does not threaten the copyright interests of the organizations. The letter also said that the videos are outside the companies' interest because no one would mistake them for an endorsement of a particular candidate. In a second letter, the groups asked YouTube to modify its takedown policies to more carefully review the videos and re-post the videos if they fall into a fair use category.

The EFF press release may be found at

<http://www.eff.org/press/archives/2008/10/20>

STUDY FINDS MOBILE E-MAIL HAS DETRIMENTAL EFFECTS

On October 21st, Texas based software company Neverfail, Inc. released its Mobile Messaging Marketing Trends report, which found that employees feel pressured to be available 24/7 because of mobile messaging devices. The

study showed that 94 percent of those surveyed said they had responded to a work message while at home, and 80 percent would not leave the device at home while on vacation. This pressure led to e-mail addiction and risky behavior to respond to messages while off the clock, along with poor work-life balance and detrimental effects on health. The survey found that 77 percent of respondents had used the devices while driving a moving car, and 79 percent had responded while in the bathroom. The research also indicated that companies rely on the devices to make time sensitive decisions.

The Neverfail press release may be found at
<http://www.neverfailgroup.com/news/press/2008/q4/67ffad.aspx>

ELECTRONIC VOTING MACHINE RELIABILITY STILL QUESTIONABLE

On October 16th, Common Cause, Verified Voting, and the Brennan Center for Justice at NYU School of Law released a report questioning whether the states are prepared to use electronic voting machines on November 4th. Since it is impossible to tell where voting machines might fail on Election Day, every state should be prepared in case of a failure. The report found that several states were not doing enough to ensure voting accuracy, as ten states received inadequate grades in three out of four categories. Those ten states included the battlegrounds of Colorado and Virginia. Only three states – California, and toss-ups Ohio and Indiana got satisfactory grades in all four categories. Concerns included inadequate backup plans in case of voting machine failure, no requirement for emergency paper ballots, inadequate paper records for recounts, and inadequate provisions for post-election day audits. While the report indicated some shortcomings, generally the results showed improvement from the last presidential election.

The report may be found at
http://www.brennancenter.org/content/resource/is_america_ready_to_vote/

COMING SOON: SPAM ON YOUR MOBILE PHONE

On October 15th, the Georgia Tech Information Security Center researchers issued a report finding that botnet based attacks could hit cell phones in the next few months. Since cell phones are now used as Internet browsers and mobile computers, their propensity for cyber crime has increased. Cell phones are attractive targets because of increasing computing power, their “always on” nature, and the fact that people now trust voice technology since we are used to entering credit cards and social security numbers over the phone. However, there is some encouraging news. The researchers claim that since they are aware of the risks to cell phones, opportunities exist to design security properly. Further, no attacks like this have been detected yet, and the closed nature of cellular networks makes it more difficult for hackers.

The report may be found at
<http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf>

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

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