

# {bytes in brief}

LAW AND TECHNOLOGY NEWS MONTHLY

EDITORS: Sharon D. Nelson, Esq. and John W. Simek  
ASSOCIATE EDITOR: Nicole Kolinski EDITOR EMERITUS: G. V. Nelson



© 2009 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

## Issue 143 - April 2009

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

---

### CVS SETTLES PATIENT INFO INVESTIGATION FOR \$2.25 MILLION

On February 18th, the Federal Trade Commission (FTC) announced that CVS Caremark Corp. would pay \$2.25 million to settle allegations that its pharmacy workers did not properly dispose of items containing personal information. The items included pill bottles, medication instruction sheets, computer order forms, payroll information, job applications, credit card numbers, and insurance information. The forms contained personal information such as Social Security numbers or account numbers. The FTC and the Department of Health and Human Services (HHS) alleged that items were left outside in open trash bins and that CVS did not have a proper policy for disposing of such information. In addition to the fine, CVS agreed to comply with privacy rules and be subject to independent monitoring for 20 years. HHS will monitor CVS for the next three years to ensure employees are properly trained and patient information is protected. Employees who do not follow the proper disposal rules will be sanctioned. CVS was not aware of any harm to consumers, but said it settled to avoid the time and expense of litigation. The FTC press release may be found at <http://www.ftc.gov/opa/2009/02/cvs.shtm>

---

### CRIMEWARE TRACKING SERVICE ATTACKED BY CYBERCRIMINALS

On February 14th, the Zeus tracker, a newly launched crimeware tracking service, was hit with a distributed denial of service (DDoS) attack, thus proving the usefulness of the service. Unlike other crimeware trackers, the Zeus tracker operates in real time, keeping track of known Zeus hosting locations used by cybercriminals. The real time feature allows the web community to take action against known Zeus IP addresses. As the tracker allows active crimeware campaigns to be stopped in their tracks, it is easy to understand why it was attacked. The story may be found at <http://blogs.zdnet.com/security/?p=2596>

---

### NEW SERVICE TO REVEAL ANONYMOUS CALLERS

On February 17th, a new service called TrapCall was released by TelTech System that reveals phone numbers, and in some cases, names and addresses, of blocked Caller IDs. To use the program, a user must reprogram his or her cell phone to send all missed and unanswered calls to TrapCall. When a blocked or restricted number appears, the user presses a button that re-routes the call to TrapCall's toll free line, where the caller's information is obtained and sent back to the original recipient. The basic service is free and works on any standard cellular phone that is registered to a carrier. The service also includes the option of blacklisting unwelcome callers. For a fee, premium features include recording incoming calls (which may be illegal depending on state law), voicemail transcriptions via e-mail and text message, and the ability to listen to voicemail online. While it may be useful, the service raises privacy concerns, particularly in cases of domestic violence, where abusers could use the service to locate victims. More information may be found at <http://www.trapcall.com/learnmore>

---

### COMPUTERS DISAPPEAR FROM NUCLEAR LAB

On February 11th, the Project on Government Oversight, a nonprofit group that exposes government misconduct,

announced that government officials are investigating the disappearance of sixty-seven computers from the Los Alamos nuclear weapons lab. While the total number of computers disappeared over a longer period of time, thirteen disappeared in the last year, including three stolen from a scientist's home last month. The security risk of the missing computers was unknown, but the lab was rebuked for treating the situation as property management rather than a security risk. The story may be found at <http://www.pogo.org/pogo-files/alerts/nuclear-security-safety/nss-lanl-20090211.html>

---

### **ELECTRONIC EVIDENCE FIRM REPRIMANDED FOR INTERNAL DIGITAL SEARCH**

On February 14th, the Associated Press reported that electronic evidence firm Guidance Software, which handles its clients' electronic data on a regular basis, did not handle its own data properly. Guidance's mishandling of its own evidence led an arbitrator to accuse the company of gross negligence and proceeding in bad faith. The dispute stemmed from a wrongful termination suit filed by a former employee, in which both sides were ordered to conduct discovery. The former employee believed that Guidance's e-mail production was incomplete, and her theory was confirmed when a former colleague produced e-mails that Guidance had not. The arbitrator was annoyed by Guidance's conduct, especially considering its area of expertise. As a sanction, Guidance was ordered to pay for the former employee's expert witnesses, travel costs, and costs of rescheduling the trial. In addition, the arbitrator ordered Guidance to search its backups, despite arguments by the company that it was unduly burdensome. The story may be found at [http://biz.yahoo.com/ap/090214/tec\\_guidance\\_s\\_missing\\_evidence.html?.v=2](http://biz.yahoo.com/ap/090214/tec_guidance_s_missing_evidence.html?.v=2)

---

### **STUDY FINDS EX-EMPLOYEES ADMIT TO STEALING COMPANY DATA**

On February 23rd, the Ponemon Institute released the results of a survey that found six out of ten employees fired in the past year stole company data before leaving. Seventy nine percent admitted that their former employer did not allow them to have the information. Types of information stolen included: e-mail lists, non-financial business information, customer information, including contact lists, employee records, and financial information. The study also looked at the methods used to transport the data outside the office: 61 percent took the data as paper documents or hard files, 53 percent burned the information onto a CD or DVD, and 42 percent downloaded it onto a USB memory stick. The author of the study attributed the losses to companies not doing enough to protect their data. The study shows that companies need to better protect their proprietary information. The story may be found at <http://www.cbc.ca/technology/story/2009/02/23/tech-steal-data.html?ref=rss>

---

### **JUDGE ORDERS DEFENDANT TO DE-ENCRYPT A LAPTOP**

On February 26th, a U.S. District Judge ordered a defendant to decrypt his hard drive so prosecutors can view the information, holding that doing so did not violate the defendant's Fifth Amendment right against self incrimination. In 2006, Sebastian Boucher was arrested for possession of child pornography incident to a border search when he re-entered the country from Canada. The border agents initially accessed Boucher's hard drive and found child pornography, but later were unable to access the hard drive because it was encrypted. Boucher claimed that forcing him to turn over his password violated his Fifth Amendment right against self incrimination. U.S. Magistrate Judge Jerome Niedermeier agreed, and in November 2007 ruled that Boucher did not have to turn over his password. The case turned on whether forcing someone to turn over his password is "testimonial." U.S. District Judge William Sessions found that entering a password is not testimonial because Boucher entering his password would not be used by the government as evidence to link Boucher to the computer, as the government could prove Boucher's link to the computer in other ways. The story may be found at [http://news.cnet.com/8301-13578\\_3-10172866-38.html](http://news.cnet.com/8301-13578_3-10172866-38.html)

---

### **HEARTLAND UNDER INVESTIGATION AFTER DATA THEFT**

On February 22nd, Heartland Payment Systems admitted in a conference call that it was under investigation by numerous government agencies, including the Federal Trade Commission, the Securities and Exchange Commission, Department of Justice, and U.S. Department of the Treasury's Office of the Comptroller of the Currency, for a data breach announced in January. The breach occurred when a hacker broke into Heartland's

systems and stole unencrypted data from credit card transactions. While a Heartland representative could not say why it was being investigated by the SEC, it could be connected to insider stock trading that took place after the company found out about the breach. The Treasury Department could be involved as the breach may be part of a larger global scheme. The story may be found at [http://www.pcworld.com/article/160264/sec\\_ftc\\_investigating\\_heartland\\_after\\_data\\_theft.html?t k=rss\\_news](http://www.pcworld.com/article/160264/sec_ftc_investigating_heartland_after_data_theft.html?t k=rss_news)

---

## **OBAMA'S BUDGET INCREASES CYBERSECURITY SPENDING, PROPOSES WIRELESS SPECTRUM FEE TO ALLEVIATE DEFICIT**

On February 26th, President Obama announced his 2010 budget, which allocates \$355 million for operations of the National Cyber Security Division and the Comprehensive National Cybersecurity Initiative. The money will largely be used to secure the nation's information networks, but \$36 million will be allocated to improve surveillance technologies that detect advanced biological threats. The budget proposal also indicates the administration's intention to enhance the intelligence community's role in overseeing cybersecurity. To help alleviate the massive national deficit, a new wireless spectrum fee is included in the budget to the bane of wireless providers. The fees would start at \$50 million in 2009 and increase to \$200 million in 2010. The fees would continue to gradually increase, generating an estimated total of \$4.8 billion over the next decade. A story about the wireless spectrum fee may be found at <http://uk.reuters.com/article/americasRegulatoryNes/idUKN2617163420090226>

Information on DHS spending in the budget may be found at [http://www.whitehouse.gov/omb/assets/fy2010\\_new\\_era/Department\\_of\\_Homeland\\_Security.pdf](http://www.whitehouse.gov/omb/assets/fy2010_new_era/Department_of_Homeland_Security.pdf)

---

## **FACEBOOK TO CREATE BILL OF RIGHTS AFTER TERMS OF USE SCANDAL**

On February 26th, after a change in the site's terms of use that caused an uproar, Facebook announced that it would release two new documents to govern the site. The documents will be reviewed by Facebook users before going into effect. According to its press release, the two documents will be "The Facebook Principles, a set of values that will guide the development of the service, and Statement of Rights and Responsibilities that make clear Facebook's and users' commitments related to the service." Facebook also stated that there would be a 30-day discussion period for amendments to the two documents. Facebook CEO Mark Zuckerberg explained that the new developments showed that Facebook trusts its users, and that the site was committed to openness and transparency. Zuckerberg also stated that these developments had been in the works for some time, but were fast-tracked by the terms of use controversy. The Facebook press release may be found at <http://www.facebook.com/press/releases.php?p=85587>

---

## **STUDY FINDS U.S. COULD OBTAIN BILLIONS FROM ONLINE GAMBLING**

On February 26th, PricewaterhouseCoopers released a study that indicated the U.S. could raise \$52 billion if it legalizes and taxes online gambling. Current law bans online gambling altogether. It is hoped that with the increasing national deficit, the study will influence Congress to repeal the law. Online gambling associations are pushing for the law not only for their own profits, but because the entire industry would benefit from regulation. Despite its illegality, the online gambling industry has grown in the United States since 2007. The story may be found at <http://www.reuters.com/article/technologyNews/idUSTRE51O85J20090226>

---

## **MICROSOFT SUES TOMTOM FOR PATENT INFRINGEMENT**

On February 25th, Microsoft announced that it had filed two patent infringement lawsuits against GPS company TomTom in the U.S. District Court for the District of Washington and the International Trade Commission. Microsoft is alleging infringement of eight patents, five which have to do with car navigation systems, and the rest with file management technologies. Microsoft stated that it attempted to enter into licensing talks with TomTom, but that TomTom was not interested. Other GPS companies have similar licenses with Microsoft. Microsoft said that it filed both lawsuits simultaneously to recoup past losses, stop infringing activity, and minimize potential future losses. Microsoft's statement may be found at <http://www.microsoft.com/presspass/press/2009/feb09/02-25statement.mspx>

The District Court complaint may be found at [http://news.cnet.com/i/ne/pg/fd\\_2009/Complaint.pdf](http://news.cnet.com/i/ne/pg/fd_2009/Complaint.pdf)

The ITC complaint may be found at [http://news.cnet.com/i/ne/pg/fd\\_2009/2009.02.25\\_Public\\_ITC\\_Complaint\\_MSFT\\_TomTom.pdf](http://news.cnet.com/i/ne/pg/fd_2009/2009.02.25_Public_ITC_Complaint_MSFT_TomTom.pdf)

Last minute update: It was announced on March 30th that the case had settled. TomTom is paying Microsoft an undisclosed amount as part of the deal. Further information may be found at <http://blogs.zdnet.com/microsoft/?p=2398>

---

## **U.S. SUPREME COURT RULES FOR AT&T IN ANTITRUST LAWSUIT**

On February 25th, the U.S. Supreme Court unanimously ruled in favor of Pacific Bell Telephone company, a subsidiary of AT&T accused of anti-competitive practices in the high speed Internet market. The plaintiffs buy high-speed service from AT&T, combine it with other services and then sell Internet-access services that compete with AT&T. The lawsuit alleged that AT&T was conducting a "price squeeze," meaning that it was selling at higher rates to plaintiff buyers to try to squeeze them out. The U.S. Circuit Court in San Francisco found that AT&T was setting its wholesale prices so high that the ISPs could not compete with the low prices AT&T charged in the retail market. The U.S. Supreme Court reversed, and found that the suit could not be brought under a section of the antitrust law when the defendant has no duty to deal with the plaintiffs at wholesale. Chief Justice John Roberts wrote the majority opinion, and explained that the court would not create a new cause of action that did not exist under current law. The decision may be found at <http://www.law.cornell.edu/supct/html/07-512.ZS.html>

---

## **CENTER INTRODUCES TOP 20 CYBERSECURITY DEFENSES**

On February 23rd, federal agencies and private organizations introduced the Consensus Audit Guidelines, the top twenty cybersecurity defenses to protect against cyberattacks. The guidelines are security controls that organizations should take to defend computer systems. The practices include: inventories of hardware and software, secure configurations for programs, security audit logs, anti-malware protections, and numerous other things to protect against cyberattacks. The guidelines now face a six-step review process: 30 days of public comment, a pilot test, a CIO Council review, an inspector general review, control automation workshops, and comparison with existing audit regulations. The report may be found at [http://www.csis.org/component/option,com\\_csis\\_pubs/task,view/id,5300/type,1/](http://www.csis.org/component/option,com_csis_pubs/task,view/id,5300/type,1/)

---

## **PROPOSED INTERNET LAW WANTS ISPS & WI-FI TO KEEP LOGS FOR POLICE**

On February 19th, legislation was introduced by Republican Senator John Cornyn that would require Internet Service Providers and Wi-Fi operators to keep user records for two years to help police investigations. One bill was introduced in each house of Congress entitled "Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act," or Internet Safety Act. Both use the same language, most relevantly that "A provider of an electronic communication service or remote computing service shall retain for a period of at least two years all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that user." Retaining records for law enforcement purposes is a notion that appeals to both Democrats and Republicans. Privacy groups will likely rebuke the retention of data for such a long period of time. The Senate Bill may be found at <http://thomas.loc.gov/cgi-bin/bdquery/z?d111:s.00436>:

---

## **COURT DISMISSES CLAIMS AFTER PLAINTIFF DISCARDS LAPTOP**

On February 13th, in an advertising dispute, the U.S. District Court for the Middle District of Pennsylvania sanctioned the Plaintiff, Nancy Kvitka, for discarding a laptop by dismissing her claims and imposing an adverse inference instruction against her for the Defendant's cross claims. In the litigation, Defendant requested that Kvitka preserve her computer and all e-mails. Despite the preservation instructions, Kvitka discarded and replaced her laptop due to supposed problems with the computer, and did not transfer any files from the old computer to the new

one. The court first determined that the evidence showed that Kvitka intentionally discarded the laptop despite instructions not to. The court laid out several key considerations to determine sanctions for such conduct, including: the accused party's degree of fault, the degree of resulting prejudice, the propriety of sanctions in light of fairness, and the future deterrent effect. The court determined that Kvitka acted in bad faith and that dismissal of her claims was warranted because the damage to Defendant's case could not be repaired with lesser sanctions. The court also allowed Defendant to pursue its cross-claims, with an adverse inference instruction against Kvitka to be considered by the jury for those claims. The opinion may be found at [http://www.ediscoverylaw.com/uploads/file/Westlaw\\_Document\\_Kvitka.doc](http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_Kvitka.doc)

---

### **NJ COURT FINDS E-MAIL SENT FROM COMPANY COMPUTER WAIVES PRIVILEGE**

On February 5th, a New Jersey Superior Court held that e-mails sent from an employee's personal e-mail account to her lawyer on her employer's computer during business hours are not protected by attorney-client privilege. The court's decision turned on whether the employer had a clear policy that would notify the employee that e-mails sent on the employer's system are not private. The defendant, a home health care company, had an employee handbook that was distributed to staff and available on company computers. The handbook included a warning that any e-mails were considered part of the company's business records and were not to be considered private by any employee. The court found that because of the warning, the employee sent the e-mails with knowledge that they would not be private, thus waiving attorney client privilege. The opinion may be found at <http://www.judiciary.state.nj.us/decisions/Stengart090305.pdf>

---

### **COURT DENIES COST SHIFTING AFTER CONSIDERING ZUBULAKE FACTORS**

On February 19th, the U.S. District Court for the Eastern District of Texas refused to shift the cost of electronic discovery to the requesting party after considering the seven-factor test laid out in the infamous Zubulake decisions. In a prior decision, the court ordered that the producing party produce the electronic documents in TIFF format with Optical Character Recognition. The producing party claimed that the cost of this production should be shifted to the requesting party, as it would cost over \$200,000 and only benefit the requesting party. The court considered the seven-factors for cost-shifting laid out in Zubulake v. UBS Warburg, which are: 1) the extent to which the request was specifically tailored to discover relevant information; 2) the availability of such information from other sources; 3) the total cost of production, when compared to the amount in controversy; 4) the total cost of production, when compared to the resources available to each party; 5) the relative ability of each party to control costs and the incentive to do so; 6) the importance of the issues at stake in the litigation; and 7) the relative benefits to the parties of obtaining the information. The court first noted that the producing party did not contend that the information requested was not relevant or likely to lead to the discovery of admissible information. The court also found that defendants did not show that the documents were available from other sources, and that OCR was valuable to both parties, as it decreases the time and effort of searching documents. In light of the Zubulake factors, the court concluded that cost shifting was not warranted. The decision may be found at [http://www.ediscoverylaw.com/uploads/file/Westlaw\\_Document\\_Proctor%20&%20Gamble.doc](http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_Proctor%20&%20Gamble.doc)

---

### **AWAY MESSAGE USED TO OPPOSE SEXUAL MOLESTATION CHARGES**

On February 26th, a California appellate court upheld the conviction of Earl Eugene Cannedy for oral copulation over his objection that the away message of one of his victims exculpated him for the crime. Cannedy was accused of oral copulation of his wife's 17-year-old sister, and his 13-year-old stepdaughter, which resulted in the stepdaughter moving in with her father. Cannedy argued that an "away message" put up on AOL Instant Messenger by the stepdaughter exculpated him. The message stated that the stepdaughter was moving to her father's "because everyone hates me and I don't want to put up with it anymore. Everything that you heard is not true. I just made it up so I could get away from it all." The message was written down by one of the stepdaughter's friends, who was willing to testify at trial. Cannedy argued that only a person with the stepdaughter's password could have typed the message, but the judge found problems with the message's authenticity, as passwords are not always kept secret. Cannedy was convicted by a jury and sentenced to two years in prison, on top of an earlier sentence of 10 years and 8 months in prison for a previous related case. The California Court of Appeals for the Fourth District affirmed the conviction. The court found that Cannedy was not denied his Sixth Amendment right to

present a defense because there was no evidence that the message was written by the stepdaughter. The story may be found at [http://news.cnet.com/8301-13578\\_3-10190451-38.html](http://news.cnet.com/8301-13578_3-10190451-38.html)

---

## **PRESIDENT OBAMA NAMES TECHNOLOGY OFFICER**

On March 5th, President Obama named Vivek Kundra, chief technology officer for the District of Columbia, the new federal Chief Information Officer (CIO). President Obama created the office to ensure that the government was using its technology efficiently. The primary responsibilities of the CIO will be to oversee how government agencies use information technology and government technology spending. In addition, the CIO will ensure that the various government networks work together without compromising privacy or security. President Obama stated that "Vivek Kundra will bring a depth of experience in the technology arena and a commitment to lowering the cost of government operations to this position. I have directed him to work to ensure that we are using the spirit of American innovation and the power of technology to improve performance and lower the cost of government operations. As Chief Information Officer, he will play a key role in making sure our government is running in the most secure, open, and efficient way possible." The White House press release may be found at [http://www.whitehouse.gov/the\\_press\\_office/President-Obama-Names-Vivek-Kundra-Chief-Information-Officer/](http://www.whitehouse.gov/the_press_office/President-Obama-Names-Vivek-Kundra-Chief-Information-Officer/)

---

## **SHERIFF SUES CRAIGSLIST OVER SEX ADS**

On March 5th, Cook County, Illinois Sheriff Tom Dart filed suit against Craigslist, accusing the website of promoting prostitution. Dart claims that the website ignores obviously illegal ads posted on its website while warning that solicitation of prostitution is prohibited. The Sheriff is requesting that a federal judge shut down the "erotic services" section of the website, claiming that it is equivalent to somebody working with a pimp to advertise the women working for the pimp. Craigslist was previously sued for its sexually explicit ads, and reached an agreement in November with attorneys general from several states to regulate the ads. Dart explains that his lawsuit is different from previous suits because the suit alleges that the purpose of the "erotic services" section is to facilitate prostitution. Previous suits only generally opposed the ads. The Cook County Sheriff press release may be found at [http://www.cookcountysheriff.org/press\\_page/press\\_craigslistProstitution\\_03\\_05\\_2009.html](http://www.cookcountysheriff.org/press_page/press_craigslistProstitution_03_05_2009.html)

---

## **JUDGE ALLOWS REPORTER TO SEND TWITTER UPDATES FROM COURTROOM**

On March 6th, the Associated Press reported that a federal judge would allow a reporter to send Twitter updates from the courtroom. Lawyers expressed concern that jurors could access the reporter's updates, but U.S. District Judge Thomas Marten said that jurors are always told to avoid reports of the trial, regardless of format. The reporter, Ron Sylvester of the Wichita Eagle, had been using Twitter to send updates from state court, but this was the first federal trial where he was allowed to Tweet. Twitter updates, called "tweets," are limited to 140 characters and can be sent and received on a cell phone or computer. Reporters believe that Twittering in the courtroom would make the courts more accessible to the public. One of Sylvester's subscribers in the federal racketeering trial is one of the defendant's fathers, who cannot make it to the trial. The story may be found at [http://www.siliconvalley.com/latestheadlines/ci\\_11851007](http://www.siliconvalley.com/latestheadlines/ci_11851007)

---

## **COURTS DECIDE WHETHER ANONYMOUS POSTERS SHOULD BE REVEALED**

On February 28th, the Maryland Court of Appeals held that a website does not have to disclose the identities of anonymous posters in defamation lawsuits. The decision reversed a lower court ruling that online forum NewsZap.com had to disclose the identities of forum participants who posted about the cleanliness of a Dunkin' Donuts shop in 2006. Maryland businessman Zebulon J. Brodie filed a defamation lawsuit over the comments. In finding that the posters' identities did not have to be disclosed, the court laid out a test for judges to use to balance the First Amendment interests of anonymous speech on the Internet with the opportunity to seek redress for alleged defamation. The test required a plaintiff claiming defamation to try to notify the poster, identify the exact statements made by the poster, and show how those comments caused damage to the plaintiff. On March 4th, however, a California judge threatened to turn over the identities of Comcast customers who allegedly made libelous statements about champagne company Korbel, if the posters did not file a legal challenge. The lawsuit

dealt with negative postings on Craigslist about Korbel, which allegedly damaged the company's reputation. The ruling required Comcast to alert the subscribers to the lawsuit within one week, after which the subscribers will have one month to contest the order and protect their identities. The Korbel story may be found at <http://www.pressdemocrat.com/article/20090305/ARTICLES/903040184/1350?Title=Judge-Korbel-may-get-IDs-of-anonymous-critics> The Maryland opinion may be found at <http://mdcourts.gov/opinions/coa/2009/63a08.pdf>

---

### **SURVEY FINDS 1/3 PEOPLE USE THE SAME PASSWORD FOR ALL WEBSITES**

On March 10th, security firm Sophos released a survey that indicated 33% of web users use the same password for every website. While easier on the memory, using the same password is risky, as it is also easier for hackers to access all the user's accounts. Only 19% of those surveyed never use the same password twice, while 48% use a few different passwords. In addition to using multiple passwords, many users overlook the importance of using "strong" passwords, which are passwords that cannot easily be hacked. One way to create a strong password, according to Graham Cluley, senior technology consultant at Sophos, is to choose a sentence and take the first letter of every word as your password, and to use the number "4" instead of the word "for." The story may be found at <http://www.sophos.com/pressoffice/news/articles/2009/03/password-security.html>

---

### **D.C. TECH OFFICIAL CHARGED WITH BRIBERY**

On March 12th, the Federal Bureau of Investigation arrested the District of Columbia's top information security official, Yusuf Acar, on bribery charges. Acar is being held without bail, partially because it is unclear whether he can still access D.C.'s IT systems. Acar had access to personnel data and other confidential information for his job. The FBI alleged that other D.C. officials were involved in the scam, which dealt with security software, raising serious issues about the security of D.C.'s IT systems. Whether any data has been compromised can only be determined through computer forensic investigation, and FBI officials did not say whether any data had been compromised. The FBI press release may be found at <http://washingtondc.fbi.gov/dojpressrel/pressrel09/wfo031209.htm>

---

### **TELECOM COMPANIES OPPOSE SET INTERNET SPEEDS IN STIMULUS PACKAGE**

On March 19th, Reuters reported that telecommunications companies are opposing a provision in President Obama's stimulus package that would require the companies to provide a super-fast Internet speed to win \$7.2 billion in broadband funds. Telecom companies were concerned that the cost of providing the fast service would be too high and decrease the companies' profits. Those in support of increased speeds blamed the lack of government standards for the United States lagging behind other industrialized nations in average broadband speed. The Federal Communications Commission's currently defined broadband speed is 768 Kilobits per second, which is slow by most standards. The story may be found at <http://www.reuters.com/article/internetNews/idUSTRE52I60120090319>

---

### **PRIVACY GROUP URGES FTC TO INVESTIGATE GOOGLE'S CLOUD- COMPUTING**

On March 17th, the Electronic Privacy Information Center (EPIC) filed a Federal Trade Commission (FTC) complaint against Google, asking the FTC to investigate Google's cloud- computing services to ensure that they are as secure as Google alleges. The complaint stemmed out of an incident earlier in March where a Google Docs software bug exposed private documents, which according to Google only affected 0.5% of documents stored online. EPIC is concerned that Google advertises that the documents remain private and secure, but that Google had multiple security breaches. EPIC also requested other forms of relief, namely that Google be forced to make its security policies more transparent, and that Google contribute \$5 million to a privacy research fund. The EPIC complaint may be found at <http://epic.org/privacy/cloudcomputing/google/ftc031709.pdf>

---

## **DISCOVERY FILES PATENT INFRINGEMENT SUIT AGAINST AMAZON**

On March 17th, Discovery Communications, parent company over the Discovery Channel and Animal Planet, filed suit against Amazon.com alleging that Amazon's electronic book reader, Kindle, violates a Discovery patent. The patent was issued to Discovery in 2007, and is for an Electronic Book Security and Copyright Protection System. According to the lawsuit, the technology "provides for secure distribution of electronic text and graphics to subscribers and secure storage." The lawsuit was filed in U.S. District Court in Delaware, and Discovery seeks unspecified money damages. The Discovery press release, with a link to the complaint, may be found at <http://corporate.discovery.com/discovery-news/discovery-communications-files-patent-infringement/>

---

## **JURORS USING TECHNOLOGY TO CONDUCT OUTSIDE RESEARCH**

On March 18th, the New York Times reported on the impact technology can have on trials, from jurors sending updates about the trial through Twitter or text message, to jurors conducting outside research on smartphones, which can result in a so-called "Google mistrial." Jurors are not supposed to obtain outside information about a trial, as their inquiries are limited to the evidence that the judge deems admissible. In early March, a juror on a Florida federal drug trial admitted that he had conducted outside research on the case, including research on evidence excluded by the judge. The judge was going to expel the juror and move on with the case, until eight other jurors admitted to conducting outside research as well. At that point, the judge had no choice but to declare a mistrial, throwing away eight weeks of work by the prosecution and defense attorneys. This type of research causes serious problems for the legal system, as it ignores years of evidence jurisprudence. Google and other resources like Wikipedia make answers to jurors' questions a click away, something courts have never dealt with before the advent of new technology. Another important issue arose in a recent Arkansas case where a juror allegedly sent Twitter messages during a trial. The judge did not declare a mistrial, but the losing side appealed the \$12 million judgment based on the messages. The juror claims that he did not send any messages until after the trial was over. These issues may indicate that courts should reevaluate jury instructions and what electronic devices are allowed in the courtroom. The story may be found at <http://www.nytimes.com/2009/03/18/us/18juries.html?partner=rss&emc=rss>

---

## **CYBERSQUATTING CASES HIT RECORD HIGH IN 2008**

On March 15th, the World Intellectual Property Organization (WIPO) announced that there were a record number of cybersquatting cases filed in 2008. There were 2,329 complaints filed through the Uniform Domain Name Dispute Resolution Policy (UDRP), a quick and cost-effective method of resolution offered by the organization. The number of cases increased 8% from 2007. The cases involved a variety of business sectors, with complaints arising most often in pharmaceuticals, followed by banking and finance, Internet and telecommunications, retail, and food, beverages, and restaurants. Cybersquatting disputes will most likely continue to increase, as the Internet Corporation for Assigned Names and Numbers (ICANN) is set to release new series of suffixes to Internet addresses, providing more room for imitation. The WIPO press release may be found at [http://www.wipo.int/pressroom/en/articles/2009/article\\_0005.html](http://www.wipo.int/pressroom/en/articles/2009/article_0005.html)

---

## **SECOND LIFE TO FLAG ADULT CONTENT, VERIFY AGE**

On March 12th, Second Life, a virtual world interactive website, announced that it would be making changes to better identify the adult content on its website. The new policy will require users to flag adult content, and the content will only be accessible in an adults-only area of the website. Users who want to enter the adults-only area of the website will have to provide age verification, perhaps through credit cards, though the actual method of verification has not been decided. The changes were not intended to rid the site of adult content, but to make the adult content available only to those who want to access it. The site is allowing for a comment period of six weeks so users can have input on how the policies should change, including what the definition of "adult content" should be. The Second Life blog post may be found at <https://blogs.secondlife.com/community/community/blog/2009/03/12/upcoming-changes-for-adult-content>

---

## GOOGLE INTRODUCES VOICEMAIL AND BEHAVIORAL ADS

On March 11th, Google announced two new developments: Google Voice, which will translate voicemail messages into e-mail messages, and a new form of advertising. Google Voice is based on the technology of GrandCentral Communications, which Google acquired in 2007. The technology uses voice recognition technology that automatically transcribes voicemail into text. Once transcribed, the messages may be forwarded as an e-mail or SMS-text message to a person's e-mail inbox. The program is available to existing GrandCentral users, and will be available to the general public in a few weeks. Another new development was a way to "make advertising more interesting," by showing ads to people based on their habits. Previously, ads were based on interests at a specific moment (i.e. what was typed into Google searches). The new advertising is, according to Google "interest based," meaning it is based on habits over time rather than at the moment. For those who do not approve of the changes, Google will be providing a tool called Ads Preference Manager that allows a user to edit their preferences for advertising and opt out of the new program. The Google blog post on Google Voice may be found at <http://googleblog.blogspot.com/2009/03/here-comes-google-voice.html>

The Google blog post about the advertising may be found at <http://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html>

---


*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.

Subscribe to *Bytes in Brief*

Email:

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

---

Copyright © 2009 Sensei Enterprises, Inc. All rights reserved.