

{ 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 155 - APRIL 2010

PLEASE NOTE: The URLs referenced in bytes frequently link to newspapers and other current news sources. These links may fail over time. [Click here to visit Sensei home page at www.senseient.com](http://www.senseient.com)

AG SEEKS AUTHORITY TO ACCESS INTERNET, CELL PHONE RECORDS

On February 22nd, The Salt Lake (UT) Tribune reported that the Utah attorney general has asked for a dramatic expansion of his office power to compel Internet and cell phone providers to turn over the identities of customers suspected of engaging in illegal activity. This request comes after the Utah Legislature approved a bill that permitted prosecutors to issue administrative subpoenas demanding that Internet companies provide certain information about an individual suspected of committing a child sex crime. The proposal would allow a prosecutor, without going to a judge, to demand that an Internet company turn over the name, address and telephone number for the individual using the Internet address at a given time. The prosecutor could also demand the individual's history, including how long they had been a customer and any credit card or bank information used to pay for the account. This new request by the attorney general would, however, allow prosecutors to obtain administrative subpoenas for the investigation of suspected felonies or in the case of cyber stalking or cyber harassment - expanding the subpoena authority dramatically from the current authority for child sex crimes. Some argue that extending the subpoena power might be a good thing, noting that because the state has to go to the FBI in some cases to obtain a subpoena, it can take up to six weeks just to get one. Others, however, aren't so sure. Sean Hullinger, a defense attorney in Salt Lake City, compared the added powers to National Security Letters authorized by the Patriot Act and implored the Utah Legislature to oppose granting a power that could easily be prone to abuse. A copy of the story may be found at http://www.sltrib.com/news/ci_14451150.

FTC WARNS NEARLY 100 FIRMS OF P2P DATA LEAKS

On February 22nd, the Federal Trade Commission (FTC) released a statement regarding a recent FTC investigation during which the agency discovered numerous examples of health-related information, financial records, drivers' licenses and Social Security numbers and other data leaked on P2P networks. In most cases, the leaks were the result of improperly configured peer-to-peer software, which wind up exposing the entire contents of the computer on which it is installed. In conjunction with the statement, the FTC also sent out letters to about 100 companies, informing them that sensitive and confidential data from their networks had been found on publicly available peer-to-peer networks. The letter warned the companies that failure to prevent such information from being shared on these networks could result in a violation of a number of laws enforced by the Commission. The letter went on to say that each of the companies responsible for controlling the use of peer-to-peer software on their networks and on those of their third-party service providers. The FTC also stated that it has opened private investigations against an unspecified number of other companies over data leaks involving confidential customer and employee data. According to Alain Sheer, an attorney with the FTC's Bureau of Consumer Protection, part of the investigation into these firms will be to determine whether they may have violated data privacy laws. And while Sheer emphasized that all that the FTC is doing right now is seeking more information about inadvertent data leaks from companies, some see these investigations as the first step towards a formal complaint being lodged against the companies. If anything, this recent action has highlighted the growing concern over inadvertent leaks on peer-to-peer networks as, over the past few years, the number of reported incidents of sensitive data being leaked has grown tremendously. In fact, such leaks have prompted considerable concern from lawmakers and have resulted in at least two bills being introduced in Congress during the past year. A copy of the FTC press release may be found at <http://www.ftc.gov/opa/2010/02/p2palert.shtm>.

A sample notification letter may be found at <http://www.ftc.gov/os/2010/02/100222sampleletter-b.pdf>.

MICROSOFT OFFERS CLOUD SERVICES FOR THE FEDS

On February 24th, Microsoft launched a special new cloud-computing service called Business Productivity Online Suite Federal aimed at attracting the patronage of the federal government. According to the company, the new service offers higher security standards, including fingerprinting as part of background checks and biometric access control. Additionally, the standard suite has obtained a number of security and privacy certifications that could help make it more attractive to local and state governments. To date, companies like McDonald's and Coca-Cola, as well as the U.K. postal service and more than 500 state and local governments, including the cities of Newark, New Jersey, and Carlsbad, California, have already begun using the software. Microsoft's main competition is none other than the Internet search giant Google, which announced last September that it was planning to launch its own dedicated cloud for government users in 2010. However, Microsoft doesn't seem too worried. In fact, the company has released a statement heralding the superiority of its product, focusing on its belief that it has raised the bar with regard to security and privacy. A statement by Microsoft concerning its new services may be found at <http://www.microsoft.com/Presspass/press/2010/feb10/02-24CIOsummitPR.msp>.

NEW CLASS ACTION LAWSUIT TARGETS YELP

On February 24th, a Long Beach, California, veterinary hospital filed a class action lawsuit against Yelp, a business review site, alleging that it was victimized by Yelp sales representatives who asked for payments in exchange for the removal of negative reviews. According to the complaint, the hospital asked Yelp to remove a false and defamatory review from the Web site; however, the company refused to take down the review and instead, one of Yelp's sales representatives continually contacted the hospital and demanded roughly a \$300 per-month payment in exchange for hiding or removing the negative review. Calling the conduct a classic case of extortion, the hospital noted that the payments were to be made under the guise of advertising contracts. In response to the lawsuit, Yelp has since released a statement stating that the company provides a valuable service to millions of consumers and businesses based on its trusted content. Further, the release contended that the allegations against it are demonstrably false, since many businesses that advertise on Yelp have both negative and positive reviews. Interestingly, this isn't the first time that Yelp has been in the news for similar conduct. An expose in the East Bay Express newspaper early in 2009 reported that several small businesses have claimed Yelp's advertising sales team was removing negative reviews on behalf of paid advertisers. More information may be found at http://news.cnet.com/8301-13577_3-10459197-36.html.

WHY BECOMING A DATA THIEF IS ALL TOO EASY

On February 19th, USA Today explained that it's becoming way too easy for people to steal corporate data. In fact, one firm has estimated that anyone with \$325, average computer skills and a stomach for larceny can amass a treasure trove of corporate data. While current versions of the Zeus hacking tool sell for up to \$10,000, older versions are readily available for free on criminal websites and work just fine for turning an infected computer into a bot and harvesting all of the PC's account logons that are stored in Web browser cookies. Dish out \$25 and a spamming specialist will send out around 250,000 e-mail lures to unsuspecting individuals in the hopes they will click on a corrupted Web link that will infect their computer with your free copy of Zeus. Shell out a few more dollars and you can send spam through Facebook messages and Twitter microblogs. From there, all an individual needs to do is rent an Internet-connected server for \$300 and he or she is now in business and can collect and store all the harvested account logons that his or her bots have captured. It seems that this type of amateur criminal activity appears to be catching on. According to security experts, these types of criminals are getting more widely involved in harvesting data, largely due to the rich and robust markets for valid account logons. Making matters worse, corporations are having a difficult time keeping up. Phil Neray, Vice President of Security Strategy at IBM Guardium subsidiary, explained that most companies don't have the continuous, real-time monitoring in place to detect this type of activity. Instead, many organizations simply focus on defending network perimeters or focus on meeting compliance checklists and forget that the true mission of security is to protect high-value corporate data. A copy of the story may be found at <http://content.usatoday.com/communities/technologylive/post/2010/02/why-becoming-a-hacker-is-all-too-easy/1>.

PENTAGON OKS SOCIAL-MEDIA ACCESS

On February 26th, the Defense Department released a memorandum, which makes it official policy that the agency's nonclassified network will be configured to provide access to Internet-based capabilities across all Defense components, including various combat branches. This move effectively clears the way for employees to use social-networking services and other interactive Web 2.0 applications, although soldiers, sailors, and airmen will still be expected to keep from engaging in any conduct that could compromise military actions or undercut readiness. Further, the Defense Department stated that it will continue to defend against malicious activity on military information networks, deny access to prohibited content sites (e.g., gambling, pornography, hate-crime related activities), and take immediate and commensurate actions, as required, to safeguard missions (e.g., temporarily limiting access to the Internet to preserve operations security or to address bandwidth constraints). The decision to permit access, even if limited in nature, comes in large part due to the Pentagon's recognition that social networks, among other Web capabilities, are useful tools for different agencies to interact with other agencies within the department as well as with the general public. According to David M. Wennergren, Deputy Assistant Secretary of Defense for Information Management and Technology, it's important to look at security and information sharing collectively today and not as two separate subjects. You can focus on having great security, but then you won't have any ability to access information sharing. Or, you can think only about sharing information, but then you run into issues of operational security and letting bad things into your system. A copy of the Defense Department's policies regarding social networking and other Web 2.0 applications may be found at <http://www.defense.gov/NEWS/DTM%2009-026.pdf>.

GOOGLE EXECS CONVICTED IN ITALY FOR DOWN VIDEO


On February 24th, a Milan court convicted three Google executives for violating the privacy of an Italian boy with Down's syndrome after a video of him being bullied was posted to Google Video in 2006. While the executives do not face actual imprisonment as the sentences were suspended, both the public prosecutor and Vivi Down, the Italian advocacy group for people with Down syndrome that brought the suit, were happy with the verdict, with the public prosecutor noting that the sentence sent a clear message that a company's rights cannot prevail over a person's dignity. However, in emphasizing its intention to appeal the sentence, Google called the verdict a threat to Net freedom since none of the three employees found guilty had anything to do with the offending video. In the company's opinion, if employees can be held criminally liable for any video posted on a hosting site, when they had absolutely nothing to do with the video in question, then the liability of those sites is virtually limitless. Censoring of websites has, in recent months, become a hot issue in Italy, especially after hate sites began to pop up against various governmental officials. The government had initially planned to black out Internet hate sites after some of the comments about the sites praised an attack on the Premier, but dropped the idea after top officials from Facebook, Google and Microsoft agreed to a shared code of conduct rather than legislation. A copy of the story may be found at <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>.

COURT REAFFIRMS I4I PATENT WIN AGAINST MICROSOFT

On March 11th, PCWorld.com reported that the U.S. Federal Court of Appeals has once again upheld a jury's verdict that Microsoft willfully infringed on patents awarded to i4i. The verdict required Microsoft to pay more than \$240 million in damages and forced the company to remove a feature in versions of Microsoft Word 2007 that lets people create custom XML documents. This latest decision to reconsider its decision to affirm the district court's ruling is virtually identical to the appeals court's earlier decision in December, except for an expanded explanation of the decision to uphold the willfulness issue. In that particular portion, the court explained that a reasonable jury could have concluded that Microsoft willfully infringed the patent in question, noting that evidence presented at trial demonstrated that Microsoft employees attended demonstrations of i4i software and received i4i sales kits that identified the software as patented technology. Similarly, the court reasoned that nothing indicated that Microsoft ever made a good faith effort to avoid infringement. Rather, internal e-mails showed that Microsoft intended to render i4i product obsolete and assure there wouldn't be a need for i4i product. Microsoft has since requested an en banc review. While there is no set time frame for the court to decide whether it will accept the request, it is expected that the court will decide in the next four to six weeks. If the judges decide against the en banc request, Microsoft can always ask the Supreme Court to hear the case. More information may be found at <http://www.pcpro.co.uk/news/356320/microsoft-loses-again-in-word-patent-suit>.


CLOUD SECURITY SEVEN DEADLY SINS

On March 3rd, PCWorld.com reported that a new study conducted by the Cloud Security Alliance has identified seven types of security risks present in cloud computing that can be exacerbated by both the openness and the scale of cloud services. First on the list is misuse of cloud computing, where the cloud itself is used to host attacks. The report noted that clouds have been infected with various types of malware and, because people can access services with just a credit card, or even a free trial period, criminals are able to spam and spread malware in relative anonymity. To help prevent misuse, the report recommended stricter registration and validation, better credit card fraud detection and data traffic monitoring. Another problem is unsecured APIs, which can contain exploitable loopholes. To combat the problem, the study suggests closer analysis of API security as well as strong authentication, access controls, and encryption. The third threat listed is malicious insiders. While this threat is well known in corporate networks, the problem is further exacerbated with cloud services, as you don't have control over who works at the cloud vendor and what they may be up to. Another area of concern is shared technology. The report explained that in an environment where multiple virtual servers have the same configuration, a single bug or misconfiguration can be replicated across a broad patch of a cloud provider infrastructure. To combat this problem, the report stated that companies should make sure their cloud vendor follows best practices for network and server configuration and should enforce service level agreements for patch management and vulnerability remediation. Another common concern that is magnified in the cloud is data leakage. A sixth concern mentioned in the report is account or service hijacking. If an attacker can hijack a legitimate customer's account, he or she can gain control of that customer's virtual machines. The study recommended two-factor authentication and proactive monitoring to detect unauthorized activity. Finally, the last threat listed in the report is the unknown. As the report noted, Cloud vendors and their customers may think they've covered every possible risk, but something may still happen that they weren't aware of. Many companies don't think through security risks because they don't believe it will happen to them. A copy of the report may be found at <http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>.



BILL TO BAN SOCIAL NETWORKING FOR SEX OFFENDERS

On March 2nd, The San Francisco Chronicle reported that Assemblywoman Norma Torres, D-Pomona (Los Angeles County) had introduced a bill that would make it a crime for any of California 63,000 registered sex offenders to use social networking sites - defined as a website designed with the intent of allowing users to build networks or connect with other people and that provides means for users to connect over the Internet. The proposed bill is similar to legislation passed last year in Illinois, but it is not as expansive as the new state law, which additionally requires sex offenders to register their e-mail addresses and online aliases with state authorities, who can then turn over the names to the companies that run the social networking sites. And while all of the laws depend to some extent on the assumption that sex offenders will police themselves, San Francisco District Attorney Kamala Harris said the proposed law will act as a deterrent to sex offenders who do not want to return to jail and will also create more public awareness about the issue. Facebook attorney Chris Kelly said that the law is a good start, but noted that the legislation will need to be strengthened in order to have a considerable impact. A copy of the story may be found at <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/03/01/BAIN1C98UB.DTL>.



WHEN TWEETS CAN MAKE YOU A JAILBIRD

On March 16th, The Associated Press reported that individuals may have one more reason to watch what they say and do on social networking sites - law enforcement agencies have jumped on the Web 2.0 bandwagon, even going undercover with false online profiles to communicate with suspects and gather private information. According to a recently released internal Justice Department document, U.S. agents have been logging on surreptitiously to exchange messages with suspects, identify a target friends or relatives and browse private information such as postings, personal photographs and video clips. In so doing, these agents have been able to check suspects' alibis by comparing stories told to police with tweets sent at the same time about their whereabouts. Online photos can also be used to link suspects or their friends to a crime. While the Justice Department has applauded these tactics, one potential hurdle facing agencies as they move forward and continue to utilize these undercover practices is the possibility of violating the website's terms of service if an agent is found to have lied about his or her identity. Many websites require that subscribers use their real name. Facebook terms of service require users to agree not to "create an account for anyone other than yourself without permission." At Twitter, "impersonation is against the terms of service." Further, former U.S. cybersecurity prosecutor Marc Zwillinger noted that while he

agreed that investigators should be able to go undercover in the online world, he believes that careful oversight is required so that law enforcement does not use social networking to intrude on an individual's personal relationships. A copy of the Justice Department document may be found at http://www.eff.org/files/filenode/social_network/20100303_crim_socialnetworking.pdf.

SECURITY EXPERT: U.S. WOULD LOSE CYBER WAR

On February 23rd, former U.S. Director of National Intelligence Mike McConnell told the Senate Commerce, Science, and Transportation Committee that the U.S. government, if confronted in a cyber war today, would lose. Further, McConnell also stated his belief that the U.S. won't make many improvements in its cybersecurity until a catastrophic attack forces the government to get involved. These sentiments were also shared by James Lewis, director of the Technology and Public Policy Program at the Center for Strategic and International Studies, who explained that the Internet was designed as a global commons that polices itself, but that model has failed and instead we are left with the Internet version of the Wild West. In his mind, the government shouldn't simply let the market try to fix cybersecurity, it needs to proactively come in and give the market a kick. However, for all those grim and gloomy opinions, there is some light at the end of the tunnel. Senators Jay Rockefeller (D-W.Va.) and Olympia Snowe (R-Me.) have been working on a proposed bill which would create new cybersecurity regulations for private companies designated as critical infrastructure, require a national licensing and certification program for cybersecurity professionals, and, in some versions of the bill, allow the U.S. president to order that parts of the Internet under attack be shut down. Yet, even with this proposed legislation, some believe that this bill alone is not enough. According to Mary Ann Davidson, chief security officer at Oracle, U.S. technology users and policymakers need to stop tying more and more systems to the Internet. Davidson believes that the government should stop making cybersecurity worse by rushing to use technology in ways that it knows it cannot completely secure. As an example, Davidson pointed to the U.S. electrical system and the possible implementation of SCADA (supervisory control and data acquisition) systems, which would allow individuals to turn systems on and off through a smartphone. She believes that it won't be long until there's an app for moving control rods in and out of a reactor. And there might come a day, she says, when we have a power plant meltdown when all someone was trying to do is answer the phone. A copy of the story may be found at <http://www.infoworld.com/d/security-central/security-expert-us-would-lose-cyber-war-730>.

CHATROULETTE IS 'PREDATOR PARADISE,' EXPERTS SAY

On March 1st, Fox News reported on the many dangers that stem from Chatroulette, a new website that connects videochatters with a limitless number of random strangers from around the globe. The site, which launched late last year, has become an overnight Internet sensation, attracting tens of thousands of videochatters at a time. However, a large number of these members have a tendency to expose themselves while online, or to entice others to do so - a fact that is raising some red flags with police and child protection advocates. Further, legal experts have noted that although users of the site must confirm that they are at least 16 years old and that they agree not to broadcast obscene, offending or pornographic materials, these barriers can be easily bypassed and can connect children with sexual predators and child molesters. Making matters worse, police and other law enforcement officials have found their hands are tied when dealing with the site's inherent dangers. One problem is that the Communications Decency Act of 1996 may exempt civil liability for Chatroulette itself, because the law has been interpreted to imply that operators of Internet services are not publishers, and therefore not legally liable for the content of third-party users. Thus, authorities would be forced to go after individuals who expose themselves while using the site - something easier said than done. The question then becomes one of whether local police are going to have the resources to chase after someone who could be a continent away. And even though a prosecutor would theoretically have sufficient basis to start an investigation based solely on an offending broadcast shown in his or her jurisdiction, getting a copy of that broadcast could be virtually impossible unless the images and messages are being archived by the site's providers. For now at least, Chatroulette appears to be here to stay and there isn't very much anyone can do about it. More information may be found at <http://www.foxnews.com/scitech/2010/03/01/chatroulette-chock-legal-questions-attorneys-say/>.

DATA BREACHES ARE HEAVIEST AT HOTELS

In a recent report, Spiderlabs, a unit of data-security firm Trustwave, highlighted a recent trend in data theft: hackers are now stealing credit-card data from hotels more often than any other industry. In fact, according to the study, 38% of the company's data-breach investigations of 2009 occurred at hotels compared to only 19% for

financial service providers. What's worse, it took an average of 156 days for the business to realize that a breach had occurred. The most common weakness exploited by these cyber criminals is the security surrounding point-of-sale software-the software hotels use to process credit-card transactions. For example, often the systems are maintained remotely by an outsourced information-technology company. To maintain the computer system, the IT firm employees must sign in remotely. When remote access user names and passwords are left blank or not changed from their default setting, hackers can find those usernames and passwords to gain access to the system to steal credit-card information. And while there is little customers can do to protect themselves besides checking their credit-card statements carefully, both Trustwave and security firm Verizon Business recommend that businesses follow data-security standards established by the PCI Security Standards Council. A Verizon spokesperson explained that the company has never run an investigation of a successful data breach where a merchant was PCIDSS compliant. More information may be found at <http://online.wsj.com/article/SB10001424052748704743404575127674094249164.html>.

MYSPACE USER DATA FOR SALE

On March 17th, PCWorld.com reported that information from MySpace customers is now being sold to third parties ranging from academics and analysts to marketers. The information being sold includes any activity or information that is attached to an account - basically all blog posts, location, photos, and status updates, among other data. Because MySpace legally owns the data and server logs, the company is perfectly within its rights to work with Infoclimps, the Austin Texas company contracted to sell the data. Basically, users have waived their rights to privacy in exchange for free Web hosting and access to its social features. A copy of the story may be found at <http://www.digitaltrends.com/computing/myspace-offers-user-data-for-sale/>.

STUDENT FILES PETITION TO PRESERVE EVIDENCE IN WEBCAM SPYING CASE

On February 22nd, Blake Robbins, the student who accused his suburban Philadelphia school district of spying on him and other students via their school-issued webcams, filed an emergency petition in court requesting district officials not to remove any potential evidence from student computers. The petition comes after Robbins filed suit against the school for allegedly taking a picture of him in the confines of his home. The American Civil Liberties Union has backed up the student's allegations, arguing that the photo amounted to an illegal search. Both the FBI and local authorities have begun to investigate the claims to determine whether the district broke any wiretap, computer-use or other laws. In the wake of the outcry over the alleged misconduct, school district officials have stated that they have abandoned the practice of activating the webcams, but Robbins' attorney, in filing the emergency petition, has explained that he wanted to make sure the school does not remove any information or programs from the 2,300 laptops issued to students at its two high schools. In the petition, he claimed that the Defendants intend to reclaim each laptop from the possession of members of the class for the purpose of wiping clean the hard drive or otherwise engaging in the spoliation of evidence. In response, counsel for the district has urged families and community members not to jump to conclusions and noted that the district will make recommendations for any needed changes in policies and procedures if any mistakes are found to have occurred. A copy of the story may be found at http://www.siliconvalley.com/ci_14449371?nclick_check=1.

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 <i>Bytes in Brief!</i>	
Email: <input type="text"/>	<input type="button" value="Go"/>

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

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