

{ 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 158 - July 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)

WHAT SITES SUCH AS FACEBOOK AND GOOGLE KNOW AND WHOM THEY TELL

On May 29th, The Washington Post reported on the startling issue of just what your social-networking sites know about their users and with whom they share that information. In fact, many online service providers over the past few years have been building huge dossiers with minute details of each user's online activities - a practice that isn't usually mentioned in privacy policies. Some companies anonymize the data, while others do not. Some store detailed data for a month, while others keep it for years. Moreover, internal compliance manuals for law enforcement for Facebook, Yahoo, and Microsoft show that these companies have data collections much more extensive than users might believe based on what they themselves can access. For example: Microsoft tracks the Xbox LIVE start and end dates and times for game-playing and notes the game played, Yahoo keeps chat and instant messenger logs for 45 to 60 days and finally, for every user ID, Facebook keeps a log of the IP address that accessed the account, the date and time, and what exactly the user did. At the same time, the ease with which outsiders can access the data is increasing, as corporations, insurance companies and parties in divorces or employment disputes make widespread use of subpoenas. And according to some attorneys, such subpoenas have become standard practice in litigation and are meant to discover information that would be embarrassing or might be used adversely even if it has nothing to do with the claim. Worse yet, because your account information is stored on a company's servers, on the "cloud" that is the Internet rather than on your personal laptop, the company owns the right to share it, not you. While accessing your laptop may require a difficult-to-obtain search warrant, getting certain data on Facebook, MySpace, Meetup, LinkedIn and other social-networking sites' servers may require only a simple subpoena. Content is often protected under the Electronic Communications Privacy Act, but the time of connection, originating IP address, etc. will not generally be protected. Efforts to give consumers more control over their private information recently have accelerated. In Washington, representative Conyers Jr. (D-Mich.), chairman of the House Judiciary Committee, wrote to Facebook and Google demanding that the Internet giants cooperate with congressional investigators looking into privacy practices. Facebook has recently come under fire over privacy policy changes while Google has drawn scrutiny for accessing information including e-mails and surfing from open Wi-Fi networks while photographing streets for its mapping service. And companies have also responded as well. In an effort to improve transparency about how it handles private data, Google launched a new tool revealing how many requests it gets from different governments around the world. Additionally, four New York University students recently designed a software program called Diasposa, which they say will allow users to keep control over their social-networking information. More information may be found at http://www.washingtonpost.com/wp-dyn/content/article/2010/05/28/AR2010052804853_pf.html

FTC CRACKS DOWN ON SPYWARE SELLER

On June 3rd, ComputerWorld.com reported that the U.S. Federal Trade Commission has reached a settlement with spyware vendor CyberSpy Software, two years after suing the company for selling allegedly undetectable keylogging software. According to the settlement agreement Cyberspy is permitted to sell its RemoteSpy software, but the company must take steps to prevent it from being misused or advertised as a tool for spying on someone else's computer. More specifically, to prevent its program from being used illegally, CyberSpy must make changes to it to prevent surreptitious installation and encrypt data transmitted over the Internet, police their affiliates to ensure they comply with the order, and remove legacy versions of the software from computers. Previously, CyberSpy had advertised its product as a tool that permitted users to secretly and covertly monitor

and record computers without the need for physical access and, additionally, had provided detailed instructions on how to attach a RemoteSpy executable file to an e-mail message, disguised as a photo or legitimate file attachment. Spyware such as this can be a big headache for system administrators. For instance, in March, a surgical assistant, Scott Graham, was sentenced to three years probation and ordered to pay \$33,000 in restitution to an Akron, Ohio, hospital after a spyware program that he'd sent to an employee's Yahoo e-mail address was inadvertently installed on a computer in Akron Children's Hospital's pediatric cardiac surgery department. The spyware product, called SpyAgent, captured about 1,000 screen shots containing confidential patient information and sent them to Graham. All documents related to the case may be found and downloaded at <http://www.ftc.gov/os/caselist/0823160/index.shtm>.

SOCIAL NETWORKING HEATS UP ON BROWSING PHONES

On June 2nd, a new study released by ComScore reported that more and more individuals are using their cell phone minutes to access social networks. In fact, the study pegs social networking as the fastest growing activity among people with smart phones and other advanced phones that offer Web browsing. Among the nearly 73 million who used mobile browsers, 30 million jumped onto social networks through the browser - a 90% increase from the previous year. With 20 % of mobile users now accessing social networking sites via their phone, ComScore's senior vice president Mark Donovan said his company expects to see both application and browser usage continuing to drive future consumption of social media. Another popular activity is accessing a user's bank account from a smart phone. ComScore noted that almost 5 million people banked online through a dedicated app and 13.2 million via mobile browser. Finally, it seems that cell phone users like news and sports too. 9.3 million of them used dedicated news apps and 26 million cell phone users accessed news via a browser. And about 7.7 million played with sports information apps and 21.5 million tracked sports via a browser. Further information is available at <http://www.mobilemarketingwatch.com/comscore-publishes-report-on-fastest-growing-mobile-app-and-browser-content-categories-7178/>.

FACEBOOK CEO ANNOUNCES REVAMPED PRIVACY SETTINGS

On May 27th, Facebook founder and chief executive Mark Zuckerberg presented new one-click options designed to help subscribers protect their privacy. These new privacy settings come in response to a torrent of complaints from users. The most recent wave of criticism of Facebook began in December, when users were caught off guard with new tools that they found confusing and, in some cases, made user information more broadly available to other websites and anyone searching the Internet. The changes, which will be introduced over the next few weeks, mean that a single click will allow users to block any third-party sites from tapping into their Facebook data. A similar one-click option will allow users to stop applications on Facebook from tapping into their information unless told otherwise. And reversing a confusing feature introduced in December, users will be presented with simpler options on who gets to see information. Further, instead of being forced to customize every status update, users can put information such as employment history and vacation videos into "buckets" designated either for friends, friends of friends or everyone on the Internet. These new changes come amid growing scrutiny from U.S. and European regulators over the privacy practices of Internet giants such as Google and Facebook. For instance, the European Union told Google, Yahoo, and Microsoft that their search engines failed to comply with European privacy laws and told them to prove that they are making user information anonymous. U.S. lawmakers sent a letter to Google's CEO asking how the company scooped up personal information from WiFi residential networks through its mapping program Street View. A blog post written by Zuckerberg may be found at <http://blog.facebook.com/blog.php?post=391922327130>.

IPHONE 3GS FLAW LEAVES DATA VULNERABLE

On May 28th, PCWorld.com reported that the iPhone isn't nearly as secure as you may think, even if you are using a four-digit PIN to lock your phone. According to security and IT blogger Bernd Marienfeldt, he was able, with the help of security expert Jim Herberck, to exploit a "data protection vulnerability" on at least three non-jailbroken iPhone 3GS handsets with different iPhone OS versions installed. Apparently, by plugging an up-to-date, non-jail-broken, PIN-protected iPhone (powered off) into a computer running Ubuntu Lucid Lynx allows anyone to see practically all of the user's data - all the while leaving no trace that the incursion occurred. And while the hacker can access all of the data stored on the phone but not make any phone calls, Marienfeldt warned that the access could also lead into triggering a buffer overflow. If this occurred, it could allow full write access, and full write access could potentially allow the attacker to make phone calls. This is especially disheartening for corporate and

business users, who often expect that all the information stored on their iPhone is protected by encryption with a passcode based authentication in place to unlock it. Even worse, AT&T has stated that it generates almost half of its revenue from business customers and that a principal reason for this is because of the iPhone's "awesome" security. More information may be found at http://www.pcworld.com/article/197419/iphone_security_flaw_using_a_pin_wont_help_you.html.

YAHOO TO TURN SUBSCRIBERS' E-MAIL CONTACT LISTS INTO SOCIAL NETWORKING BASE

On June 1st, Yahoo announced that it will be throwing its name into the social networking foray by using its population of e-mail subscribers as a base for sharing information on the Web. Once operational, the 280 million Yahoo e-mail users will be able to exchange comments, pictures, and news articles with others in their address books. While the program won't be quite as expansive as Google's social networking application, Buzz, unless a user proactively opts out of the program, those Yahoo e-mail subscribers will automatically be part of a sweeping rollout of features that will incorporate the kinds of sharing done on sites such as Facebook and MySpace. Interestingly, the Yahoo social networking move comes amid growing concern by federal lawmakers and regulators over how companies such as Facebook, Google and Microsoft have handled the privacy of Internet users. To allay such concerns, Yahoo said it would give users a week's notice before launching the new features and provide a single button on the site for opting out entirely. Further, the company explained that it will launch a product called Yahoo Updates that allows e-mail users to see what other contacts on their lists are commenting about or sharing on sites like Yahoo Finance, Facebook and the photo sharing site Flickr. Updates will initially include 15 sites and partnerships and will eventually expand to include partners such as Twitter this summer. Yahoo's move has been viewed as a revamping of the once-rudderless Internet pioneer. New CEO Carol Bartz has stripped the company of unprofitable business units to focus on its greatest strengths - its popular free e-mail and messaging programs, and its library of sports, news and finance sites - to keep users in the Yahoo universe longer. As we all know, the longer a user stays on the site, the more advertising dollars and e-commerce it generates. More information may be found at www.washingtonpost.com/wp-dyn/content/article/2010/06/01/AR2010060100577.html.

ATTORNEYS GENERAL FROM 30 STATES DISCUSS JOINT ACTION AGAINST GOOGLE FOR STREET VIEW SNAFU

On June 15th, The New York Times reported that attorneys general from about 30 states have discussed joining forces via conference call in the investigation into whether Google violated any laws when vehicles used by the company to snap pictures for the Street View service also collected snippets of personal information sent over unsecured wireless networks. The call was spearheaded by Richard Blumenthal, Connecticut's attorney general, who was one of the first to open an investigation into the data gathering by Google. According to Mr. Blumenthal, the group conference call was the first step in an effort to cooperate in a possible joint investigation and action. For those unfamiliar with the underlying issue, Google revealed in May that it had collected private data like e-mails and other communications from unsecured wireless networks. Since then, the company has faced a wide array of civil and criminal investigations from various European countries as well as Australia. In the United States, the matter has been the subject of Congressional inquiries and class action lawsuits in various states. Google has thus far declined to comment on individual investigations or lawsuits. The company has repeated earlier statements that its collection of data from Wi-Fi networks was a mistake but not illegal. The New York blog posting may be found at <http://bits.blogs.nytimes.com/2010/06/15/states-discussing-joint-investigation-of-googles-wi-fi-data-collection/>.

FACEBOOK FOR BIGLAW? BELIEVE IT

On May 11th, Green Target released a survey that highlighted the fact that in-house counsel are not only using social media and reading blogs, but they are also trusting them for their news. More specifically, the survey notes that 37% of in-house counsel ages 30-39 used Facebook for professional reasons during the day and 28% of all in-house counsel for companies ranging from \$1-10 billion in revenue used Facebook for professional reasons in the last 24 hours. So what exactly does this mean? To some, it means that what law firms think about Facebook is wrong; Biglaw needs to start paying attention to Facebook, not because that is where in-house counsel is headed, but because that is where they are spending their time now. But, as of March 2010, only 31 firms from

the AmLaw 100 had Facebook pages. However, due to an agreement between Facebook and Wikipedia if your firm has a Wikipedia entry, it also has a Facebook page. Facebook will pull information from the firm's Wikipedia page to populate the firm's community page whether you like it or not. LinkedIn also takes a similar stance, populating the company page with information entered by the past and present employees. While firms might not turn their focus to Facebook immediately, this survey's findings is definitely shaking up the legal world. More information, including a summary of the report may be found at http://greentarget.net/newsandthoughts/news/newsitem_54/tabid/579/Default.aspx.

THE TOP FIVE SOCIAL MEDIA RISKS FOR BUSINESSES

On June 8th, IT governance group ISACA released a report which ranked the top five risks social media poses to companies. The top three include viruses and malware, brand hijacking, and lack of control over corporate content. Rounding out the top five are unrealistic expectations of customer service at "Internet-speed" and non-compliance with record-management regulations. John Pironti, an ISACA Certification Committee member, explained that most of the risks simply stem from users not understanding how their own behavior can impact their company. With social media, there are so many platforms and environments to learn. People don't think of the damage that could occur to an organization but rather, they see it as a way to explore relationships with work people. In the end, Pironti stated that it comes down to a need for organizations to educate users about how posting something could breach company security, hurt the company's image, or even open the company up to being hit by malware. Workers need to understand the line between social and business. They also need to have set corporate guidelines about what information can be shared and what needs to stay inside corporate walls. Additionally, company executives need to be aware themselves that workers are using social networking sites and tools so they need to have a hand in it to better protect themselves. Executives can't be aware of what is being said about a company unless someone is paying attention. The research paper titled Social Media: Business Benefits and Security, Governance and Assurance Perspectives may be downloaded from <http://www.isaca.org/Knowledge-Center/Research/Pages/Featured-Deliverables.aspx#socialmedia>.

MOBILE PHONE SECURITY DOS AND DON'TS

On June 8th, NetworkWorld.com reported that as the popularity of smartphones skyrockets, so too do the headaches associated with them. As a result, some experts on securing mobile phones have compiled an extensive list of the dos and don'ts on securing mobile phones. A few of the more interesting ones include:

DO:

- Evaluate the products for security/performance features that fit your market and that will integrate well with existing infrastructure.
- No unmanaged mobile devices - central management is a mandate. Unmanaged devices should not have access to corporate data
- Create specific security policy and procedure items for mobile devices that govern acceptable use, responsibilities (e.g. what to do if device is lost or stolen), etc.
- Solicit info from similar companies who have already implemented what you are looking to implement.
- Try to expand your corporate phone system to your smart devices. There are soft clients that expand into mobile devices seamlessly so that all voicemails/extensions/DIDs do work on your smartphones. Again do not get overexcited. This expansion will carry over your existing security to mobile devices.

DON'T:

- Deploy devices for enterprise use without proper protections and control. The loss of proprietary information can be very costly to the business.
- Block all third-party applications. Have a process to approve applications. Create a whitelist for approved applications. 'Blocking' is not the keyword, the keyword is 'controlling'.
- Do not allow unmanaged devices to access and retrieve classified data (and if you do not have data classification, please do). The data on the unmanaged devices should be treated as lost (they will be). If you allow unmanaged device access make sure that you manage the risk.
- Do not make these devices more slow or more complicated for end users, your projects will be terminated regardless of the security merits.

- Do not allow every single carrier. Try to standardize end point device types and the carrier.

While the list is in by no means exhaustive, it's a good first step. More helpful dos and don'ts may be found at <http://www.networkworld.com/news/2010/060810-mobile-phone-security-dos-and.html>.

FACEBOOK AND NATIONAL PTA JOIN FORCES ON ONLINE CHILD SAFETY

On June 10th, The Los Angeles Times reported that Facebook has teamed up with the National PTA to spread information to kids, parents and teachers about how to responsibly and safely use the Internet. The two organizations have explained that the partnership's aim is to reduce cyberbullying and other risks to children online, two hot topics that have captured the attention of parents, lawmakers and regulators in recent years. To help achieve this goal, Facebook and the National PTA said they would provide information and other resources through their respective websites and through the PTA's 24,000 local chapters. In conjunction with this collaboration, Congress also is in the process of examining the Child Online Privacy Protection Act, or COPPA. Other agencies, such as the Federal Trade Commission and Department of Justice, are reviewing online safety and privacy for children. In the end, it seems that parents spoke and a variety of organizations and governmental agencies listened. A Yahoo survey conducted in April found that 78% of parents are concerned about their children's online safety, with 70% talking to their children two to three times a year about it and 45% talking to their children about it at least once a month. More information may be found at <http://latimesblogs.latimes.com/technology/2010/06/facebook-and-national-pta-join-forces-on-online-child-safety.html>.

JUDGE LIMITS DHS LAPTOP BORDER SEARCHES

On June 2nd, a federal judge ruled that border agents cannot seize a traveler's laptop, keep it locked up for months, and examine it for contraband files without a warrant half a year later. The government had invoked a novel argument, stating that while Andrew Hanson, the unlucky traveler, was able to enter the county, his laptop, because it never cleared customs and was maintained in government custody until it was searched, remained in a kind of legal limbo where the Bill of Rights did not apply. Customs agents have said that after the individual was randomly selected for a secondary baggage examination, he became nervous. That led the customs agent to ask for an examination of Hanson's laptop, a digital camera with memory card, two CD-ROMs, and two DVDs. For his part, Eric Chase, an attorney representing Hanson, acknowledged that an immediate search conducted at the border without a warrant was permissible. But police perusal of a hard drive six months later definitely is not, he argued when he asked the court to toss out the results of the June 2009 search. Chase further went on to contend that as applied to border searches generally, agents, after taking their permissible look while at the border crossing itself, would be free to detain electronic devices and conduct further examinations whenever and wherever they pleased as justified solely because their peek exposed the computer's contents to law enforcement. This is not exactly a new dispute. In fact, just two years ago, the U.S. Department of Homeland Security's Customs and Border Protection announced that it reserved the right to seize for an indefinite period of time any laptops that are taken across the border. And last year, the department reiterated that claim, further asserting that laptops and electronic gadgetry can still be seized and held indefinitely. In response to these assertions, Senator Russ Feingold (D-WI) introduced a bill that would require border agents to obtain a warrant or court order to hold such a device for more than 24 hours. More information, including an excerpt from the court's decision, may be found at http://news.cnet.com/8301-13578_3-20007315-38.html?tag=contentMain;contentBody.

'SHADY' PORN SITE PRACTICES PUT VISITORS AT RISK

On June 14th, The Huffington Post reported that a recent study led by International Secure System Lab revealed what many have already concluded: Porn sites are dirty! But here dirty means that visitors frequenting these sites are at serious risk of being exploited by cyber criminals. More specifically, the study found that many of these sites harbored malware or used "shady" practices to squeeze money out of their visitors. The researchers found that, of the 269,000 Web sites hosted on the 35,000 pornographic domains, about 3.23% of these Web sites were booby-trapped with adware, spyware, and viruses. Further, many other sites used so-called "shady" practices to keep visitors onsite. For instance, some sites included javascript catchers that made it hard for people to leave a page while others use scripts that re-direct visitors so when they click on a link they do not see the video or image they were expecting but are passed to an affiliate site. What's worse, with many porn sites appearing in the top 100 most popular sites on the web, huge numbers of people could be falling prey to cyber

criminals when they browse for adult content. The study concluded by recommending that anyone visiting porn sites keep their security software up to date and use the "safe browsing" modes found in many browsing programs. A copy of the story may be found at http://www.huffingtonpost.com/2010/06/14/porn-site-practices-put-v_n_610486.html.

CITY OF ONTARIO V. QUON: SUPREME COURT UPHOLDS SEARCH OF EMPLOYEES TEXT MESSAGES

On June 17th, the U.S. Supreme Court issued its opinion in *City of Ontario v. Quon*, a case addressing whether a government employer's search through an employee's text messages, sent and received on a work-issued pager, violated the Fourth Amendment. The Court, in reversing the Ninth Circuit, held that the search was reasonable and that the employee's Fourth Amendment rights were not violated. The case arose after Quon, a police officer for the City of Ontario, was allegedly disciplined after the City discovered many personal, and often sexually explicit, text messages were sent from his work-issued pager. The text messages were discovered after the City launched an investigation into why Quon and other officers had repeatedly exceeded the 25,000 monthly character limit. The City argued that the investigation was not motivated to uncover any wrongdoing, but rather to determine whether the overages were due to personal use. Quon disagreed, and he and those with whom he had been communicating sued the city, alleging their Fourth Amendment rights had been violated. The District Court held that Quon had a reasonable expectation of privacy as to the text messages but that, given the motivation of the search there had been no violation of the Fourth Amendment. The Ninth Circuit reversed in part and held that the search was not reasonable in scope and thus violated the Fourth Amendment. The Supreme Court, in crafting its decision, relied heavily on *O'Connor v. Ortega*, 480 U. S. 709 (1987), a case that addressed the application of the Fourth Amendment when the Government acts in its capacity as an employer. There, the four justice plurality concluded that the court should undertake a two step analysis: 1) determining the applicability of the Fourth Amendment based on operational realities of the workplace and 2) applying the standard of reasonableness under all the circumstances to the employer's intrusion on that expectation for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct. Deciding that it was better to dispose of this particular case on narrow grounds, the Court assumed that Quon had a reasonable expectation of privacy in the text messages sent on the pager, that the city's review of the messages constituted a search within the meaning of the Fourth Amendment, and that the principles applicable to a government employer's search of an employee's physical office apply with at least the same force when an employer intrudes on the employee's privacy in the electronic sphere. Applying the test articulated by the *O'Connor* plurality, the court held that the search was justified because there were reasonable grounds for suspecting that the search was necessary for a noninvestigatory work-related purpose - namely to determine the sufficiency of the character limit on text messages. The Court further held that the scope of the search was reasonable because it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or "personal use" and because the review was not excessively intrusive. Accordingly, the search did not violate Quon's Fourth Amendment rights. Additionally, the Court also held the rights of those with whom Quon was communicating were not violated. A copy of the court's decision may be found at <http://www.law.cornell.edu/supct/html/08-1332.ZS.html>.

APPLE STIRS PRIVACY ROW WITH IOS 4 POLICY

On June 22nd, InfoWorld.com reported that Apple may be about to get roped into the privacy policy debate that has dogged other technology companies like Facebook and Google. More specifically, Apple has decided to change its privacy policy as part of the iOS 4 update to allow the company to collect and share your Apple's device location information. The company has, however, stated that most location data is collected anonymously with the exception of services like Find My iPhone, which needs your personal information to work. Under the new iOS 4, Apple has added new controls for location services that help you understand how your location data is being used. As was the case with iPhone OS 3, whenever an iPhone application wants to use your location data you must explicitly authorize it do so. In iOS 4, after that first-time authorization, a small arrow appears on the top right of your iPhone screen every time your location information is being accessed by an application. Additionally, Apple provides users with granular control over which apps can use your location data in a new panel under Settings>General>Location Services. You can either turn off all location services or you can choose to block individual apps from using your location data. Overall, it appears that Apple has done a fairly thorough job in ensuring consumers are able to control their location data; however, there still are some critics of the new policy. For instance, Apple does not specify whether or not it will track an iPhone's location even with the Location

Services global control turned off. Further, it is also not clear how long Apple intends to store your location data and what kind of safeguards it has in place to protect its database of location information. For now, cell phone location data appears to become the next major privacy battlefield for civil rights advocates. More information may be found at http://www.pcworld.com/article/199497/apple_headed_for_privacy_row_with_ios_4_update.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 <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.