

{bytes in brief}

LAW AND TECHNOLOGY NEWS MONTHLY

EDITORS: Sharon D. Nelson, Esq. and John W. Simek
ASSOCIATE EDITOR: Jason R. Foltin EDITOR EMERITUS: G. V. Nelson



© 2010 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

Issue 154 - March 2010

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

PHILLY TARGETS FACEBOOK, TWITTER AFTER SNOWBALL FIGHT TURNS UGLY

On February 17th, *CNET News* reported that at least two members of the Philadelphia City Council have considered filing suit against social networking giants - Facebook, Twitter, and MySpace - after a "flashmob" turned violent. Apparently the mayhem began after several individuals sent text messages and other types of mass communication, possibly via Facebook, and resulted in a rampage through the Macy's department store at the Market East mall and a massive snowball fight. In a letter sent to Mayor Michael Nutter, the council members asked permission to pursue the possibility of a lawsuit, contending that social media sites don't do enough to keep tabs on violence that could be organized through the sites' communication channels. While stories like this pop up every once and a while, some have argued that suing Facebook for the isolated incident is like suing the phone company if telephone calls were used to plot a bank robbery; it's not the responsibility of a social network with hundreds of millions of users to monitor conversations between mischievous high schoolers. Moreover, it may just be impossible to actually monitor everything that is said by users. Generally speaking much of the information sent and/or received on Facebook is publicly available, but the site isn't equipped with straightforward search capabilities. Likewise, while Twitter offers optional geotagging as well as a strong search engine, tracking down a specific conversation can be like finding a needle in a haystack. Additionally, lawsuits against the social networking sites might strain pre-existing relationships between federal authorities and the Web sites, which have, for the most part, been very cooperative with authorities and have provided information on registered sex offenders who may be using the sites. For now, it remains to be seen what action, if any, the council members will take and what the potential ramifications may be. More information may be found at

http://www.philly.com/inquirer/breaking/news_breaking/20100217_Police_take_a_hard_line_after_teen_rampage_in_Center_City.html

LEXIS TURNS UP HEAT ON LEGAL RESEARCH COMPETITION TODAY: UNVEILS PARTNERSHIP WITH MICROSOFT

On February 1st, *The ABA Journal* reported on the newest tool for legal researchers: LexisNexis integrated directly into Microsoft Office products. According to Lexis, this partnership will allow users to do legal and general research while working in Microsoft Word, Outlook and SharePoint. Those who have a Lexis subscription will simply have to click on a Lexis tab in the ribbon of utilities to start researching, Shepardizing cases or even gathering information from Bing or Google search engines without ever leaving a Microsoft Office program equipped with this feature. According to information provided during the release of this new product, once the Lexis tab is toggled "on," users can then access a variety of information from Lexis as well as utilize the functions from the new Lexis platform. Some of these new function include the ability to pull results from Lexis' filtered web search function and checking the validity of all the cases in the document simply by clicking the Shepardizing tab. Additionally, users will be able to find information about a person or case or related document by highlighting text, which brings up information stored in a firm's document management system, the user's own computer or, with other clicks, pulled from the Web. But, while the research and information data accessible via Lexis for Microsoft Office offers a world of possibilities, it is not the complete set of data and information available through the traditional Lexis.com website and may, in the future, come with additional charges. Not to be outdone Westlaw, the other big legal research provider, introduced its revamped version of Westlaw, WestlawNext, which features better search results and improved ease of use. What will they think of next? A copy of the story may be found at

http://www.abajournal.com/news/article/lexis_just_a_click_away_in_microsoft_office_programs

WEB SEARCHES FOR IPAD LEADING TO MALICIOUS SITES

On January 28th, *CNET News* warned that consumers and website operators should be wary of iPad related search scams. The problem, which has nothing to do with the iPad itself, has been viewed as an opportunistic attempt to capitalize on the hype that has been generated by the newest Apple creation. In fact, similar techniques have exploited other popular searches such as the Haitian earthquake and the death of Michael Jackson. According to Don Debolt, CA's director of threat research, cybercriminals will likely employ what's called "black hat search optimization" - a scam whereby hackers take advantage of security flaws in blogs and other sites that use PHP to imbed popular search terms like iPad to trick search engines into directing people to compromised legitimate sites that may have nothing to do with the subject matter at hand. If someone clicks on the link to a page on that infected site they are then redirected to a malicious site, which can implant malware on their machine or tempt them to install a rogue security product. Debolt has warned people to be careful if a search engine directs them to a site where the root domain of the URL has no affiliation to the topic or is not an information portal that they are familiar with. Additionally, he cautioned site operators, especially those with a content management system that uses PHP, including Joomla, WordPress and Droopa, to be sure they are using the latest version of their web software. As usual, some of the best advice is also the most overlooked; all Internet users should make sure that they are using up-to-date security software and that both their operating system and browser are up-to-date. A copy of the story may be found at http://news.cnet.com/8301-19518_3-10443931-238.html

CONGRESSIONAL SITES DEFACED AFTER OBAMA SPEECH

On January 27th, hackers defaced the Web pages of nearly 50 members of the U.S. House of Representatives, posting an explicit insult directed at President Obama after he gave his State of the Union address. The websites, representing both Democrats and Republicans, were managed by a company known as GovTrends. A spokesman for the House chief administrative office was quoted as saying that the attack occurred while GovTrends was performing an update. Interestingly, last August, other House sites managed by GovTrends were also defaced, leading some to contend that perhaps it is time to reconsider the business relationship the federal government has with the website service provider. A blog post on the topic may be found at <http://praetorianprefect.com/archives/2010/01/congressional-web-site-defacements-follow-the-state-of-the-union/>

JAMMIE THOMAS REJECTS RIAA'S \$25,000 SETTLEMENT OFFER

On January 27th, attorneys for Jammie Thomas-Rasset, the Minnesota woman who was found liable of willful copyright infringement and ordered by a jury to pay \$1.92 million in damages, rejected RIAA's settlement offer just days after a federal court judge reduced the damage amount to \$54,000. The RIAA informed Thomas-Rasset that it was willing to accept \$25,000 if she agreed to ask the judge to vacate his decision to reduce the overall damage award. According to the RIAA, Thomas-Rasset's decision to refuse the settlement agreement means only one thing; the court fight will go on. In fact, a spokesperson for the RIAA stated that it is a shame that Ms. Thomas-Rasset continues to deny any responsibility for her actions rather than accept a reasonable settlement. However, the decision to refuse the settlement shouldn't come as much of a surprise. Attorneys for Thomas-Rasset had already said that they planned to challenge even the lowered amount set by the court, noting that the only satisfactory result would be a \$0 award. One thing is for certain; this case has and will continue to stir the debate over copyright and illegal file sharing. Look for an appeal, if possible, sometime later this year. A copy of the RIAA's settlement offer may be found at http://www.wired.com/images_blogs/threatlevel/2010/01/riaaletter.pdf

TWEET QUESTIONING LANDLORD'S SERVICE DEEMED NOT ACTIONABLE AS DEFAMATION

On January 20th, Judge Diane Larson dismissed an apartment company's defamation action against one of its tweeting residents with little fanfare, finding that the statement was not actionable as defamation per se. The dispute arose after Amanda Bonnen posted a message to her Twitter account that said: "Who said sleeping in a moldy apartment was bad for you? Horizon realty thinks it's okay." Apparently taking issue with the tweet, Bonnen's landlord Horizon sued her, arguing that Illinois law recognizes, *inter alia*, words that prejudice a party, or impute

lack of ability, in his or her trade, profession, or business as defamation per se. However, according to Bonnen, the tweet did not actually charge the realty company with any lack of ability, nor did it unfairly prejudice the company. As Bonnen saw it, her tweet was no more than her own opinion, and was not presented as fact. Ultimately siding with Bonnen, the court dismissed the company's complaint with prejudice; albeit, there was no reasoning accompanying its decision. In fact, the court did not address context or construction, nor did it weigh in on whether the tweet was fact or opinion. A copy of the complaint may be found at <http://www.chicagonow.com/blogs/chicago-bar-tender/Twitter%20lawsuit.pdf>.

70 PERCENT OF HIRING MANAGERS SAY THEY REJECT JOB APPLICANTS BECAUSE OF INFO THEY FIND ONLINE

On January 28th, a Post Tech blog posting reported on the surprising new results of a Microsoft commissioned survey of 1,200 human relations managers and consumers. According to the results, a striking 70% of hiring managers say they've decided not to hire an applicant because of information they've found online. And while almost all of those surveyed stated that they go online to research candidates to hire and think they are justified in doing so, only 7% of consumers actually believed that recruiters check out potential candidates online in hiring decisions. Also interesting was the fact that over half of the managers surveyed agreed that data on lifestyle, inappropriate written text, and inappropriate photos were types of information that could prompt them to reject a candidate. Perhaps Internet users can take a page out of an attorney's manual and utilize their own version of the "red-face test." If the information posted online would make you blush in front of your parents then maybe, just maybe, you might want to reconsider it. An overview of the survey's findings may be downloaded at <http://www.microsoft.com/privacy/dpd/research.aspx>.

MORE THAN 75,000 COMPUTER SYSTEMS HACKED IN ONE OF LARGEST CYBER ATTACKS, SECURITY FIRM SAYS

On February 18th, *The Washington Post* reported on a massive computer attack, dubbed the Kneber bot, involving more than 75,000 computer systems at nearly 2,500 companies in the United States and around the world. The attack, which began in late 2008 and was discovered just last month, targeted proprietary corporate data, e-mails, credit-card transaction data and login credentials at companies in the health and technology industries. The hackers lured unsuspecting employees to download infected software, or baited them into opening e-mails containing the infected attachments. If the employee fell for the ruse, malicious software embedded in the sites or the e-mails enabled the attackers to commandeer users' computers, scrape them for log-in credentials and passwords - including online banking and social networking sites - and then exploit that data to hack into the systems of other users. Amit Yoran, the chief executive of the security firm NetWitness, explained that the attack's scale demonstrates the increasing sophistication of the cybercriminals involved and has highlighted the inability of the private sector, including industries that would be expected to employ the most sophisticated cyber defenses, to protect itself. As Yoran explained, the traditional security approaches of intrusion-detection systems and anti-virus software are by definition inadequate for these types of sophisticated threats. Those companies affected are reported to have begun to contact security vendors, like NetWitness, in an attempt to mitigate the damages. More information may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/17/AR2010021705816.html>.

TSUNAMI OF SPAM AHEAD AS PHISHERS TARGET FACEBOOK

On January 25th, *FOX News* reported that social network users can expect a veritable tidal wave of spam as cyber criminals are increasingly targeting social networking sites like Facebook and MySpace. Cisco has estimated that, as a result, worldwide spam volumes could rise by 30 to 40% when it is all said and done. One of the more popular scams utilized by spammers are phishing attacks that lure unsuspecting victims to click on links that download malicious software onto their computers to steal personal information including banking details and passwords. Interestingly, just two years ago there were virtually no Facebook phishing messages; however, today, Facebook ranks as the second most phished organization online and, if current trends continue, is on track to take the top spot in 2010. A copy of the story may be found at <http://www.foxnews.com/scitech/2010/01/25/tsunami-spam-ahead-phishers-target>.

OHIO HIGH COURT NARROWLY INTERPRETS ANTI-PORN LAW

On January 27th, *The Associated Press* reported that the Ohio Supreme Court has narrowly interpreted a state law aimed at protecting children from online pornography and predators. In its decision, the court said a 2004 law extending the state's definition of "material harmful to minors" to the Internet is clearly intended to apply only to person-to-person communications - not to generally accessible websites and public chat rooms. Calling the court's ruling a partial victory, a coalition led by the American Booksellers Foundation for Free Expression explained that they were happy that they had succeeded in getting the state to voluntarily limit the effects that state restrictions might have had on Internet content, but remained concerned that many questions remain unanswered as to how it will apply to online content. The group had argued the law could be applied broadly to online material and could erode the constitutional free speech rights of online booksellers, newspaper publishers and video game dealers. The Ohio Supreme Court's legal interpretation now goes back to the 6th Circuit located in Cincinnati, which is considering the larger constitutional question. More information and a link to the decision may be found at <http://www.librarystuff.net/2010/01/27/ohio-high-court-narrowly-interprets-anti-porn-law/>.

TAGGED WINS LAWSUIT AGAINST SPAMMER

On January 29th, *ABC News* reported that Tagged.com, one of the many social networking sites on the Web today, has been awarded over \$200,000 as the result default judgment against Erik Vogeler. Vogeler is the man accused of spamming Tagged members by sending them messages with links to an adult dating website. The suit alleged that the messages sent by Vogeler violated the federal CAN-SPAM Act because they had false and misleading header information. Further, the company argued that Vogeler's actions were calculated to lead Tagged users who received defendant's messages to believe that the emails came from other Tagged users who sought them out for personal and social reasons. Ironically, in a separate lawsuit, Tagged was itself accused of sending e-mail solicitations to people that appeared to come from the individual's friends. Also, last year law enforcement officials in New York and Texas agreed to a \$750,000 settlement with the company after looking into what the enforcement officials called "deceptive e-mail marketing." A Tagged.com blog posting on the topic may be found at <http://blog.tagged.com/?p=259>

STUDY LINKS EXCESSIVE INTERNET USE TO DEPRESSION

On February 3rd, British scientists revealed that a direct relationship existed between the amount of time spent surfing the Internet and the signs of depression; albeit, it is not clear whether the Internet causes depression or whether depressed people are drawn to it. The study analyzed Internet users and depression levels of 1,319 Britons aged between 16 and 51, finding that, of those surveyed, 1.2% were addicted to the Internet. While the number may seem insignificant, it was markedly higher than the incidence of gambling in Britain, which is around 0.6%. That notwithstanding, these Internet addicts were found to spend proportionately more time browsing sexually gratifying websites, online gaming sites, and online communities, as well as having a higher incidence of moderate to severe depression than normal Internet users. And while it is unclear whether depressed people are drawn to the Internet or whether the Internet causes depression, what is clear to many is that, for a small subset of people, excessive use of the Internet could be a warning signal for depressive tendencies. As the study's lead author pointed out, this study reinforces the public speculation that over-engaging in websites that serve to replace normal social function might be linked to psychological disorders like depression and addiction. More information may be found at <http://www.msnbc.msn.com/id/35207840/>

TWITTER REVEALS TORRENT SCAM DETAILS

On February 2nd, Twitter explained to its users why it was forced to reset passwords for many of them. In a blog post by Twitter's director of trust and safety, Del Harvey, the social networking site discovered a widespread phishing attack that stemmed from a scam being run by a torrent website creator and, as such, sought to protect its

users by resetting their passwords. According to the blog post, the company just recently became aware that someone had been building torrent sites and forums requiring a log-in and password. This individual then sold these websites and forums to people interested in starting their own torrent download sites. Unbeknownst to the buyers, these sites were littered with various security flaws, some of which allowed the cybercrook to gain access to the buyers' log-in information for sites like Twitter. Cybercriminals then waited until the forums and websites got popular before entering through one of the security holes to gain access to the username, email address, and password of every person who had signed up. Luckily, Twitter was able to recognize the scam after noticing an abnormally high number of followers for certain accounts. The company has advised its users who have signed up for third-party torrent accounts to change their passwords at those sites and to refrain from using the same password at multiple sites. More helpful hints on safe tweeting may be found at <http://twitter.zendesk.com/forums/10711/entries/76036>.

OFFICER'S FACEBOOK POST DRAWS GUN RIGHTS FIRE

On February 17, *CNET News* reported that Rod Tuason, an East Palo Alto police detective, has learned the hard way the perils of posting a comment on a social networking site. Tuason is alleged to have posted a note on Facebook where he threatened to kill anyone he found openly carrying a handgun, even if that person was carrying it legally. In Tuason's own words, if he had seen someone exercising their right to bear arms, he would have "pulled the AR out and prone them all out! And if one of them made a furtive movement ... 2 weeks off!!!" Tuason's comments have caused some serious outcry, especially from Second Amendment advocacy groups, and even an anti-Tuason Facebook page. Jason Davis, an attorney representing the nonprofit Calguns Foundation, sent a letter to the police department where Tuason works, chastising the comments and, among other things, requesting a formal apology from the East Palo Alto Police Department for the conduct of its own detective regarding on-duty activities. While the Calguns Foundation has yet to receive a response from Davis letter, the East Palo Alto Police Department has begun an internal investigation. Moreover, Captain Carl Estelle was quick to point out that the alleged Facebook comments were not reflective of our department or any policies or procedures. Additionally, Estelle attempted to downplay the post while not defending the words or the officer Tuason, stating that the post was made on a personal Web page that Tuason believed was private and suggested that the screenshot of the post may have been altered in an attempt to make it look worse than it really was. The screenshot of the Facebook post may be found at <http://kevinthomason.blogspot.com/2010/02/local-cop-advocates-shooting-law.html>

EDITOR'S NOTE: PHISHING ATTACKS STEADILY RISE

On February 5th, the Anti-Phishing Working Group (APWG) issued its Phishing Activity Trends Report for the third quarter of 2009 and, boy, is the outlook grim. According to the report, almost every statistic relating to phishing attacks is on the rise. In fact, unique phishing reports submitted to APWG during this period also broke new records, up 5.5 percent from the previous record in September, 2007, reaching 40,621 in August. And while the total number of malware infected computers did decrease slightly, more than 48% of the total samples of scanned computers were infected. What's worse is that these numbers could continue to increase. Today, many phishing e-mails now rival e-mails sent by legitimate businesses and most people will click on anything that appears to have come from someone they trust. However, what most people forget is that it only takes one wrong click for their system to become infected. The United States is the king of phishing, which, in September, hosted 75.76% of all such sites. A distant second was Hong Kong with 6.49 % and rounding out the top three was China, with 3.44% of all phishing sites hosted. The report may be found at http://www.antiphishing.org/reports/apwg_report_Q3_2009.pdf

PRESIDENT OBAMA: COMMITTED TO NET NEUTRALITY, DESPITE ISPS PUSHBACK

On February 1st, President Obama expressed his commitment to net neutrality despite considerable pushback from large Internet service providers (ISPs) who want to extract more money from wealthier customers. According to the President, this scenario runs afoul to the whole spirit of openness that has made the Internet such a powerful engine not only for economic growth but for the generation of ideas and creativity. The President also noted that his pick to chair the Federal Communications Commission, Julius Genachowski, supports his views and is in the process of crafting open-Internet rules that would make carriers treat all content equally - not slowing or speeding or charging more or less for certain traffic that travels over their networks. But the President's remarks don't come without controversy. Comcast, the nation's largest cable and Internet service provider, has sued the agency in a

federal appeals court, asserting, among other things, that the FCC didn't have the authority to rule against it for allegedly blocking traffic from the Web application BitTorrent. Comcast's position has been echoed by other industry representatives, noting that they believe Congress has ultimate authority over broadband Internet services, not the FCC. A video of a Q&A session where the President discusses net neutrality may be found at http://voices.washingtonpost.com/posttech/2010/02/president_obama_reaffirms_comm.html

RULING ON ONLINE TERM PAPERS CITE COPYRIGHT QUESTIONS

On February 1st, *USA Today* reported that a district court judge in Illinois has ordered Rusty Carroll, the owner of the Web-based company R2C2, to stop selling term papers unless he can prove he has permission from the papers' authors. In so ruling, the court found that Carroll and his company had caused continued irreparable harm to the authors of the works posted on the website. While the case does not specifically address whether it's legal to sell or buy term papers, according to Stetson University School of Law Dean Darby Dickerson, the opinion does help the public see some of the sharp and shady practices of at least some of these companies. Lawyers for the authors say they hope the court's decision has a chilling effect on other U.S.-based providers and noted that it will seek compensation for its clients, which could number in the tens of thousands when it is all said and done. And while money is always nice, some Plaintiffs, like Chad Weidner, have explained that they sued in part to send a message to students about plagiarism and academic integrity. Weidner has explained that real research is both time-consuming and difficult. To think that there is some kind of quick fix, be it a paper sold online, a paper borrowed from a peer or creative rewriting of an academic's work, the practices are just unacceptable. Even after the ruling, however, Carroll is not prohibited from offering custom-written papers and he had until mid-February to show that he has complied with the order. Alternatively, Carroll could appeal the decision or develop a proposal to gather electronic signatures from the papers' authors. A copy of the story may be found at http://www.usatoday.com/news/education/2010-02-01-term-papers_N.htm

GOOGLE SLAPPED WITH CLASS-ACTION LAWSUIT OVER BUZZ

On February 17th, Eva Hibnick, a Florida resident, filed a class-action lawsuit against Google, Inc., alleging that the company's new Buzz social networking tool set violates the privacy rights of users. For those in the dark about this new service offered by Google, the Buzz program is Google's venture in the social networking ring and was designed by the company to help make the flood of social posts, pictures and videos easier to weed through and to make it easier for a user to find the information he or she seeks. However, almost immediately after its launch users began expressing concerns about the complexity of the privacy settings. According to the complaint, Google Buzz made private data belonging to Gmail users publicly available without the users' knowledge or authorization. And although the company has made several changes to the program, these modifications have not been viewed as adequately addressing the problem. Furthermore, the complaint contended that even if the modifications had addressed all the problems, the damage was already done; the Buzz program disclosed private user information the moment Google launched the service. For some like Dan Olds, an analyst with The Gabriel Consulting Group, Hibnick's lawsuit comes as no surprise and further stated that he wouldn't be surprised if state and federal regulators got into the act, too. If nothing else, Olds noted that the lawsuit should definitely be a wake-up call for Google to go over Buzz with a magnifying glass and a fine-toothed comb, looking for any other potential problems and try to fix them proactively. Google has yet to comment, noting that it would only do so after it has been served with the lawsuit and had a chance to review the complaint. A copy of the complaint may be found at http://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf

SCHOOL ACCUSED OF OFF-CAMPUS WEBCAM SPYING

On February 18th, *CNET News* reported that a class action lawsuit has been filed against the Lower Merion School District in Pennsylvania, alleging numerous violations including violations of the Fourth Amendment, as well as transgressions of the Electronic Communication Privacy Act, the Computer Fraud Abuse Act, the Stored Communications Act, Section 1983 of the Civil Rights Act, the Pennsylvania Wiretapping and Electronic Surveillance Act, and Pennsylvania common law. These alleged violations stem from the school district's questionable decision to remotely activate the webcam contained in a student's personal laptop computer issued by the school at any time it chooses, and to view and capture whatever images were in front of the webcam. Understandably, the complaint contended that many of the images captured and intercepted may consist of images

of minors, and their parents or friends, in compromising or embarrassing positions, including, but not limited to, in various stages of dress or undress. The Lower Merion School District has since released a statement in which it noted that the ability to remotely access the webcam was to help facilitate the recovery of laptops that have been stolen; however, it was quick to point out that it had disabled that ability soon after the lawsuit was filed. A copy of the complaint may be found at <http://americasright.com/wp-content/uploads/2010/02/robbins17.pdf>

The school issued statement may be found at http://www.lmsd.org/sections/news/default.php?m=0&t=today&p=lmsd_anno&id=1137

FACEBOOK GRIPES PROTECTED BY FREE SPEECH, RULING SAYS

On February 16, *CNN.com* reported that a federal magistrate judge has ruled that a high school student has a constitutional right to criticize a teacher on Facebook. The lawsuit was filed after Katherine Evans was suspended from school for using her home computer to create a Facebook page titled "Ms. Sarah Phelps is the worst teach I've ever met." After learning of the Facebook page, school principal Peter Bayer suspended Evans for three days for disruptive behavior and cyberbullying of a staff member and also removed her from Advanced Placement classes and assigned her to regular classes. However, the court held that Evans had a constitutional right to express her views on the social networking site. More specifically, U.S. Magistrate Barry Garber explained that Evans' speech fell under the wide umbrella of protected speech because it was an opinion of a student about a teacher, that was published off-campus and further, it was not lewd, vulgar, threatening, or advocating illegal or dangerous behavior. In so holding, the court denied a motion to dismiss the case and allowed the lawsuit to move forward. Matthew Bavaro, an attorney with the American Civil Liberties Union who is representing Evans, indicated that he was pleased with the decision, asserting that the First Amendment provides protection for free speech regardless of the forum, being the Internet, the living room or a restaurant. Baravo explained that his client will seek nominal, token damages to show that her rights were violated and simply wants the court to hold the school's suspension invalid and to have documents related to the suspension removed from her school file. As Ryan Calo, an attorney with Stanford Law School's Center for Internet and Society explained, we have constitutional values that will always need to be redefined due to changes in technology and society. A copy of the story may be found at <http://www.cnn.com/2010/TECH/ptech/02/16/facebook.speech.ruling/>

APPEALS COURT LETS GOOGLE STREET VIEW SUIT CONTINUE

On January 29th, *CNET News* reported that the Third Circuit Court of Appeals has reinstated a lawsuit filed by a Pennsylvania couple against Google after a driver for its Street View service took a panoramic photograph of their secluded home. In its opinion, the court ruled that the trial judge correctly dismissed the couple's other claims - that their privacy had been violated, that they should be awarded at least \$25,000 in damages, and that punitive damages were also justified - against the Internet search giant, leaving only the couple's claim based in trespass. However, the court's ruling hinted that the couple's remaining claim may only warrant \$1 in damages unless they can prove that they were actually harmed in the moment the Google driver paused while on their property. In so doing, the court pointed to a 1982 case where a coal company had brought an action against picketing union members for, among other things, trespassing. Quoting the district judge in that case, the court explained that Pennsylvania law provides that when a plaintiff proves a violation of a legally protected interest but fails to prove that any injury or damage resulted only nominal damages may be recovered. So, if the couple wants "real" money, they have to prove they suffered a "real" injury. A copy of the opinion may be found at <http://www.ca3.uscourts.gov/opinarch/092350np.pdf>

OLD SECURITY FLAWS STILL A MAJOR CAUSE OF DATA BREACHES, SAYS REPORT

On February 11th, a recent report issued by TrustWave highlighted how a company's over-emphasis on tackling new and emerging security threats may cause that company to overlook older, but far more frequently exploited vulnerabilities. The report, which was based on an analysis of data gathered from over 1,900 penetration tests and over 200 data breach investigations, showed that major global companies are focusing on the latest vulnerabilities and zero-day threats while overlooking the most common ones. As such, companies continue to be felled by old and supposedly well-understood vulnerabilities rather than by the newest attack tools and methods. In fact, as noted in the report, the top three attacks utilized by hackers to gain initial access to corporate networks in 2009

were via remote access applications, trusted internal network connections and SQL injection attacks, all of which have been well researched and known about for several years. Nicholas Percoco, senior vice president at TrustWave's SpiderLabs research unit, explained that the report highlighted basically two themes: first, there are some very old vulnerabilities present within enterprises and second, attackers are targeting these old flaws to break into enterprises, then using increasingly sophisticated tools to harvest data from companies. TrustWave has also provided several measures companies can take to mitigate the risks posed by the older and often overlooked vulnerabilities. One step is to maintain a complete asset inventory. Another way is to decommission older legacy systems as much as possible. Finally, monitoring third-party relationships is key - in 80% of the cases that TrustWave looked at, third-parties were responsible for introducing vulnerabilities. The report may be found at <https://www.trustwave.com/whitePapers.php> (registration required)

POLICE WANT BACKDOOR TO WEB USERS' PRIVATE DATA

On February 3rd, *CNET News* reported that cybercrime investigators are pushing for the creation of a national Web interface linking police computers with Internet and e-mail providers so that legal requests for documents from these companies can be sent and received electronically. According to a recently released report, 89% of the police officers surveyed stated that they want to be able to exchange legal process requests and responses to legal process through an encrypted, police-only nationwide computer network. Further, 61% percent of those surveyed stated that they had their investigation harmed because data was not retained and only 40% of the officers were satisfied with the timeliness of responses from Internet providers. However, this private Web interface has drawn its share of skeptics, many of whom argue that such a system could raise novel security and privacy concerns. One obstacle facing a nation-wide Web interface for cops is that some of its thousands of users could be infected by viruses and other malware. And once an infected computer is hooked up to a national network, it could leak confidential information about ongoing investigations. Lee Tien, an attorney with the electronic Frontier Foundation, voiced his concern, stating that a police-only Web interface sounds very dangerous. He wonders what is going to stop officers from looking through transactional information for anyone once the system is in place. Some companies already operate a police-only Web interface. For instance, Sprint Nextel operates what it calls the L-Site and even offers a course that will teach individuals how to create and track legal demands through L-site. Excerpts from the survey may be found at <http://politechbot.com/docs/kardasz.police.isp.survey-1.020210.png> and at <http://politechbot.com/docs/kardasz.police.isp.survey-2.020210.png>

WAR GAME REVEALS U.S. LACKS CYBER-CRISIS SKILLS

On February 17th, *The Washington Post* reported that a recent cyber war game has illustrated that the U.S government lacks basic cyber-crisis skills. The simulation, developed by Bipartisan Policy Center, was staged to demonstrate to a complacent public the plausibility of an attack that could, in many ways, be as crippling as the September 11th terrorist attacks. Michael V. Haden, former CIA director and the principal creator of the Cyber Shockwave simulation, also noted that the simulation was designed to tee up specific issues that would be digestible so they would become the building blocks of a broader, more comprehensive cyber strategy. Those who participated had much to say about the results of the game. Former Senator Jamie S. Gorelick, a deputy attorney general under President Bill Clinton, pressed the issue of individual privacy, noting that Americans need to know that they should not expect to have their cellphone and other communications to be private especially if the government is going to have to take aggressive action to tamp down a threat. As such, she recommended that the Obama administration seek legislation for comprehensive authority to deal with a cyber emergency. Other participants debated over how far to go in regulating the private sector, which owns the vast majority of the critical infrastructure that is vulnerable to a cyber attack. Many believe that the private sector is not prepared to defend against a cyber act of war and that the government needs to play a role. And while the surprisingly dismal results might shock and scare some people, former Clinton press secretary Joe Lockhart said that's a good thing. Only then, he said, would Congress act. More information may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2010/02/16/AR2010021605762.html>

Bytes in Brief[®] is a FREE monthly digest of Internet law and technology news delivered to you by e-mail. For members of the legal and business community interested in Internet law and technology developments, *Bytes in Brief* provides a synopsis of related news and links to sources with more expanded coverage. In the time it takes to


drink a cup of coffee, *Bytes in Brief* is designed to make sure you are tracking major developments in this fast moving area.

If staying current in this field is important to you and you find yourself buried under unread magazines, newspapers and journals, *Bytes in Brief* can help you stay in touch without a major outlay of time or expense.

To subscribe, enter your e-mail address into the sign-up box below. It will take you offsite to the *Constant Contact* website, where our opt-in only list is maintained and updated. After you confirm your e-mail address, you will receive an e-mail asking for confirmation that you do wish to become a *Bytes In Brief* subscriber. Once you reply to that e-mail, you will be added to the subscription list.

Subscribe to *Bytes in Brief*!

Email:

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

Copyright © 2010 Sensei Enterprises, Inc. All rights reserved.