

{ 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 157 - JUNE 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)

THE DIGITAL UNIVERSE IS BIG! 1.2 ZETTABYTES

On May 12th, research and consulting firm IDC estimated that the Digital Universe, meaning every electronically stored piece of data or file out there, will reach 1.2 million petabytes, or 1.2 zettabytes, this year. Despite an economic slowdown, this is a 62 percent increase, up from 800,000 petabytes, from 2009. Interestingly, the IDC reported that most of this content is not unique; in fact, nearly 75 percent of it is a copy of another piece of electronic information. Yet, no matter what, IDC noted that this is only the beginning of a data explosion. By 2020, it is estimated that the amount of data will have grown 44-fold, to 35 trillion gigabytes. In addition, by 2020, at least 15% of the Digital Universe is expected to be managed or stored in the cloud - that is, created in the cloud, delivered to the cloud, stored and manipulated in the cloud. However, as the amount of data available electronically increases, so too does the need for added security. The IDC report cautioned that by 2020 almost 50 percent of the information in the Digital Universe will require a level of IT-based security beyond a baseline level of virus protection and physical protection. Ending on a bit of good news, IDC explained that it believes that staffing and investment needed to manage the evolving Digital Universe will only grow modestly between now and 2020, which means the cost of managing each byte in the Digital Universe will drop steadily - an incentive to create even more information. An informative presentation of the data may be found at <http://www.emc.com/collateral/demos/microsites/idc-digital-universe/iview.htm>.

COURT TO DECIDE IF STATE CAN REGULATE VIDEO GAMES

On April 26th, the Supreme Court agreed to review a challenge to California's ban on the sale of violent video games to minors. The decision comes hot on the heels of the court's decision to overturn a congressional ban on videos depicting animal cruelty, with the justices saying they would consider the constitutionality of California's 2005 law sometime during the term that starts in October. The law's author, state Sen. Leland Lee, D-San Francisco, said he was pleased with the upcoming court review, noting that the Supreme Court has never heard a case dealing with violent video games so states are now certain to receive direction on how to proceed with this important issue. Opponents of the California law, such as Entertainment Software Association President Michael D. Gallagher, have stated that the public agrees that video games should be provided the same protections as books, movies and music and added that his company looked forward to vigorously defending the works of the industry's creators, storytellers and innovators. Those in favor of the law, like California Attorney General Jerry Brown, have argued that the Supreme Court should permit states to treat extremely violent material the same as sexually explicit material, adding that the First Amendment rights of minors are not coextensive with those of adults. At least one child psychologist has backed the statute, citing academic studies suggesting links between playing violent video games and aggressive behavior. The law in question prohibits the sale of video games to minors under 18 where a reasonable person would find that the violent content appeals to a deviant or morbid interest of minors. Similar to laws governing obscenity, the California statute exempts games that have serious literary, artistic, political, or scientific value. In California, retailers are subject to \$1,000 fines for each violation. At least nine other states and localities have enacted similar restrictions, including Washington, Minnesota and Illinois. A copy of the story may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2010/04/26/AR2010042601762.html>.

U.S. STUDENTS SUFFERING FROM INTERNET ADDICTION: STUDY

On April 23rd, PCWorld.com reported that a new study has found that American college students are hooked on cellphones, social media, and the Internet and showing symptoms similar to drug and alcohol addictions when the media is taken away. In fact, researchers at the University of Maryland, who asked 200 college students to give up all media for one full day, observed that after 24 hours many showed signs of withdrawal, craving and anxiety along with an inability to function well without their media and social links. Susan Moeller, the study's project director and a journalism professor at the university, said many students wrote about how they hated losing their media connections, which some equated to going without friends and family. Moeller said students complained most about their need to text and to have instant messaging services. One student wrote that texting and IM-ing her friends gave the student a constant feeling of comfort: "when I did not have those two luxuries, I felt quite alone and secluded from my life." It is important to note that the American Psychiatric Association does not recognize so-called Internet addiction as a disorder, but it appears that such problems seem to be an affliction of modern life. In one extreme example in South Korea, a couple allegedly neglected their three-month-old daughter, who died of malnutrition, because they were on the computer for up to 12 hours a day raising a virtual child. Just recently, Internet addiction clinics have popped up across the globe. In the United States, a small private center called ReSTART, located near Redmond, Washington, opened last year in the shadow of computer giant Microsoft to treat excessive use of the Internet, video gaming and texting. The center's website cites various examples of students who ran up large debts or dropped out of college due to their obsession. More information may be found at <http://www.techjackal.net/internet/2010/04/25/us-students-suffer-from-internet-addiction-study-claims/>.

1.5 MILLION STOLEN FACEBOOK IDS UP FOR SALE

On April 23rd, InfoWorld.com reported that the hacker known as Kirlos has offered up to 1.5 million Facebook user names and passwords for sale. To put this number in perspective, if the accounts are legitimate, Kirlos is offering the account information of about one in every 300 Facebook users. Also interesting is the low, low price at which Kirlos is offering the information - \$25 to \$45 per 1,000 accounts, depending on the number of contacts each user has. Kirlos' Facebook prices are extremely cheap compared to what others are charging. In its most recent Internet Security Threat Report, Symantec found that e-mail usernames and passwords typically went for between \$1 to \$20 per account -- Kirlos wants as little as \$0.025 per Facebook account. More coveted credit card or bank account details can go for much more, ranging between \$0.85 to \$30 for credit card numbers to \$15 to \$850 for top-quality online bank accounts. To date, Kirlos seems to have sold close to 700,000 accounts. This latest sale is just the latest of a string of sales of social-networking credentials; however, just recently, there has been a shift to global targets, such as Facebook. The social-networking giant has more than 400 million users worldwide, many of whom fall victim to scams each day. In one such scam, criminals send out messages from a compromised account, telling friends that the account's owner is trapped in a foreign country and needs money to get home. In another, they send Web links that lead to malicious software, telling friends that it's a hilarious or sensationalistic video. According to Randy Abrams, director of technical education with security vendor Eset, people will follow it because they believe it was a friend that told them to go to this link. Once the malware gets installed, criminals can steal more passwords, break into bank accounts, or simply use the computers to send spam or launch distributed denial of service attacks. A copy of the story may be found at http://www.infoworld.com/d/the-industry-standard/15-million-stolen-facebook-ids-sale-645?source=rss_infoworld_news.

OUR BLACKBERRY'S DIRTY SECURITY SECRETS

On April 19th, PCWorld.com reported that while BlackBerry has been viewed as a "secure" mobile phone, it too has its shortcomings. More specifically, Tyler Shields, senior member of the Veracode Research Lab, has explained that cyber criminals can plant spyware on the device and make off with your sensitive data if the BlackBerry user isn't careful. For starters, there's an application called FlexiSpy, which allows users to get copies of SMS, call logs, e-mails, and locations and listen to conversations within minutes of purchase. Then there's Mobile Spy, which will allow a purchaser to see exactly what the unsuspecting individual is doing while you are away. To be fair, some of these programs, particularly those whose focus is on catching employees sending out confidential or proprietary data, could be viewed as security-enhancing programs. But, spyware has always been a double-edged sword as IT administrators have long used variations of it to access remote company machines that need repair, for instance. That aside, the mobile spyware, at least according to Shields, is very easy to write

and the security model of mobile platforms is too loose. In his opinion, there is no easy or automated way to confirm for ourselves what the applications are actually doing and we're trusting the application vendor for the majority of our mobile device security. And BlackBerry isn't the only mobile phone brand facing scrutiny. In fact, Apple's iPhone has been viewed by many to be the phone most susceptible to cybercrime. A recent presentation by Trevor Hawthorn, founder and managing principal at Stratum Security, discussed security holes found in AT&T's network, which Apple's iPhone uses, and how an epidemic of "jailbreaking" is disabling critical security controls on the device. More information may be found at http://www.pcworld.com/article/194577/your_blackberrys_dirty_little_security_secret.html.

CHINA SET TO TIGHTEN STATE SECRETS LAW FORCING INTERNET FIRMS TO INFORM ON USERS

On April 28th, The Washington Post reported that China is poised to strengthen a law requiring telecommunications and Internet companies to snitch on customers who discuss state secrets, potentially forcing businesses to collaborate with the country's vast, dissent-stifling security apparatus. The move comes as China continues to tighten controls on communications services and follows a dispute over censorship that prompted Google to move its Chinese site to Hong Kong, which provides broader protection of civil liberties than mainland China. The proposed change would make more explicit the requirement that telecommunications operators and Internet service providers assist police and state security departments in investigations of leaks of state secrets. The official Xinhua News Agency quoted the new amendment as requiring information transmissions to immediately be stopped if they are found to contain state secrets and further, once a leak has been discovered, records should be kept and the findings reported to authorities. In China, state secrets have been so broadly defined that they could mean virtually anything and the new draft amendment preserves this wide scope, defining state secrets as information that concerns state security and interests and would, if leaked, damage state security and interests in the areas of politics, economy and national defense, among others. While the new amendment's passage will probably not mean a significant change to communications companies, it most likely will affect people using local Internet service providers. More specifically, Beijing-based human rights lawyer Mo Shaoping said the amended law would mean that communications service providers would be unable to protect the privacy of their clients. In his opinion, such regulation will leave users with no secrets at all, since the service providers have no means to resist the police. The draft amendment was just submitted to the National People's Congress Standing Committee for a third review, usually the final stage before being adopted by lawmakers. A copy of the story may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2010/04/27/AR2010042704503.html>.

SMARTPHONE MANAGEMENT BECOMING A NIGHTMARE

On April 29th, NetworkWorld.com reported that Smartphones and mobile devices generally are becoming a nightmare for IT shops to manage, with users carrying multiple types of phones with different operating systems and expecting access to e-mail, video-conferencing, and various types of corporate applications. While initially, management was relatively simple when all employees simply were given a Dell Latitude laptop and a BlackBerry. Now, phones are becoming like mini-computers and, to further complicate matters, there are six major platforms: BlackBerry, iPhone, Android, Palm, Windows Mobile and Symbian. Giving customers e-mail is easy, but taking all sorts of corporate applications and running them on all of these platforms isn't. And, as the mobile world becomes more complicated, companies can't just decide to support one device. As Lisa Phifer, president of Core Competence, a business technology consulting firm, said: "An enterprise may focus more of its efforts on a few strategic platforms and applications, but IT executives will find it difficult to block certain mobile devices." Ultimately, she believes companies need new management platforms and policies that are inclusive of multiple types of devices. If all mobile applications ran in Web browsers, creating standard tools that can be used across the gamut of mobile platforms would be easier. But, the rise of the iPhone and Android has fueled the rise of individual apps, many of which work on one device but not another. More information may be found at <http://www.networkworld.com/news/2010/042810-interop-smartphone-management.html> On April 29th, NetworkWorld.com reported that Smartphones and mobile devices generally are becoming a nightmare for IT shops to manage, with users carrying multiple types of phones with different operating systems and expecting access to e-mail, video-conferencing, and various types of corporate applications. While initially, management was relatively simple when all employees simply were given a Dell Latitude laptop and a BlackBerry. Now, phones are becoming like mini-computers and, to further complicate matters, there are six major platforms: BlackBerry, iPhone, Android, Palm, Windows Mobile and Symbian. Giving customers e-mail is easy, but taking all sorts of corporate applications and running them on all of these platforms isn't. And, as the mobile world becomes more

complicated, companies can't just decide to support one device. As Lisa Phifer, president of Core Competence, a business technology consulting firm, said: "An enterprise may focus more of its efforts on a few strategic platforms and applications, but IT executives will find it difficult to block certain mobile devices." Ultimately, she believes companies need new management platforms and policies that are inclusive of multiple types of devices. If all mobile applications ran in Web browsers, creating standard tools that can be used across the gamut of mobile platforms would be easier. But, the rise of the iPhone and Android has fueled the rise of individual apps, many of which work on one device but not another. More information may be found at <http://www.networkworld.com/news/2010/042810-interop-smartphone-management.html>.

FINAL TALLY: IT LOST 250,000 JOBS LAST YEAR

On April 28th, ComputerWorld.com reported that the U.S. tech industry lost about 250,000 jobs last year - about 4 percent of its total workforce - but it is seeing signs of a hiring turnaround, particularly in software services. Yet, even in a downturn, tech remains one of the better occupations; while the overall unemployment rate was about 9.3 percent last year, for computer programmers it was 5.2 percent and for computer scientists, 6.1 percent. And, in the fourth quarter of last year, software services grew by 10,100 jobs or 0.6 percent. The top state for those seeking technology jobs is California, with nearly 1 million jobs out of the 5.9 million employed nationally in tech. In second place is Texas at 492,000. Rounding out the top five is New York, 309,000; Florida, at 292,000 and Virginia, 283,000. To help improve the overall tech business climate Phil Bon, TechAmerica's president and CEO, said that his group is lobbying Congress to extend the research and development tax credit. Without the tax credit, he believes that the government is encouraging the outsourcing of innovation around the world. In addition, his group is also urging the U.S. Department of Health and Human Services to move ahead on its health IT programs. Bond said health IT will require tens of thousands of new highly skilled workers and will have a very positive, stimulating effect on job creation. No matter what, Evelyn Hirt, president of the Institute of Electrical and Electronics Engineers (IEEE-USA), said that re-employed engineers, scientists and other technology professionals will help create more jobs and ratchet the economy forward. A copy of the story may be found at http://www.computerworld.com/s/article/9176061/Final_tally_IT_lost_250_000_jobs_last_year.

REPORT SAYS 33 SEC STAFF MEMBERS VIEWED PORNOGRAPHY AT WORK

On April 24th, The Washington Post reported that dozens of Securities and Exchange Commission (SEC) staff members used government computers in the past five years to access and download pornographic images, with most of the reported incidents occurring in the 2 1/2 years since the global financial meltdown began. In the report, which was prepared by SEC watchdog Kotz, three incidents were reported this year, ten occurred in 2009, 16 in 2008, two in 2007, and one each in 2006 and 2005. While the discovery of an employee surfing the Internet for porn is nothing new, whether in a federal agency or a private entity, the SEC revelations sparked a broader question about how well federal agencies block such activity. The General Services Administration has stated that each federal agency is responsible for setting an Internet usage policy. The SEC uses Blue Coat Secure Web Gateway software and McAfee SmartFilter to block inappropriate Web sites. But, according to agency spokesman John Nester, workers apparently were able to evade the blocking software. Nester further stated that all of the employees involved have been disciplined or are facing discipline. The report could not have come at a worse time; it was released less than a week after agency announced its decision to file fraud charges against Goldman Sachs and amid reports that two Republican commission members sharply questioned senior investigators about their evidence. A summary of the report highlighting the conduct may be found at <http://cnnac360.files.wordpress.com/2010/04/secretreport.pdf>.

MICROSOFT GETS MORE AGGRESSIVE WITH FREE SOFTWARE

On May 12th, Microsoft rolled out a new edition of its Office programs to businesses and, for the first time ever, it is adding versions of Word and other programs that will work in a Web browser that will be free for consumers. This pragmatic shift comes as Microsoft tries to keep up with a market-wide shift from programs that are stored on PCs to free ones that can be accessed from any computer, over the Internet. True, businesses aren't ready to embrace Web-based Office-style programs quite yet, but people still want access to their files when they're not online. Forrester analyst Sheri McLeish sees this as a defensive move against the online apps from Google and other rivals that are pushing this concept, which is often called cloud computing. She noted that businesses that do want Web-based programs might prefer Microsoft's because its online software was built to trade documents with Microsoft's desktop programs without losing formatting. However, as one reporter pointed out, Microsoft must be

careful not to make the free apps so appealing as to undermine its lucrative desktop software business, which accounted for 29 percent of Microsoft's revenue and 51 percent of its operating income in the most recent quarter. The free apps will have fewer features than the desktop versions. For businesses, access to the apps is included in the regular Office licensing fees, while the consumer apps will carry advertisements. In addition to these new apps, Office 2010 also incorporates a plethora of new features and updates to individual programs. Several of these updates allow people to work on the same document simultaneously, a feature Google's programs already allow. In addition, Office 2010 incorporates a powerful photo-editing tool and adds video and audio editing functions to PowerPoint. Finally, Outlook will now be able to pull in information from users' outside social networks, such as Facebook and LinkedIn and adds new features to tame the ever-growing number of messages in a user's inbox. Office 2010 and the free Web Apps will be available in June. A copy of the story may be found at http://www.usatoday.com/tech/products/2010-05-12-microsoft-office_N.htm.

STOLEN VA LAPTOP CONTAINS VETERANS' PERSONAL DATA

On May 13th, The Washington Post reported that the laptop belonging to a contractor working for the Veteran's Affairs Department, which was stolen earlier this year and contained the personal data of hundreds of veterans stored on the computer, was not encrypted, a violation of a Virginia information technology policy. While it was bad enough the laptop was stolen, if the data had been encrypted, it would have prevented a thief from accessing the information. Once it became known that the data was unencrypted, Representative Steve Buyer launched an investigation regarding how many VA contractors are not complying with the encryption requirement. Through the investigation, Buyer found that 578 vendors had refused to sign new contract clauses that required them to encrypt veteran data on their computers, an apparent violation of rules. Buyer sent these findings to Virginia Secretary Eric Shenseki and informed him that his staff also had uncovered another recent theft of an unencrypted laptop from a separate contractor that he did not identify. This vendor had 69 contracts in more than half of the department's 21 regional medical networks operated by the Veterans Health Administration, and 25 of those contracts, more than a third, did not have a clause that required data be encrypted. While there have been no reports of the information being used maliciously, if nothing else, these recent violations truly are an alarming trend. More information may be found at http://www.nextgov.com/nextgov/ng_20100513_1937.php.

CRAIGSLIST DIAMOND AD LEADS TO DEADLY HOME INVASION, POLICE SAY

On May 7th, Washington state authorities stated that four suspects have been charged with first-degree murder in connection with a home invasion that began with an ad on Craigslist. According to Pierce County Prosecutor Mark Linquist, the case began when James Sanders and his wife posted an ad on Craigslist offering a diamond ring for \$1,050. Sanders then arranged to meet prospective buyers of the ring at the family's home. It all went downhill from there. Two individuals showed up and pretended to be a couple looking to purchase the ring for a mother-in-law; however, once they entered the house, the man posing as the husband pulled out a handgun. Sanders, his wife, and their sons, ages 14 and 10, were restrained with plastic handcuffs. Two other suspects then entered the home, one of which pistol-whipped the older son. According to Linquist, Sanders was able to free himself from the restraints and attempted to defend the 14-year-old. It cost him his life. The latest tragedy comes just a year after a medical student in Boston, Massachusetts, was charged with killing a woman who advertised a massage service on Craigslist. Perhaps prosecutor Lindquist said it best: you hate to tell people to be wary of your fellow citizens, but the reality is you've got to be wary when you are doing something when interacting with strangers on Craigslist. A copy of the story may be found at <http://www.cnn.com/2010/CRIME/05/07/craigslist.diamond.killing/index.html>.

SMARTPHONES ARE THE LATEST PATENT BATTLEGROUND

On May 12th, Business Week reported that the recent onslaught of patent lawsuits in the mobile-phone market could push up costs for handset makers and consumers. For starters, there is the Nokia v. Apple battle, which began in October 2009 when Nokia accused Apple of infringing on 10 patents and demanded royalties. This just recently heated up on May 7, 2010, after Nokia lodged a patent infringement suit against Apple in Madison, Wis., saying that Apple's iPhone and iPad violate five Nokia patents. And then there is the Apple, HTC debacle. In March, Apple sued HTC, contending that the Taiwan-based company infringed on 20 Apple patents relating to touch and menu controls. HTC responded to the Apple litigation with a complaint at the U.S. International Trade Commission, asking the agency to halt imports and sales of iPhones and iPads in the U.S. Finally, Microsoft has also pursued patent payments from companies that make phones based on Android software. In fact, on April

27th, Microsoft said HTC would license its software for the phones. Patents also played a role in the recent \$1.2 billion deal for Palm. Hewlett-Packard has said that patents associated with Palm's WebOS operating system for smartphones is one reason it wants to acquire Palm. With the added litigation comes added costs as patent holders are asking a large slice of the smartphone revenues pie. Some have estimated that HTC likely pays Microsoft \$20 to \$40 per phone for use of certain licenses and one Android handset maker has already budgeted for its patent royalty payments to double next year. In the end, the popularity of smartphones has led patent holders to say it is time to pay up - and ultimately that's what consumers may be forced to do. A timeline of all the recent patent litigation may be found at http://www.businessweek.com/technology/content/may2010/tc20100512_956709.htm.

GOOGLE'S WI-FI SNOOPING EARNS IT A CLASS-ACTION LAWSUIT

On May 17th, an Oregon woman and a Washington man filed a federal lawsuit against Google, accusing the Internet search provider of violating federal privacy and data acquisition laws when Google Street View vehicles snatched up data from unprotected hotspots. According to court documents, the data collection systems located on the vehicles were outfitted with wireless packet sniffers that, in addition to collecting the user's unique or chosen Wi-Fi network name (SSID information), the unique number given to the user's hardware used to broadcast a user's Wi-Fi signal MAC address, also collected data consisting of all or part of any documents, e-mails, video, audio, and VoIP information being sent over the network by the user payload data. Google has acknowledged the privacy problem exists, but stated that it had not known that it was collecting data from unprotected wireless networks until recently. The company explained that the blunder was discovered when Google audited the Street View Wi-Fi data after a request by Hamburg, Germany, data protection authorities. The lawsuit seeks class-action status, which would open the case to a pool of Plaintiffs potentially numbering in the millions, and seeks both statutory and punitive damages. The former is set as the greater of \$100 for each day any plaintiff or class member's data was grabbed by Google, or \$10,000 per violation suffered by each plaintiff or class member. Further adding salt to the wound are the additional legal actions arising from the Street View snafu. German prosecutors, for example, have launched a criminal investigation into Google's actions, while in the United States, the Federal Trade Commission (FTC) has been asked to investigate Google by the consumer group Consumer Watchdog. A Google blog post on the topic may be found at <http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html>.

EFF WARNS: YOUR BROWSER HAS FINGERPRINTS

On May 18th, InfoWorld.com reported that, even without cookies, popular browsers such as Internet Explorer and Firefox give Web sites enough information to create a unique "fingerprint" of their visitors about 94 percent of the time. More specifically, the Electronic Frontier Foundation has compiled research demonstrating that configuration information - data on the type of browser, operating system, plug-ins, and even fonts installed - can be compiled by Web sites to create a unique portrait of most visitors. So what does this mean to the casual user? It means that most Internet users are a lot less anonymous than they believe. Even a cautious user that turns off his or her cookies and uses a proxy to hide his or her IP address can still be tracked. True, the data doesn't actually identify the Web user and no single piece of data is enough to identify the visitor on its own, but when it's all strung together, a fairly clear picture of who is doing the Web browsing appears. In fact, the picture is allegedly so clear that there are already a handful of companies offering this kind of cookie-less Web tracking to help e-commerce sites identify fraudsters. And it seems to be working. For instance, when Serbian criminals started testing stolen credit cards by posting hundreds of \$1.99 transactions to the iReel.com online movie site each day last August, iReel turned to such a company to get a fix on the fraudsters. The company ThreatMetrix generated digital fingerprints of site visitors, enabling iReel to know when a single user was trying to use hundreds of different credit cards, even when the fraudster was using proxy IP addresses. For people who think they are anonymously surfing the Web, the fact that these products are catching on is bad news. However, there are some effective countermeasures individuals can employ. A uniquely identifiable IDG News Service Windows XP computer running Firefox could not be identified with the NoScript safe browsing extension turned on. Adding the Tor Internet anonymization software also works. And mobile browsers needn't worry for now. Both the iPhone and Android platforms often are not identifiable given the lack of variety in the browser plug-ins and font add-ons. A copy of the report may be found at <https://panoptickick.eff.org/browser-uniqueness.pdf>.

FCC RELEASES ANNUAL WIRELESS COMPETITION REPORT: NO CONCLUSION THAT

MARKETPLACE WAS EFFECTIVELY COMPETITIVE.

On May 20th, the Federal Communications Commission (FCC) released its annual wireless competition report and, for the first time since 2003, the agency declined to conclude that the wireless marketplace was "effectively competitive." In response, Verizon Wireless issued a statement, arguing that the U.S. has the most intensely competitive wireless market on the planet, and it's becoming more competitive by the day. In the company's opinion, the facts and the record establish conclusively that the wireless marketplace is effectively competitive, as the FCC has found in the previous six wireless competition reports. And while two FCC commissioners did question the omission, the FCC report did indicate that figuring out whether the industry is competitive can be complicated. For instance, in the report, the agency noted that competition is dependent on a company's respective position within the market and the dynamics associated with said position. Furthermore, the FCC explained the mobile wireless ecosystem is sufficiently complex that any review or analysis of competitive market conditions must take into consideration a multitude of factors. As such, the FCC declined to reach an overarching, industry-wide determination with respect to whether there is "effective competition," choosing instead to comply with the statutory requirement by providing a detailed analysis of the state of competition that seeks to identify areas where market conditions appear to be producing substantial consumer benefits and provides data that can form the basis for inquiries into whether policy levers could produce superior outcomes. A copy of the report may be found at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-81A1.pdf.

The statement released by Verizon Wireless may be found at <http://finance.yahoo.com/news/Verizon-Statement-on-FCC-prnews-415690907.html?x=0>

MARSHALL COUNTY CHIEF DEPUTY ACCUSED OF "CYBERSQUATTING"

On May 18th, whnt.com reported that Ed Teal, a candidate for Marshall County Sheriff, had filed a lawsuit against his opponent, incumbent Scott Wall's Chief Deputy, Doug Gibbs, accusing Gibbs of cybersquatting. For those unfamiliar with the term, cybersquatting refers to the use of a domain name that could have someone else's name (or company) in it, to make profit off their name or to prevent that person from using it themselves. As it relates to this particular lawsuit, Teal alleged that in January he went to register a Web site to be used in connection with his campaign only to find that most, if not all of the Web addresses he could use had already been registered. Using a court order, Teal's attorney discovered that current chief deputy, Gibbs, had registered 19 Web addresses that use some variation of Teal's name. Teal has claimed that Gibbs obviously intended to deprive Teal's campaign from the use of the Internet in support of his candidacy and has asked that the court order Gibbs to surrender the addresses. A copy of the story may be found at <http://www.whnt.com/news/whnt-cybersquatting-ed-teal-scott-walls,0,5103139.story>.

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  SafeSubscribeSM
For Email Marketing you can trust

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