

# { 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 159 - August 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)

---

### PARENTS, TEENS OFTEN TEXT WHILE DRIVING

On July 14th, cell phone maker LG Electronics released the results of a recently conducted survey about the texting habits of children and their parents. The survey found that 44% of parents have texted while driving, and 28% have done some form of sexting, which is defined as the sending, receiving, or forwarding a text containing sexual content. This comes in spite of 53% of parents indicating that they were "very informed" about the impact of negative habits like sexting and texting while driving. Among teens, the survey revealed 43% of children admitted to participating in some form of sexting, while 45% said they text while driving. Yet, alarmingly, very few parents said that they believed their teens engage in harmful or inappropriate texting behaviors. Dr. Charles Sophy, a member of LG's Text Ed advisory council, a program that provides advice on mobile communications issues, and a child and family psychiatrist, stated that he believes the survey revealed the root of bad texting habits. More specifically, he believes the "do as I say, not as I do" approach to child-rearing isn't cutting it. With so many adults engaging in sexting and texting while driving, it is no wonder that children don't think they are doing anything wrong. True, texting is a powerful tool that can open the lines of communication and facilitate closer relationships between teens and their parents, but it must be used properly and responsibly. A copy of the results may be found at <http://www.gomonews.com/mobile-abuse-teens-and-parents-are-naughty-when-texting/>.

---

### APPLE, AT&T SUED OVER IPHONE 4 ANTENNA PROBLEMS

On July 1st, two Maryland residents filed a suit, which recently achieved class-action status, against Apple and AT&T, arguing that the new iPhone 4 suffers from a defective antenna design that causes the smartphone to drop calls and not hold a strong cellular signal. More specifically, the lawsuit claimed that Apple knowingly sold defective phones and thereby broke its warranty promises. Additionally, more charges were levied against Apple and AT&T, including general negligence, deceptive trade practices, fraud, and misrepresentation. The suit is the first stemming from complaints about sub-standard iPhone 4 call reception, which started when the new phone first reached users. Almost immediately, owners reported that their phones would lose a signal, or that the signal indicator would show a weakened signal, when the smartphone was gripped in a certain way, especially if it was held in the left hand. Hardware experts have reported that holding the new iPhone a particular way can bridge the two antennas embedded in the steel band that encircles the device, lowering signal strength and changing its ability to receive and transmit signals at the designed frequencies. The suit demanded Apple and AT&T pay compensatory and punitive damages, and that Apple be barred from selling more iPhone 4s until it has "repaired the design and/or manufacture defect." This suit will likely not be the last. A Californian law firm has recently begun soliciting iPhone users who have experienced poor reception for a class-action case. Thus far, the firm stated it had received more than 1,400 emails from iPhone 4 owners interested in joining a lawsuit. More information may be found at <http://www.networkworld.com/news/2010/070110-apple-att-sued-over-iphone.html>.

---

### SOCIAL NETWORK SECURITY POLICIES LACKING

On June 28th, *TechWeb.com* reported on the fascinating statistics highlighted by a recent Symantec study. Specifically, the report found that while a little more than 30% of employees never access social networking sites from work, an equal number access them once or twice per day, 16% access them up to five times per day, and

2% hit them more than 20 times in a single work day. But, of those that do, 53% of the time they spent on social networking sites at work was allegedly for work purposes. So how do businesses approach access to social networking sites? Symantec found that only 5% of organizations block such sites outright, 33% don't block but have policies stating that social networks can only be used for business purposes, and 42% have no policy or blocking whatsoever. So what's the right approach? Having no policy, or an inadequate policy, could result in lost productivity or poor customer service on the one hand, and security threats on the other. Symantec suggests that companies address these problems by developing social networking security policies and guidance for employees. Crucial to creating an effective policy, however, is then having the ability to monitor and enforce the policy as well as having a process for regularly updating it to keep it relevant. But, Symantec cautions against barring social media entirely. Researchers are finding that having access to at least some social networking tools is often beneficial, even for productivity purposes. In fact, in another study, Forrester Research found that 70% of IT personnel viewed Web 2.0 and social media as having a beneficial impact on their organization's productivity. In addition, four out of five respondents said social media had a positive impact on organizational innovation, and 78% believed it helped the organization provide better customer service. More information may be found at <http://www.techweb.com/article/showArticle?articleID=225701636>.

---

## NETWORK SECURITY THREATS INCREASING

On June 24th, a study conducted by security information and event management provider netForensics reported that 80% of IT managers expect network-borne threats to increase throughout 2010 and 2011, and 85% see their security environment becoming more complex. Yet over half of them stated that their organization wasn't budgeting sufficiently, or recruiting enough new talent, to counter the added threats or complexity. In addition, the study also found changes in security staff size over the past year. 15% of IT managers reported an increase in staff, 24% reported a decrease, and 54% reported that their organization's staff remained unchanged. However, going forward, 20% of organizations planned to hire more security personnel, 15% planned to downsize, and 51% expected to stay the same. According to Dale Cline, CEO of netForensics, with security staff size remaining static or decreasing, and budgets not being allocated to put security processes in place, organizations are going to face greater challenges than ever to their security posture. The company's VP of product and marketing, Tracy Hulver, recommended that organizations should look at using tools and technologies that can scale up their response, without adding staff or budget. Examples of such tools include outsourcing to cloud security, deploying technologies that maximize existing security infrastructure without having to invest in new, big-budget items, and acquiring technology via SaaS pricing models. Interestingly, even with the majority of organizations seeing increasing numbers of threats, but little or no increase in their security budget, 70% of respondents said they wouldn't outsource their organization's security. Key results may be viewed at <http://www.wten.com/Global/story.asp?S=12703145>.

---

## GOOGLE DEFEATS VIACOM IN LANDMARK COPYRIGHT CASE

On June 23rd, U.S. District Judge Louis Stanton, who has overseen the longtime copyright fight between Viacom and Google over YouTube, granted summary judgment for the Internet search giant. In so doing, the court concluded that YouTube was protected by the safe harbor of the Digital Millennium Copyright Act (DMCA) against claims of copyright infringement. In a posting to its website, Google stated that the decision followed established judicial consensus that online services like YouTube are protected when they work cooperatively with copyright holders to help them manage their rights online. Viacom, parent company of Paramount Pictures and MTV, indicated that it plans to continue to fight. It responded to the ruling by stating that the opinion was fundamentally flawed and contrary to the language of the DMCA. The company stated that it intends to have these issues before the U.S. Court of Appeals for the Second Circuit as soon as possible. In other words, look for round two of this battle soon. A copy of the summary judgment opinion may be found at <http://www.scribd.com/doc/33470608/Viacom-Google-summary-judgement-opinion>.

---

## FEDERAL IT SPENDING TO REACH \$112 BILLION

On June 22nd, *InformationWeek.com* reported that federal IT spending is expected to grow by more than 5% to \$112 billion by 2015 thanks to the Obama's administration's plan to use technology to achieve key cost-saving and transparency measures. In fact, according to a report conducted by INPUT, many of the administration's priorities to improve how the government engages both with the public and among agencies hinge on technology, as do cybersecurity measures and a focus to increase program oversight and performance. In addition, the report noted

that the federal government has also viewed technology as a way to help reduce energy costs. Even with this substantial investment, the report concluded the government lacks the personnel necessary to achieve those goals. This means that there still will be plenty of contracts awarded to IT professionals serving the government. Moreover, expect growth to continue into the foreseeable future. INPUT analyst John Slye stated that the criticality of IT to government operations and priorities, as well as the gap in federal IT expertise, suggests that IT spending will continue with modest growth. The report also asked government IT professionals which technologies will get more attention in the next five years. Not surprisingly, cloud computing topped the list, with 67% of those surveyed saying it will receive new or increased focus. IT security was close behind, with 62% of those surveyed acknowledging a greater focus there. The other priorities for the government sector include virtualization (48%), IT modernization (38%), infrastructure consolidation (35%) and telework (26%). More information is available at <http://www.informationweek.com/news/government/info-management/showArticle.jhtml?articleID=225701061>.

## **NEWSPAPER WEBSITE MUST IDENTIFY ANONYMOUS WEB COMMENTERS**

On June 3rd, an Illinois appeals court ruled that a small town newspaper was required to release information identifying anonymous online writers who posted allegedly defamatory comments on the newspaper's website, overturning the lower court's ruling and granting Donal and Janet Maxon's petition for discovery. The trial court had initially dismissed the action, finding that the Plaintiffs had not satisfied the hypothetical summary judgment test established under *Dendrite Int'l Inc. v. Doe*, 775 A.2d 756, 29 Med.L.Rptr. 2265 (N.J. Super. Ct. App. Div. 2001) and *Doe v. Cahill*, 884 A.2d 451, 33 Med.L.Rptr. 2441 (Del. 2005) because the "literary and social context of the statements rendered them nonactionable opinions as a matter of law." The appellate court disagreed, finding that the trial court had improperly analyzed the legal questions. More specifically, the court said that while anonymous free speech is protected by the First Amendment, there is no constitutional right to defame. Additionally, the court found that the procedural tests created under *Dendrite* and *Cahill* added nothing to the protections provided under Rule 224 - the rule under which the Maxons sought discovery. To the extent a petitioner presents a prima facie case of defamation, the court said, the petitioner has a right to expect a remedy. Here the court found: "the Maxons have stated [a] cause of action for defamation sufficient to warrant the anonymous individual to come forward and answer the complaint. The statements that the Maxons bribed certain officials in order to obtain approval for their zoning request are not mere statements of opinion. The mere fact that a statement of fact is couched in the rhetorical hyperbole of an opinion does not render it nonactionable. The test is whether the statement can be reasonably interpreted as stating actual fact." Accordingly, the court overturned to lower court's decision. Justice Daniel Schmidt dissented, objecting to the majority's finding with respect to the *Dendrite* and *Cahill* analysis, and the question of whether the bribery comments were truly defamatory. On the latter point, Schmidt said the statements were little more than "conjecture, surmise and a statement of subjective theory." Whether the newspaper will attempt to appeal the case to the Illinois Supreme Court or provide the requested information remains to be seen. A copy of the complaint can be downloaded at <http://ipcenter.bna.com/pic2/ip.nsf/id/BNAP-86BJQB?OpenDocument>.

## **ICANN OKS .XXX DOMAIN NAME FOR PORN SITES**

On June 25th, *CNET News* reported that ICANN, after denying several requests over the years for a new .xxx top-level domain, finally relented and gave the new domain its conditional approval. ICM Registry, which will manage and sell the new domain name to porn sites, has waged a long struggle to get .xxx accepted by ICANN as a top-level domain, only to get a thumb's down at each turn. ICM's Chairman Stuart Lawley has consistently touted the .xxx domain as a way to segregate and safely filter out adult entertainment sites. However, conservative groups have in the past lobbied Washington and reportedly pressured ICANN to deny the request. Lawley added that the decision brings to fruition a six-year effort to create a specific Web address for online adult entertainment, and comes on the heels of an independent review that declared that ICANN's previous decision to deny .xxx was wrong. Although ICM has declared the instant decision a major victory, final approval of the new domain still faces some red tape. The first step, which just recently began, is for ICANN to check ICM's financial and technical ability to run the new registry. ICM would then be required to negotiate a contract that takes into account recommendations from the Government Advisory Committee, which advises ICANN on issues of public policy. Finally, the matter would go to ICANN's board for final approval. Thus far, ICM has said it already has 110,000 pre-reservations from sites looking to adopt the new address and expects that number to increase once ICANN grants formal approval. Hopefully, if all goes well, Lawley said his company expects to make \$30 million a year in sales by selling each .xxx site for \$60, but is promising to donate \$10 from each sale to child protection initiatives through a nonprofit group that he has set up. More information may be found at <http://news.cnet.com>

---

## **TORONTO LAW FIRM PREPS FACEBOOK PRIVACY SUIT**

On July 8th, *CNET News* reported that a Toronto-based law firm with a penchant of targeting litigation at corporations has a new company in its crosshairs - Facebook. The Merchant Law Group recently launched litigation seeking class action status against the social networking site, contending that the company mishandled sensitive user data. More specifically, the lawsuit has alleged that Facebook changed user privacy settings and its terms of service without first notifying users. This, in turn, purportedly allowed a large portion of information to go public on the Web when it had once been protected. Aside from the breach of privacy allegations, the complaint further alleges that Facebook intentionally or negligently designs its privacy policies, as disseminated to users, in such fashion as to mislead and induce users into putting their personal information and privacy at further risk, that these policies mean that user data can be unwittingly exposed to the harms of data mining, identity theft, harassment, and plain old embarrassment, and that Facebook has unjustly profited off of this member information. The complaint seeks damages equivalent to the total amount of money that Facebook has made through the use of that member information. In response, Facebook spokesman Andrew Noyes stated that the company has found no merit in the complaint and that Facebook will fight it vigorously. A copy of the complaint may be found at [http://docs.maars.net/32262/Facebook\\_Class\\_Action\\_Claim](http://docs.maars.net/32262/Facebook_Class_Action_Claim).

---

## **U.S. PLANS CYBER SHIELD FOR UTILITIES, COMPANIES**

On July 8th, *The Wall Street Journal* reported that the federal government is launching a program called the "Perfect Citizen," which is designed to detect cyber assaults on private companies and government agencies running such critical infrastructure as the electricity grid and nuclear-power plants. Here's how it works. The National Security Agency would provide key surveillance on critical infrastructure, relying on a set of sensors deployed in computer networks that would be triggered by unusual activity suggesting an impending cyber attack, though it wouldn't persistently monitor the whole system. In the end, NSA has stated that the program's goal is to close the big, glaring holes. The information gathered by the program could also have applications beyond the critical infrastructure sector, serving as a data bank that would also help companies and agencies who call upon NSA for help with investigations of cyber attacks. Google made such a request when it sustained a major attack late last year. Yet, for all its worth, industry and government officials have conflicting opinions on the programs. Those who view Perfect Citizen as an intrusion by the NSA into domestic affairs have argued that, "Perfect Citizen is Big Brother." Others have called the program long overdue and said any intrusion into privacy is no greater than what the public already endures from traffic cameras. Moreover, proponents of the program have stated that it is simply a logical extension of the work federal agencies have done in the past to protect physical attacks on critical infrastructure that could sabotage the government or key parts of the country. Because the program is still in the early stages, much remains to be worked out, such as which computer control systems will be monitored and how the data will be collected. NSA would likely start with the systems that have the most important security implications if attacked, such as electric, nuclear, and air-traffic-control systems. In effecting the program, some companies may agree to have the NSA put its own sensors on and others may ask for direction on what sensors to buy and come to an agreement about what data they will then share with the government. And while government can't force companies to join the program, it can provide incentives to urge them to cooperate, particularly if the government already buys services from that company. More information may be found at [http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html?mod=WSJ\\_Tech\\_LEADTop](http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html?mod=WSJ_Tech_LEADTop).

---

## **COURT RULES AGAINST FCC POLICIES ON INDECENCY**

On July 14th, the U.S. Court of Appeals for the 2nd Circuit held that the Federal Communications Commission's rules on indecency were too vague and thus violated the First Amendment. Specifically, the court stated that the FCC had not given clear guidelines on its two main tests for indecency: whether material describes or depicts sexual or excretory organs or activities, and whether a broadcast is "patently offensive as measured by contemporary community standards." As the court went on to explain: "The English language is rife with creative ways of depicting sexual or excretory organs or activities and even if the FCC were able to provide a complete list of all such expressions, new offensive and indecent words are invented every day." With the decision, the panel of three judges handed a victory to broadcasters such as Fox, CBS and ABC, which had petitioned the court to challenge the agency's muscled-up approach of imposing steep fines for impromptu expletives and sexual content.

At stake for broadcasters were fines as high as \$325,000 per violation, which made stations skittish about what to air. In fact, some stations had, in recent years, refrained from airing certain popular shows and movies during primetime hours because they contained profanity. As of this moment, it is unclear whether the FCC will pursue an appeal, with FCC Chairman Julius Genachowski noting that the agency will review the decision. The Parents Television Council called the decision a "slap in the face," and Concerned Women for America, an advocacy group for indecency rules, urged the agency to appeal, lest broadcast television be open to the sexually explicit content and language of cable programs. If nothing else, this latest decision simply highlights the FCC's struggle to change with technology on a variety of fronts. Earlier this year, another court ruled that the agency lacks the authority to oversee consumers' access to Internet services. A copy of the story may be found at [http://www.washingtonpost.com/wp-dyn/content/article/2010/07/13/AR2010071306623.html?wpisrc=nl\\_pmheadline](http://www.washingtonpost.com/wp-dyn/content/article/2010/07/13/AR2010071306623.html?wpisrc=nl_pmheadline).

## **MICROSOFT BLENDS FACEBOOK INTO OUTLOOK**

On July 13th, Microsoft announced that its new Outlook Social Connector plug-in will now support popular social media sites, like Facebook, meaning that Outlook users will be able to view newly posted status updates, pictures, and the like in real time from the convenience of Outlook. While some employers may get the chills envisioning their employees spending the day following their friends on Facebook, incorporating social networks into the work world has been shown to actually enhance work performance in some instances. Additionally, this new plug-in could aid in educating workers on how to properly use social networking sites responsibly and professionally, rather than in a way that wastes time or embarrasses their organization. However, no matter what, employers should not just block off these sites completely. As Lisa Schmeiser wrote in an article titled "The Six Commandments of Social Networking at Work":

...the primary value of a social network is the aggregation of people on it. Block your employees from getting on a network, and you block their access to developing a far-flung group of people who can act as free advisers, leads for new businesses, or prospective new hires.

Members of your sales team can see what top clients are up to, for example, and keep in touch with them. You might learn that a friend or colleague, who happens to be a talented IT pro, has just left his job and set the wheels in motion to make him a job offer. There are also your friends' shared links to articles or other information sources that can benefit you in your day-to-day job.

So, maybe this new collaboration can be a good thing for your business - only time will tell. A copy of the story may be found at <http://mashable.com/2010/07/13/outlook-facebook/>.

## **PENTAGON, STATE DEPARTMENT OKAY SOCIAL MEDIA USE**

On July 13th, *CNET News* reported that the U.S. Defense Department and State Department have okayed the use of Facebook and Twitter; albeit, the greater use comes with the usual caveats for employees. Among the caveats, don't disclose classified information; maintain a distinction between an official and personal account; and be alert to the potential targeting of users for intelligence-gathering purposes. Not all federal agencies have been so progressive. Some agencies have blocked social networking sites altogether. Many who do block access have expressed concerns over proper use, bandwidth, and security. Just look at the Department of Homeland Security. One employee noted that while the agency has a Facebook page, it doesn't "allow people to look at Facebook in the office. So we have to go home to use it. I find this bizarre." Typically, those agencies that block all forms of social networks argue: "Adversaries of the United States are also logging in to use and mine social media sites in search of ammunition for their cause against Western democracies and in the hunt for methods of engagement on the informational battlefield." Lt. Col. Michelle Barrett believes that the wide variance between agencies solidifies the need for the creation of a set of unified rules. She went on to say that the government should not ban social networking entirely, noting that enemies of the United States are already using social media to promote propaganda and the military must respond in kind if it doesn't want lies to spread. In her mind, social media gives American service members the opportunity and capability to tell their story and can at the same time decrease the enemy's credibility should they choose to distort the truth of that same story. More information, including links to the State Department's manual on social media and a memorandum issued by the Department of Defense, may

be found at [http://news.cnet.com/8301-1023\\_3-20010409-93.html](http://news.cnet.com/8301-1023_3-20010409-93.html).

---

## **VIOLATING WEB SITE RULES NOT A CRIME**

On July 22nd, a U.S. District Court judge ruled that it was not a criminal act to violate the Terms of Service of a particular website. The court's decision came after Facebook sued Power Ventures, a company offering software that allowed users to aggregate Facebook friends and other data with similar sets of data from other social networking sites. The social networking giant had argued that because its Terms of Service forbid users from using automated methods to access user data, Power's software violated California's computer crime law, specifically section 502(c), which prohibits access to computers or information that a person is not authorized to access. The Electronic Frontier Foundation filed an amicus brief in support of Power Ventures, contending that any Terms of Service violation should be treated as a civil contract dispute rather than a crime. Further, the EFF stated that turning any violation of Terms of Use into a criminal offense would give websites unfettered power to decide what conduct is criminal, leaving millions of Internet users vulnerable to prosecution for everyday activities. However, the judge was more receptive to an alternate argument raised by Facebook. After it became aware of the software company's conduct, Facebook attempted to block Power's IP address to prevent its software from gathering Facebook user data. But, Power changed its IP address to avoid being blocked. The EFF wrote that there was nothing inherently wrong or unlawful about avoiding IP address blocking, and there are valid reasons why someone might choose to do so, including to sidestep anticompetitive behavior by other Internet services. Here, the judge sided with Facebook, finding that such circumvention would be a crime, if the conduct was intended to avoid a technological protection measure. More information, including a link to download the decision may be found at [http://www.informationweek.com/news/software/web\\_services/showArticle.jhtml?articleID=226200086&cid=RSSfeed\\_IWK\\_News](http://www.informationweek.com/news/software/web_services/showArticle.jhtml?articleID=226200086&cid=RSSfeed_IWK_News).

---

## **EXPERTS PREDICT EXTENSIVE ATTACKS OF WINDOWS ZERO-DAY**

On July 19th, security organizations raised Internet threat levels concerned about widespread attacks using exploits of a just-acknowledged critical bug in all versions of Windows. For instance, the Internet Storm Center (ISC) pushed its Infocon threat indicator to "Yellow," a rare move, while Symantec also bumped up the status of its ThreatCon barometer to "Elevated." The moves come after Microsoft confirmed that attackers can use a malicious shortcut file, identified by the ".lnk" extension, to automatically execute their malware by getting users to view the contents of a folder containing such a shortcut. Malware can also automatically execute on many systems when a USB drive is plugged into the PC. Making matters worse, all versions of Windows, including the just-released beta of Windows 7 Service Pack 1 (SP1), as well as the recently retired Windows XP SP2 and Windows 2000, contain the vulnerability. Moreover, while Microsoft has offered up workarounds, there is no timeline circulating for a fix; albeit, Jerry Bryant, a group manager with the Microsoft Security Response Center (MSRC), said that the company would definitely patch the problem. But unless Microsoft makes a dramatic policy change - and backtracks on statements it gave as recently as June - patches will not be issued for Windows XP Service Pack 2 (SP2), the edition that was retired from all support on July 13th. Microsoft's next regularly-scheduled security updates are slated to ship on August 10th. Microsoft does sometimes issue emergency updates at times, so it might elect to do so again. So far this year, the company has released two "out-of-band" updates, both for IE. Microsoft's announcement of the security bug may be found at <http://www.microsoft.com/technet/security/advisory/2286198.msp>.

---

*Bytes in Brief*<sup>™</sup> 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.

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

Privacy by  **SafeSubscribe**<sup>SM</sup>  
For Email Marketing you can trust

---

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