

# { 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



© 2008 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

## Issue 137 - October 2008

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

---

### **SURVEY FINDS LITIGATION TOO COSTLY BECAUSE OF E-DISCOVERY**

On September 9th, the Institute for the Advancement of the American Legal System (IAALS) and the American College of Trial Lawyers (ACTL) Task Force on Discovery released the results of a survey of trial lawyers from across the country. The survey called electronic discovery a “morass,” with 87% of lawyers stating that e-discovery is too costly. The survey also found that the excessive cost of discovery is forcing settlements, instead having settlements take place on the merits. Lawyers also believe that judges do not do enough to control excessive discovery, especially with costly e-discovery, with 89% of lawyers saying judges needed to assume a greater leadership role.

The ABA Journal article on the survey, including a link to the report, may be found at [http://www.abajournal.com/news/litigation\\_too\\_costly\\_e\\_discovery\\_a\\_morass\\_trial\\_lawyers\\_say/print/](http://www.abajournal.com/news/litigation_too_costly_e_discovery_a_morass_trial_lawyers_say/print/)

---

### **FCC AND COMCAST BUTT HEADS, COMCAST LIMITS BANDWIDTH FOR USERS**

On August 20th, the Federal Communications Commission (FCC) released a memorandum opinion and order stating that Comcast violated network management practices. The FCC found that Comcast’s interference was “invasive and widespread,” and was not limited to times when the network was congested. Further, the FCC ordered Comcast to stop its discriminatory practices and submit a compliance plan within 30 days. In response, on September 4th, news sources reported that Comcast had appealed the FCC decision. Comcast stated that it still intended to comply with the FCC order, but believed that the order had no legal basis and the findings were not justified. Also in response, on August 28th, Comcast announced an amendment to its monthly data usage threshold. Starting October 1st, Comcast will limit users to 250GB of bandwidth per month. If a user goes over the limit, Comcast will contact the customer, and suspend their account if they do not curb their use. Comcast claimed that the limit would affect less than 1% of its customers. To reach the limit a user would have to send 50 million e-mails, download 62,500 songs, or download 125 standard definition movies.

The FCC order may be found at [http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-08-183A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf)

Comcast’s new policy may be found at <http://www.comcast.net/terms/network/amendment/>

A news story on the appeal may be found at [http://news.yahoo.com/s/nm/20080904/wr\\_nm/comcast\\_fcc\\_dc](http://news.yahoo.com/s/nm/20080904/wr_nm/comcast_fcc_dc)

---

### **JUDGE HOLDS LAW PROTECTS COMMENTERS ON NEWSPAPER WEBSITE**

On September 3rd, a Montana state court judge issued an order quashing the subpoena that sought information to

identify anonymous people who post on The Billings Gazette website. The case arose from an election dispute where losing candidate Russ Doty sued winning candidate Brad Molnar for libel and slander. Doty requested the subpoenas to learn the identity of the anonymous posters so he could use them as witnesses to show the damage to his reputation. Doty also believed some of the posts came from Molnar himself, and wanted to use the IP address information to identify him. The judge held that the state's Media Confidentiality Act, also known as a shield law, protected the anonymous posters. Under the act, any information obtained or prepared by a news agency is protected. The judge held that this included posts on the newspaper message board along with printed stories. The judge also doubted that anonymous postings would have much credibility in proving the libel and slander claims.

The story from The Billings Gazette may be found at <http://www.billingsgazette.net/articles/2008/09/03/news/local/22-doty.txt>

## **AIRPORTS LOSING MORE THAN 12,000 LAPTOPS PER WEEK**

On June 30th, a Ponemon Institute study sponsored by Dell entitled "Airport Insecurity: The Case of Missing & Lost Laptops" was released. The study indicated that business travelers are losing more than 12,000 laptops per week at major U.S. airports, with only one third of the laptops reclaimed. The study also polled business travelers, and discovered that 53% of respondents said their laptop contained confidential or sensitive information, with 65% of those respondents not taking steps to secure their laptops. The results were disturbing, because the loss of these laptops could result in data breaches for many companies. The airports with the highest number of lost, missing or stolen laptops included Los Angeles International, Miami International, Kennedy International, and Chicago O'Hare. The busiest airport in the United States, Atlanta's Hartsfield-Jackson International, ended up tied for eighth place with Washington's Reagan National.

The study may be found at [http://www.dell.com/downloads/global/services/dell\\_lost\\_laptop\\_study.pdf](http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf)

## **JUDGE ORDERS ATTORNEYS TO PAY FOR DISCOVERY DISPUTE**

On August 7th, U.S. District Judge Thomas Thrash refereed a discovery dispute in a case filed by CBT Flint Partners accusing Cisco IronPort of patent infringement related to e-mail certification services and billing. In April, CBT's attorneys filed an emergency motion to compel discovery that contained 343 pages of exhibits claiming Cisco had tried to delay discovery. By mid-May and before the end of discovery, Cisco had produced more than 1.4 million documents from electronic searches of 102 search terms chosen by CBT. Judge Thrash found CBT's complaints unwarranted, that CBT did not effectively confer with Cisco about discovery, and CBT wasted the court's time by forcing it to review the whole record. The court explained that CBT's document requests were so broad they resulted in an overbroad production. Had CBT met with Cisco about the problems, the court said that the whole dispute would have been avoided. As a sanction, Judge Thrash ordered CBT to pay 75% of the attorneys' fees for Cisco for billings that stemmed from the discovery dispute.

The decision may be found at <http://www.dailyreportonline.com/Editorial/PDF/PDF%20Archive/Cisco-order2-081908.pdf>

## **COURT DISMISSES COPYRIGHT SUIT UNDER SAFE HARBOR EXCEPTION**

On August 27th, U.S. District Judge Howard Lloyd granted summary judgment in favor of Internet video site Veoh in a copyright infringement action. Io Group, Inc. sued Veoh to stop users of the Veoh site from uploading unauthorized clips of Io's adult films. Judge Lloyd found that Veoh qualified for "safe harbor" protection under the Digital Millennium Copyright Act (DMCA) because Veoh worked to protect copyright owners. Veoh had recently barred all adult sexual content and removed the infringing videos before the suit was filed. The court rejected Io's claim that Veoh should prescreen videos for copyrighted content because a review of every file was not possible. The court also found that Io should have provided Veoh with notification of the infringing videos before filing suit.

The decision may be found at  
[http://www.eff.org/files/lo%20v.%20Veah%20\(d%20ct\).pdf](http://www.eff.org/files/lo%20v.%20Veah%20(d%20ct).pdf)

---

## **BLOGGER ARRESTED FOR SHARING MUSIC ONLINE**

On August 24th, FBI agents arrested 27-year-old blogger Kevin Cogill for posting several songs from the new Guns N' Roses album on his blog before the album was released. Cogill was charged with a felony for distributing copyrighted works on computer networks before their release, for which he could face up to three years in prison and up to \$250,000 in fines. Cogill was released on \$10,000 bond, with a preliminary hearing scheduled for September 17th, and the arraignment for September 22nd. The arrest is one of the first indications of the music industry going beyond the large-scale piracy rings and attacking individual infringers.

The LA Times story may be found at  
<http://www.latimes.com/business/la-fi-music29-2008aug29.0.7317091.full.story>

---

## **BANK DATA SOLD ON EBAY**

On August 26th, BBC News indicated that a computer with bank data from the Royal Bank of Scotland and two other companies was sold on eBay for about \$137. The purchaser was IT manager Andrew Chapman, who bought the computer with no idea that the information was on the hard drive. After he discovered the information, he reported the computer to the police. Among the information included on the computer were account details, signatures, phone numbers, and mothers' maiden names. The computer belonged to MailSource UK, a subsidiary of Graphic Data, an archiving company that stores the information for the Royal Bank of Scotland, Natwest, and American Express. Graphic Data launched an investigation to see how the information was removed, while eBay was looking into how the computer got on its site.

The story may be found at  
[http://news.bbc.co.uk/2/hi/uk\\_news/7581540.stm](http://news.bbc.co.uk/2/hi/uk_news/7581540.stm)

---

## **MICROSOFT PROPOSES DIGITAL PLAYGROUNDS TO PROTECT KIDS ONLINE**

On September 3rd, Microsoft announced a new initiative to keep children safe online – a “digital playground,” or a website where users must provide age credentials before entering. Microsoft released the idea in a paper as part of its “End to End Trust” Initiative, which addresses the problem of identity authentication on the Internet without compromising privacy. In its paper, Microsoft said it wants to use existing identity verification technology, including verification techniques used by schools, post offices, and motor vehicle departments to verify the identities. Most of these entities verify information through identity documents such as birth certificates and drivers licenses. The data would be used to verify the date of birth and authenticity of the document, and would be encrypted with a PIN number for access. The paper also proposed that websites be divided up into categories including “general audience,” which would not require age authentication, and “adults only” and “children only,” which would require authentication.

The paper may be found at  
<http://download.microsoft.com/download/2/8/4/284093f4-5058-4a32-bf13-c12e2320cd73/Digital%20Playground.pdf>

---

## **JUDGE CRITICIZES CEO FOR FAILURE TO PRESERVE E-MAILS**

On September 2nd, U.S. District Judge Susan Illston imposed an adverse inference instruction against Oracle in its shareholder lawsuit because Oracle failed to preserve e-mail. Oracle CEO Larry Ellison failed to preserve e-mails and interview materials related to a book on Oracle. During discovery, Oracle produced only 15 e-mails from Ellison's files, but produced over 1,600 Ellison e-mails from other employees – thus indicating that there were other e-mails in existence that were never produced. The book materials also were never produced because the book's

author disposed of a laptop containing the materials in 2006 or 2007. Since the destroyed evidence was relevant to the claim that Oracle knew about problems with its suite 11i, effects of the economy on Oracle's business, and problems with Oracle's forecasting model, the adverse inference instruction will tell the jury to infer that the missing e-mails and materials might show this knowledge.

The ruling may be found at

<http://online.wsj.com/public/resources/documents/ellison.pdf>

---

## **GOOGLE LAUNCHES WEB BROWSER, TAKING ANOTHER HIT AT MICROSOFT**

On September 1st, Google announced the launch of its new web browser, Google Chrome. According to the Google blog, Google developed a browser because it is where we spend most of our time while on the computer. The browser itself is "streamlined and simple," and "gets you where you want to go fast." One of the main improvements is the isolation of tabs in the browser, so one tab will not crash all the tabs you have open. The browser is also meant to offer competition in an arena where Microsoft's Internet Explorer controls 80% of the market. Chrome may be the alternative for people who would like to use Google, all the time. However, several security vulnerabilities were identified in the first day of the Chrome release.

The Google blog post on Chrome may be found at <http://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html>

---

## **RIAA WINS COPYRIGHT INFRINGEMENT CASE DUE TO ACCUSED'S SPOILIATION**

On August 26th, the RIAA won its copyright infringement suit in Atlantic v. Howell due to the defendant's destruction of evidence. The RIAA sued Howell for copyright infringement in 2006 for alleged use of Kazaa to make files available for download. Howell claimed that he had not made available the files, but that his songs were uploaded from CDs and were for personal use. In April, the RIAA was dealt a blow in the case when a judge rejected their "making available" claim. While the case appeared to be ripe for trial, the RIAA then accused Howell of destroying evidence relevant to the lawsuit. The RIAA computer forensics expert found that Howell uninstalled Kazaa and reformatted his hard drive, which the RIAA claimed was to "cover his tracks." The court agreed with the RIAA, and found that if the evidence removed by Howell was really exonerating, he would have went to greater lengths to preserve it. From Howell's actions, the court inferred that Howell willfully destroyed evidence to mislead the court, and granted a default judgment against him. Too bad that formatting a drive doesn't actually destroy the data.

The decision may be found at

[http://www.klgates.com/files/upload/eDAT\\_Westlaw\\_Document\\_Atlantic.doc](http://www.klgates.com/files/upload/eDAT_Westlaw_Document_Atlantic.doc)

---

## **COMPUTER VIRUS IS OUT OF THIS WORLD**

On August 27th, news sources reported that a computer virus was found on a laptop in the International Space Station. The virus was a W32.Gammima.AG worm, which is malware that steals login names and passwords from popular Internet games. NASA spokesperson Kelly Humphries explained that the virus was detected through virus protection software, and did not pose a threat to the ISS computer systems. NASA was conducting an investigation to determine how the virus got aboard the space station. On website SpaceRef it was suggested that a flash drive brought aboard by an astronaut was the source of the virus.

The story may be found at

<http://www.informationweek.com/news/security/antivirus/showArticle.jhtml?articleID=210201099>

---

## **BY AUGUST 22ND, DATA BREACHES SURPASSED ALL OF 2007**

On August 25th, the Identity Theft Resource Center reported that the number of data breaches reported for 2008 had surpassed all data breaches reported in 2007. By August 22nd, the number of data breaches for this year had already reached 449, three more than the 446 reported in 2007. It was unclear whether there were more data breaches this year, or if there is increased reporting of data breaches. With the 449 data breaches reported, there were 22 million consumer records compromised. There may be more records compromised since in 41% of the breaches the number of records affected was not disclosed. In some cases, the number of records was not disclosed because businesses were still figuring out how many people were affected. Further, there may be even more compromised records because many businesses are not even aware of their data breaches. According to the ITRC, malicious attacks were the leading cause of data breaches, including hacking and company employees stealing data. Another large portion of the breaches was due to lost or stolen laptops.

The ITRC press release may be found at

[http://www.idtheftcenter.org/artman2/publish/m\\_press/Breaches\\_Blast\\_2007\\_Record.shtml](http://www.idtheftcenter.org/artman2/publish/m_press/Breaches_Blast_2007_Record.shtml)

---

## **WHITE HOUSE MISSING UP TO 225 DAYS OF E-MAIL**

On August 20th, the Associated Press obtained an internal White House draft document that indicated that the White House was missing as many as 225 days of e-mail. The memo also showed that the likelihood of recovery before Bush leaves office is slim, even though it asked companies to bid on a project to recover the e-mails. The e-mails would be recovered from 35,000 disaster recovery tapes dating back to October 2003. The tapes cover the time period in which there was growing violence in Iraq, the Abu Ghraib prison scandal, and the Valerie Plame scandal. The White House declined to comment on the document and whether or not it had already hired a contractor for the job.

The story may be found at

<http://www.msnbc.msn.com/id/26316841/>

---

## **JUDGE REQUIRES WARRANT FOR GOVERNMENT TO OBTAIN CELLPHONE DATA**

On September 10th, U.S. District Judge Terrence McVerry for the Western District of Pennsylvania confirmed a magistrate judge decision that required the government to have probable cause and obtain a search warrant before a wireless provider could turn over records that show where customers use their cellphones. The District Court opinion merely stated that the magistrate decision was not "clearly erroneous" or "contrary to law," without further explanation. The case dealt with a government request for Sprint historical cellphone data which included tower locations, call time, and duration. While the government argued that the data was a routine transactional record and not a tracking device that required a warrant, the ACLU argued that information about peoples' movements is private and requires a warrant. Magistrate Judge Lisa Pupo Lenihan agreed with the ACLU, finding that the information requested was sensitive and vulnerable to abuse.

The magistrate decision may be found at

[http://www.eff.org/files/filenode/celltracking/criminalapplicationorder\\_finalopinion.pdf](http://www.eff.org/files/filenode/celltracking/criminalapplicationorder_finalopinion.pdf)

The district court decision upholding the magistrate may be found at

<http://www.eff.org/files/filenode/celltracking/lenihanorder.pdf>

---

## **SURVEY: ONE IN FIVE EMPLOYERS SCREEN POTENTIAL EMPLOYEES ONLINE**

On September 10th, online job site CareerBuilder.com announced the results of a survey that found one in five employers screen their job candidates online. The survey asked 3,169 hiring managers, with 22% of them reporting that they screen potential applicants' activities on social networking sites. This was double the amount of employers using social networking sites in 2006. Of the employers that used the sites, 34% dismissed the candidate after what they saw. The main concerns of the employer were candidates posting information about drinking or drugs, posting

provocative information or photos, poor communication skills, and lying about qualifications. On the other hand, 24% found that the social networking site solidified their desire to hire a person. Factors that made an employer hire a potential candidate were a background supporting the candidate's qualifications, proof that they had good communication skills, and evidence that the candidate was a good fit for the office culture.

The survey results may be found at

[http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr459&sd=9%2f10%2f2008&ed=12%2f31%2f2008&siteid=cbpr&sc\\_cmp1=cb\\_pr459](http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr459&sd=9%2f10%2f2008&ed=12%2f31%2f2008&siteid=cbpr&sc_cmp1=cb_pr459)

---

## **GOOGLE REDUCES DATA RETENTION TIME BY HALF**

On September 8th, Google announced a new step to increase user privacy. Its previous policy for anonymizing user IP addresses was 18 months, but under the new policy, the IP addresses will be anonymized after only 9 months. The time reduction came after U.S. and E.U. regulators urged search sites to keep their data for only six months. Google explained that it keeps the information to provide quality products and services, create accurate search results, and for system security concerns. The problem with the data retention, according to Google's blog, is that the same information that may prevent fraud also may pose a security risk. After consulting with various experts, Google compromised on the timetable as a way to preserve data utility and maintain security.

The blog post may be found at

<http://googleblog.blogspot.com/2008/09/another-step-to-protect-user-privacy.html>

---

## **VIRGINIA SUPREME COURT STRIKES DOWN ANTI-SPAM LAW**

On September 12th, the Virginia Supreme Court overturned the state anti-spam law finding it violated the First Amendment. In doing so, the court overturned the conviction of Jeremy Jaynes, one of the world's worst spammers, and the first spammer convicted of a felony. Jaynes argued that the law violated the First Amendment because it restricted other types of mass messages, not just spam. The court agreed with Jaynes, and held that the law was overbroad because it did not limit the e-mail to commercial speech, and could prohibit the sending of political or religious e-mails that are protected under the First Amendment. Attorney General Bob McDonnell said he intended to appeal to the Supreme Court.

The opinion may be found at

<http://www.courts.state.va.us/opinions/opnscvwp/1062388.pdf>

---

## **EFF SUES OVER ELECTRONIC SURVEILLANCE**

On September 18th, the Electronic Frontier Foundation filed suit against the National Security Agency over illegal surveillance of U.S. citizens' phone and Internet communications. The EFF filed suit on behalf of AT&T customers. Evidence showed that AT&T routed copies of communications from its servers to a secret NSA room in San Francisco. The EFF claimed that the warrantless surveillance violated federal wiretapping laws, along with Constitutional guarantees of free speech and privacy. The EFF also sued President Bush and Vice President Dick Cheney for their role in implementing the illegal wiretapping plan. The lawsuit is intended to stop the present illegal wiretapping as well as sending a message to future administrations that illegal wiretapping will not be tolerated.

The EFF press release, with a link to the complaint, may be found at

<http://www.eff.org/press/archives/2008/09/17-0>

---

## **AFTER TRAIN CRASH, CALIFORNIA BARS TEXTING BY TRAIN OPERATORS**

On September 18th, the California Public Utilities Commission (CPUC) passed an order prohibiting the use of cell

phones while operating a train. The order followed a September 12th crash where a Metrolink commuter train collided with a Union Pacific freight train north of Los Angeles. The crash occurred after the commuter train sped through a red light, killing 25 people and injuring 134. The feds launched an investigation of the commuter train engineer's cell phone records after two 14-year-old boys stated that they received text messages from the engineer moments before the crash. The phone records showed that the engineer had been texting while on duty, but the timeframe was unclear. In response, California passed the order, and was considering requiring automatic train stops at traffic signals.

The CPUC press release may be found at  
[http://docs.cpuc.ca.gov/PUBLISHED/NEWS\\_RELEASE/91033.htm](http://docs.cpuc.ca.gov/PUBLISHED/NEWS_RELEASE/91033.htm)

The LA Times story on the crash may be found at  
[http://www.latimes.com/news/science/la-me-traincrash13-2008sep13,0,6212375.full\\_story](http://www.latimes.com/news/science/la-me-traincrash13-2008sep13,0,6212375.full_story)

The LA Times story on the text messaging may be found at  
<http://latimesblogs.latimes.com/lanow/2008/09/metrolink-eng-1.html>

---

## **VA COURT HOLDS POSTING SSNs MAY NOT BE SANCTIONED**

On August 22nd, the U.S. District Court for the Eastern District of Virginia ruled that posting social security numbers as part of a public record may not be sanctioned under Virginia law. In Virginia, the clerks of court were posting public land records online without redacting the social security numbers. A privacy advocate, Betty Ostergren, posted public land records on her website to discourage posting without the social security numbers redacted. Ostergren filed suit against Virginia Attorney General Robert McDonnell concerning a Virginia privacy statute that prohibits intentionally communicating another person's social security number to the general public. Ostergren claimed that the statute was unconstitutional as applied to her because fining her for posting the records violated her free speech rights under the First Amendment. The court referred to the Supreme Court decision in Cox Broadcasting Corp. v. Cohn, which held that when a newspaper obtains public records lawfully, then state officials cannot prevent the publishing of the records unless there is a "need to further the state interest to the highest order." Though the website was not a newspaper, the court found that Ostergren's website was still afforded the same protections. The court then considered whether the state considered the disclosure of social security numbers an interest of the highest order. The court concluded that the state did not because it made available the numbers for public record, gave the clerks of the court three years to redact the numbers already online, and then failed to give the court funding to perform the redaction. Since Ostergren obtained the records lawfully, and the state did not consider the redaction of the social security numbers an interest of the highest order, the court held the Virginia privacy statute was unconstitutional as applied to Ostergren. The court also scolded Virginia for disregarding the serious privacy concerns at stake when posting social security numbers on the Internet.

A copy of the opinion may be found at  
[http://www.acluva.org/docket/pleadings/ostergren\\_opinion.pdf](http://www.acluva.org/docket/pleadings/ostergren_opinion.pdf)

---

## **BRAD PITT AND OTHER CELEBRITIES LURE USERS TO MALWARE**

On September 16th, McAfee released its report on the riskiest celebrities to search for on the Internet. This year, the list was topped by Brad Pitt, as 18% of searches for downloads about him could result in the placing of malware or other online threats on your computer. The rest of the top ten, in order, included Beyonce, Justin Timberlake, Heidi Montag, Mariah Carey, Jessica Alba, Lindsay Lohan, Cameron Diaz, George Clooney, and Rihanna. McAfee Senior Vice President of McAfee's Product Development & Avert Labs explained that cybercriminals take advantage of American interest in celebrity gossip. He warned that capitalizing on celebrities was common, and to beware of any downloads after doing your celebrity searches.

The McAfee press release, with more information about the threats for each celebrity, may be found at  
[http://www.mcafee.com/us/about/press/corporate/2008/20080916\\_120000\\_y.html](http://www.mcafee.com/us/about/press/corporate/2008/20080916_120000_y.html)

---

## **COURT UPHOLDS STUDENT SUSPENSION FOR CREATING FAKE MYSPACE PAGE**

On September 11th, U.S. District Judge James Munley for the Middle District of Pennsylvania upheld the suspension of an eighth grade student for making a MySpace page about her school principal that depicted him as a pedophile and a sex addict. The student appealed her suspension as a violation of her free speech rights because the speech took place outside of school and violated parental rights in raising their children. Judge Munley held that the school was within its bounds in prohibiting speech that was vulgar and promoted unlawful behavior. Judge Munley rejected the Supreme Court decision of *Tinker v. Des Moines* in favor of two more recent cases that upheld suspensions for vulgar speech and speech that promoted illegal drug use. The two latter cases took place on school property or on a school trip, unlike this case where the page was made at home, though another student printed out a copy of the page and brought it to school at the principal's request. Judge Munley also distinguished *Tinker* because the speech there was political speech, but the speech here was not. The speech here was held to be an attack on the principal that could have been the basis for criminal charges against the student.

The opinion may be found at

<http://howappealing.law.com/JSvsBlueMountainSD.pdf>

The Law.com article on the case may be found at

<http://www.law.com/jsp/article.jsp?id=1202424549808>

---

## **DHS TELLS TRAVELERS TO LEAVE LAPTOPS AT HOME**

On September 15th, Information Week reported on a Department of Homeland Security Report that warned travelers about bringing a laptop when traveling abroad. The report recognized that while it may not be possible to travel without the laptop, the DHS recommended using a travel laptop with less information on it. The reason for these alternative travel uses were because foreign governments could have access to information on the laptop at any time, and data is not secure when traveling abroad. The Washington Post pointed out that one reason why laptops may not be secure when traveling abroad comes from re-entry at U.S. borders. The government recently began disclosing policies about searching and copying laptops at the border, with changes stemming from the war on terrorism. The DHS policies state that no reasonable suspicion is required to search laptops and or to make copies of the laptop contents. Until last year, government agents needed probable cause before copying materials, and reasonable suspicion before searching materials.

The Information Week story may be found at

<http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=210601724>

The Washington Post story may be found at

[http://www.washingtonpost.com/wp-dyn/content/article/2008/09/22/AR2008092202843\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2008/09/22/AR2008092202843_pf.html)

---

## **YOU TUBE PROHIBITS VIDEOS THAT INCITE VIOLENCE**

On September 10th, YouTube announced changes to its community guidelines, which included a ban on videos that incite violence. The policy change followed criticism from Senator Joseph Lieberman that the site allowed terrorist groups to post militant propaganda videos. Earlier this year, YouTube refused to take some videos down from a list made by Lieberman, though the site did take down some videos marked with al-Qaeda logos. Now that YouTube has changed its policy, more of the videos on Lieberman's list could be taken down. What types of videos violate the new policy will be considered on a case-by-case basis.

A YouTube blog post on the updated policy may be found at

<http://www.youtube.com/blog?entry=rJc1Z2eKWeA>

The Washington Post article may be found at

<http://www.washingtonpost.com/wp-dyn/content/article/2008/09/11/AR2008091103447.html>

---

## **VP CANDIDATE PALIN'S E-MAIL HACKED, CRIMINAL CHARGES PENDING**

On September 17th, news sources reported that Vice Presidential Candidate Sarah Palin's Yahoo! e-mail account had been hacked. The hack was done to search for e-mails of a political nature, as Palin kept a separate Yahoo account from her government account, and conducted government business on the account. The practice of conducting government business on personal accounts allows politicians to avoid FOIA requests by turning over the information only from the government account. It seemed that hackers accessed the account by doing a search about some information on Palin and then tricking Yahoo! into resetting the password. The hacker was anonymous at first, but it was discovered later that David Kernell, son of Tennessee Representative Mike Kernell and a student at the University of Tennessee, might be implicated. Kernell was suspected after a post on 4chan.com recounted the details of the attack. The poster's e-mail address was the same as Kernell's, and the IP address matched Kernell's dorm. Over the weekend FBI agents searched Kernell's apartment. As of September 24th, a grand jury was hearing the case but no charges had yet been filed against Kernell.

The story may be found at

<http://www.pcmag.com/article2/0,2817,2331064,00.asp>

---

## **JUDGE SAYS 'HEADS WILL ROLL' BECAUSE OF WITHHELD E-MAIL**

On September 17th, Law.com reported that a judge threatened serious repercussions due to the delayed production of e-mail. The case involved a government stock option prosecution against former McAfee general counsel Kent Roberts. The company turned over highly relevant e-mails the night before opening arguments, resulting in a very angry Judge Marilyn Hall Patel. The government explained that the documents should have been produced much sooner, as there was a two year old grand jury subpoena in the case. Patel was forced to dismiss the jury for the day so the parties could figure out if any more documents were withheld.

The story may be found at

<http://www.law.com/jsp/article.jsp?id=1202424591001>

---

## **JUDGE ALLOWS PROSECUTORS TO SEARCH ALL OF SEIZED COMPUTER RECORDS**

On August 22nd, U.S. District Judge Robert Kugler gave prosecutors permission to go through computer records from criminal defense lawyer Donald Manno even though it included client files that were not targets of the search. Manno appealed the search warrant that was issued on May 7th, claiming the FBI was not going to distinguish which drives contain responsive information. Kugler denied Manno's request for restraints, stating that the prosecutor's procedure had adequate safeguards to protect privilege. The process involved people not involved in the prosecution screening the seized files, with an FBI agent looking for responsive materials and a lawyer ensuring the materials were not privileged. Kugler held that the process adequately protected privilege and that Manno and his clients could move to suppress if any privileged evidence turned up in a later criminal prosecution.

The story may be found at

<http://www.law.com/jsp/article.jsp?id=1202424223239>

---

## **SURVEY SHOWS THAT FIRED IT EMPLOYEES WOULD STEAL DATA**

On August 27th, security firm Cyber-Ark announced the results of a survey finding that 88% of IT administrators would steal company data if fired. Of the 88%, one third would steal the privileged password list to gain access to valuable documents. Information that would be up for grabs included CEO passwords, customer databases, research and development plans, financial reports, M&A plans, and the company list of privileged passwords. Udi Mokady, co-founder and chief executive of Cyber-Ark explained that most company directors had no idea about how much information IT staff could access. The survey also found that one third of IT staff admitted to looking around the network at confidential information like salary details and personal e-mails.

The Cyber-Ark press release may be found at  
[http://www.cyber-ark.com/news-events/pr\\_20080827.asp](http://www.cyber-ark.com/news-events/pr_20080827.asp)

---


*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 © 2008 Sensei Enterprises, Inc. All rights reserved.**