

# { 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 139 - December 2008

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

---

### CASE SHOWS WHEN E-DISCOVERY IN PAPER FORMAT IS APPROPRIATE

On October 31st, LLRX.com published its e-discovery update, explaining why requesting a secondary production of electronic evidence may be beneficial after an initial paper production is not fruitful. Some downsides to paper format are that it is not easily searchable, loss of metadata, and higher storage costs. These features sometimes make secondary production of electronic discovery necessary and appropriate, as demonstrated by the District of Kansas case *White v. Graceland College Center*. In the case, the requesting party asked for a secondary production of documents after the producing party converted electronically stored information into paper format. As secondary production places a hardship on the opposing party, the requesting party must exercise great care to get the documents it wants. First, the complaint about production should be reasonable and limited to a specific set of documents, as general complaints are usually rejected in court. In *White*, the requesting party asked for only a very limited subset of documents whose authenticity could not be identified, which showed the judge that the party had researched its claim, which undercut the other side's argument that this was burdensome. Second, the complaint should explain what parts of the document are missing and why it makes a difference. In *White*, the requesting party demonstrated a close nexus between missing metadata and their claim, which compelled the judge to order secondary production. A third argument involves the equity of the materials between parties. In *White*, the judge found that the producing party converting native files to PDF and then printing them got rid of the equity and utility of the documents for the opposing party. Litigants also should be aware of Federal Rule of Civil Procedure 34 limitations, and how these techniques may be used to get around the rule in certain instances.

The article may be found at <http://www.llrx.com/columns/hardcopiesi.htm>

---

### GOOGLE SETTLES COPYRIGHT SUIT OVER GOOGLE BOOK SEARCH

On October 28th, Google and major copyright holders came to an agreement over Google's Book Search program, which scans books and puts them online before getting permission from the publishers and authors. Under the compromise, Google will be allowed to scan and make available any out-of-print book that still has a valid copyright, offer subscriptions to the database, sell online access, and eventually let subscribers print books on demand. For books that are still in print, Google will first have to get explicit permission from the authors and publishers. Google has agreed to pay about \$125 million, including an up front payment of about \$45 million, and will share future proceeds with copyright holders. It will cost about \$35.4 million to establish the registry, but Google will take in revenue from selling subscriptions, individual books, and advertisements on the book view website. About 63% of revenue will go to copyright holders. Public libraries will get free access to the database, and patrons can view and print pages from the books but cannot copy text. On November 17th, U.S. District Judge John Sprizzo issued an order tentatively approving the deal, but scheduled a hearing for June 2009 to fully consider the deal's fairness.

The Google blog post may be found at <http://googleblog.blogspot.com/2008/10/new-chapter-for-google-book-search.html>

A news story on the preliminary approval may be found at [http://www.mercurynews.com/nationworld/ci\\_11009992](http://www.mercurynews.com/nationworld/ci_11009992)

---

## **BIG COMPANIES LAUNCH NEW INITIATIVE TO PROTECT ONLINE SPEECH**

On October 28th, Google, Yahoo, and Microsoft teamed up with human rights and public interest organizations to introduce a code of conduct that will protect online free speech and privacy against government intrusion. The initiative was started after human rights groups and Congress criticized Internet companies for cooperating with the Chinese government's censorship. In addition to the code of conduct, the initiative will also provide a non-government forum to resist the demands of censorship and establish a system of independent auditors to rate companies' conduct. While Yahoo, Google and Microsoft are participating, other companies are not, including Verizon, AT&T and Sprint, who were accused of warrantless surveillance at the Bush Administration's request. Some human rights activists have criticized the initiative, saying that it is all talk and no action.

The press release may be found at

[http://www.globalnetworkinitiative.org/newsandevents/Diverse\\_Coalition\\_Launches\\_New\\_Effort\\_To\\_Respond\\_to\\_Government\\_Censorship\\_and\\_Threats\\_to\\_Privacy.php](http://www.globalnetworkinitiative.org/newsandevents/Diverse_Coalition_Launches_New_Effort_To_Respond_to_Government_Censorship_and_Threats_to_Privacy.php)

---

## **ARMY REPORT SAYS TWITTER IS A POTENTIAL TERRORIST TOOL**

On October 16th, the Army released a draft intelligence paper on possible terrorist uses of new technology. Some examples of uses are the possibility of terrorists using GPS devices on phones for travel plans, surveillance, and targeting, using mobile phone cameras as surveillance devices, and using voice changing technology to make phone calls. Twitter also could be a terrorist tool, as the report imagines a "Red Team" scenario where terrorists send other terrorists Twitter messages as real time updates of an attack. The report warns that this could allow terrorists to select the precise moment to set off a bomb based on the Twitter messages sent to him from others. The report's goal was to lay out possible scenarios in which terrorists could use technology, but requires further research to see if the scenarios would play out.

The report may be found at <http://www.fas.org/irp/eprint/mobile.pdf>

---

## **COURT SETS E-DISCOVERY PROTOCOL AFTER PARTIES CANNOT AGREE**

On October 29th, in the U.S. District Court for the District of Columbia, Judge Facciola set his own protocol for Plaintiff's expert's search of Defendants' computer systems after the parties could not agree. Defendants offered a search protocol, but the court rejected it because it was highly restrictive, full of undefined "buzz words," and was "fundamentally misguided" as the limited search was not likely to produce all the electronically stored evidence that Plaintiff legitimately demanded. Judge Facciola then formulated his own search protocol. The protocol laid out what the Plaintiff's expert could search, the time to conduct the search, and found that Defendants' representative could be present during the search. The court also considered Defendants' concern about privileged information, and found that Defendants would have three weeks to go through the search results before the results were given to Plaintiff. Defendants were also ordered to produce a privilege log in compliance with Federal Rule of Civil Procedure 26. Finally, the court determined that Defendants would pay up to \$10,000 for the search, and if the search was more expensive, then the court would determine how to allocate costs.

The decision may be found at

[http://www.ediscoverylaw.com/uploads/file/Westlaw\\_Document\\_D'Onofrio\(1\).doc](http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_D'Onofrio(1).doc)

---

## **CRAIGSLIST RESTRICTS SEX ADS AFTER AG PROMPTING**

On November 6th, Craigslist announced a new initiative to prevent illegal activity on its website in conjunction with 40 Attorneys General across the country. In the agreement, Craigslist will implement new requirements to tame its unruly "erotic services" listings. One safeguard, implemented in March, requires erotic services advertisers to provide a phone number, where a computerized system calls and leaves automated numbers that the advertiser must type in before the ad will appear on the site. The new agreement requires advertisers to provide valid

identification, and will charge erotic services vendors a small fee for each ad that requires credit card payment. The fee will be donated to charities that combat child exploitation and human trafficking. Craigslist also filed suit against 14 companies offering services to get around the new protections.

The Craigslist blog may be found at <http://blog.craigslist.org/2008/11/joint-statement-with-attorneys-general-ncmec/>

---

## **CAMPAIGN COMPUTERS HACKED BY FOREIGNERS LOOKING FOR POLICY INFO**

On November 6th, CNN reported that computers at Obama and McCain headquarters were hacked by a foreign government or organization trying to get policy information. The hacking took place over the summer, according to a CNN source, but campaign representatives could not be reached for comment. Another source indicated that the U.S. knows which country was responsible for the attacks, but was not releasing that information. Newsweek first reported the hacking, and a source there indicated that Obama campaign workers discovered the attacks through what was thought to be a computer virus. The next day the FBI informed the campaign that the computers were compromised by something more than a virus. The FBI and Secret Service are investigating the matter, but also refused to comment.

The story may be found at <http://www.cnn.com/2008/TECH/11/06/campaign.computers.hacked/>

---

## **NEW IPHONE APPLICATION SENDS FAKE CALLS TO YOUR PHONE**

In early November, start up company Magic Tap released a new iPhone application that can help anyone get out of an awkward situation. The application is entitled "Fake Calls" and with the touch of a button, it will send a fake phone call to your iPhone whenever you like to get you out of an awkward situation or a bad blind date. The call does not start a real phone call, so no airtime charges apply. The call can look like it is from anyone you want, as you can customize the caller name, number, call time, wallpaper for caller ID, and whether the phone will ring or vibrate. The application costs 99 cents at the Apple App Store, and Magic Tap is donating 10% of its earnings to charity.

The full story may be found at <http://magictap.net/fakecalls/>

---

## **AT&T FOLLOWS OTHER COMPANIES, TESTS BANDWIDTH LIMITS**

On November 4th, *CNET* reported that AT&T would follow in the footsteps of Comcast and other Internet Service Providers and test limits on its bandwidth. The tests were set to start the following weekend in Reno, NV. For customers of AT&T's slowest service, the limit is 20 gigabytes per month, and for customers of AT&T's fastest service, the limit is 150 gigabytes per month. AT&T is also offering access to an online tool for users to track their usage, and users will be notified once they reach 80% of their limit. A charge of \$1 per extra gigabyte will apply if a user goes over the limit. Similar to other companies, the bandwidth limits are intended to deter heavy users, as AT&T estimates that 5% of subscribers use 50% of the network capacity.

The story may be found at [http://news.cnet.com/8301-1023\\_3-10082615-93.html](http://news.cnet.com/8301-1023_3-10082615-93.html)

---

## **PRIVACY CONCERNS INCREASE AS GOOGLE'S POWER INCREASES**

On November 3rd, the Associated Press reported that as Google is increasing its share in the mainstream computer scene, it is facing numerous questions by privacy advocates about the amount of private data it is keeping about its users. Google explains that it keeps the data to improve its services, but privacy advocates are concerned about what else Google does with the information, how long it keeps the information, and whether it combines the information for a single user of multiple applications. The release of Google's web browser, Chrome,

only added to the privacy concerns. One issue with Chrome was its navigation bar, which relays the keystrokes that a user types to visit a website even before the user hits enter. The feature is called "Google Suggest," which sends Google searches from what you type. While the feature may be turned off, it is not immediately clear how to do so.

The story may be found at

[http://www.usatoday.com/tech/news/internetprivacy/2008-11-03-google-privacy\\_N.htm](http://www.usatoday.com/tech/news/internetprivacy/2008-11-03-google-privacy_N.htm)

---

## **AUSTRALIA DEVELOPS NEW TOOL TO HELP CATCH CHILD PORNOGRAPHERS**

On November 4th, Australia IT reported that a new tool is in development to help law enforcement fight child pornography. The tool is in beta testing, and was developed by Perth's Edith Cowan University and the Western Australia Police. The tool enables officers to know right away whether the computer contains illicit images. The tool is called the Simple Image Preview Live Environment (SImpLE). The computer is booted from a Linux bootable CD and if suspect files are found, the user connects a USB-DVD writer to the computer and the images are written to the DVD media. With this mechanism, the police may take the DVD to a judge for review right away. SImpLE does not scan the hard drive to see what images were deleted, it only looks at what is topically available. SImpLE is intended to be ready for release by February 2009, and could provide a solution to lengthy computer searches by police officers.

The story may be found at

<http://www.australianit.news.com.au/story/0,24897,24597325-15306,00.html>

---

## **RIAA GETS NEW COPYRIGHT CHALLENGE FROM HARVARD PROFESSOR**

On October 30th, *Computer World* reported that Harvard Professor Charles Nesson filed a counterclaim against the RIAA on behalf of Joel Tenenbaum, an individual sued by the RIAA for copyright infringement. Nesson's counterclaim challenged the constitutionality of the Digital Theft Deterrence and Copyright Damages Improvement Act of 1999 and the RIAA's use of the statute against Tenenbaum. The counterclaim is broader than any previous constitutional challenge to the RIAA's anti-piracy campaign. The counterclaim states that, since the statute is a criminal statute, it was unconstitutional to apply the law to prosecute a civil case in federal court. Nesson claimed that the copyright infringers are entitled to the protections of criminal procedure and the criminal courts in these cases. Nesson also challenged the steep penalties for copyright violations, stating that they are "grossly excessive" and beyond the amount of damages. The RIAA filed a motion to dismiss the counterclaim, stating that Nesson was merely complaining about the hardship of being a defendant in a lawsuit.

The story may be found at

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=knowledge\\_center&articleId=9118599&taxonomyId=1&intsrc=kc\\_top](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=knowledge_center&articleId=9118599&taxonomyId=1&intsrc=kc_top)

---

## **MAGISTRATE JUDGE RECOMMENDS DEFAULT JUDGMENT FOR SPOILIATION**

On October 15th, a magistrate judge in the Eastern District of New York recommended the imposition of default judgment against the defendants in a fraud cause due to their intentional spoliation of evidence on a laptop. Defendants' conduct included: visiting a website that provided a computer program to delete files from a computer, downloading (but not using) the deletion program, deleting hundreds of user documents in the days before forensic imaging, deleting files that were labeled as related to the litigation and listed in Defendants' privilege log, reinstalling the operating system on the laptop two days before the forensic imaging, deleting hundreds more files after the operating system was re-installed, and changing timestamps for laptop documents. The court found that it was clear that defendants' intentionally destroyed information from this conduct. The judge recommended default judgment as a sanction and also ordered defendants to pay all plaintiffs' legal costs relating to the discovery dispute over the laptop.

The case is *Gutman v. Klein*, and it may be found at

[http://www.ediscoverylaw.com/uploads/file/Westlaw\\_Document\\_Gutman.doc](http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_Gutman.doc)

---

## **SPAM DISTRIBUTION DROPS AFTER SHUTDOWN OF ONE COMPANY**

On November 18th, the Washington Post reported one of the biggest drops in spam after one hosting firm was taken offline by its Internet Service Providers. Security experts exposed the fact that McColo, a Silicon Valley computer firm, was hosting computers of many organizations that distributed most of the world's spam. After the story broke, McColo's Internet Service Providers pulled the plug, causing a 65% drop in the amount of spam e-mail delivered. McColo was believed by security researchers to host many different botnets, or robot networks that send out massive amounts of spam from control servers. Experts said that the criminals maintaining the botnets will quickly find an alternative source to get back online. The story also reported that while spam decreased, not all users saw a decrease of spam in their inbox. Those who saw a decrease were likely to have poor spam filters, while those with better spam filters probably did not notice a difference.

The story may be found at

<http://www.washingtonpost.com/wp-dyn/content/article/2008/11/19/AR2008111903075.html>

A research report on McColo's activities may be found at

<http://hostexploit.com/downloads/Hostexploit%20Cyber%20Crime%20USA%20v%202.0%201108.pdf>

---

## **ANGRY SUBSCRIBERS SUE ISPS, WEB TRACKING COMPANY**

On November 11th, news sources reported that angry Internet subscribers filed a class action lawsuit against NebuAd and six Internet Service Providers for the development and use of online tracking tools. The lawsuit alleges privacy violations, fraud and unjust enrichment. The technology at issue is NebuAd's deep packet inspection, which is used for targeted advertising. NebuAd attached the company's hardware to ISPs' data hubs and then reported the information back to the ISPs so the ISPs could use the information for targeted advertising. The lawsuit alleges that both NebuAd and the ISPs intercepted, copied, transmitted, collected, stored, used and altered users' private data in violation of various federal and state computer laws. The lawsuit asks for injunctive relief prohibiting use of the technology and for the parties to turn over all unjust profits over to the class.

The story from *Ars Technica* may be found at

<http://arstechnica.com/news.ars/post/20081111-nebuad-isps-sued-over-dpi-snooping-ad-targeting-program.html>

---

## **CARELESS/DISGRUNTLED EMPLOYEES MAY POSE DATA BREACH THREAT**

On November 20th, Cisco released the third installation of its study on company data security. The third part deals with the "insider threat" to data leaks: company employees who are uninformed, disgruntled, careless, or all of the above. The study indicates that insider threats can be greater than attacks that originate outside the company. Other key findings were that portable hard drives are bigger security concerns than e-mail, and that some employees keep devices with employer data on them even after they leave the company. One of the biggest mistakes is assuming that a disgruntled employee, e.g. one who is fired and steals data to get even, is a bigger threat than a careless employee. A careless employee can be just as bad, e.g. the guy loudly revealing company data while talking on his cell phone, failing to log off a computer, leaving passwords lying around, or worst yet, losing his cell phone, laptop or other electronic device that's unencrypted and void of any password protection. Advice for companies dealing with these issues included education, training and awareness.

The Cisco press release with links to the studies may be found at

[http://newsroom.cisco.com/dlls/2008/prod\\_112008.html](http://newsroom.cisco.com/dlls/2008/prod_112008.html)

---

## **EQUIFAX INTRODUCES ONLINE IDENTITY CARD**

On November 13th, Equifax introduced its online information card, which is designed to make online transactions more secure. The card has been likened to an online driver's license, passport or similar ID. It would be used as an

“electronic wallet,” which would allow customers to avoid typing in a user name and password for every website, while revealing their identity. With the increase in fraud and identity theft, the card is intended to provide a secure way to conduct online transactions. Equifax paired up with information management company Parity to develop the card.

The Equifax press release may be found at

[http://www.equifax.com/cs7/Satellite?c=EFX\\_News\\_C&childpagename=US%2FEFX\\_News\\_C%2FPressReleasePage&cid=1187888570222&p=1182374863790&packedargs=locale%3Den\\_us&pagename=EFX%2FWrapper](http://www.equifax.com/cs7/Satellite?c=EFX_News_C&childpagename=US%2FEFX_News_C%2FPressReleasePage&cid=1187888570222&p=1182374863790&packedargs=locale%3Den_us&pagename=EFX%2FWrapper)



## **GOOGLE INTRODUCES ON-DEMAND WEBSITE INDEXING**

On November 13th, Google announced a new feature that allows web publishers to re-index their site on its Site Search program whenever they want. Site Search is a program designed for companies who want to use Google's search engine to power the search engine for their particular site. Prior to the new feature, Google scheduled internal algorithms automatically to control indexing. The new feature may be activated in Google's Site Search control panel by clicking a new button that says “index now.” The feature should be useful for websites that were recently updated or have been redesigned. Newly indexed pages will become searchable no more than twenty-four hours after they are activated.

The Google blog post may be found at

<http://googleenterprise.blogspot.com/2008/11/meeting-your-demands-with-google-site.html>



## **YOUTUBE LAUNCHES NEW AD PLATFORM FOR SPONSORED VIDEOS**

On November 12th, YouTube announced a new ad platform for Sponsored Videos, which will let users promote their videos by bidding on keywords. To use the program, a user needs to determine which videos they want to promote and decide which keywords to target. Google (YouTube's parent company) created automated tools to help users place bids in an automated online auction. Relevant videos will appear alongside search results and will be labeled as sponsored videos. Users of the program are charged on a cost per click basis, and only U.S. users were eligible to bid at the time of release.

The YouTube blog post may be found at

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



## **STUDY SHOWS ENERGY INDUSTRY AT RISK OF CYBERATTACK**

On November 10th, security firm Secure Computing announced the somber results of its security study - that infrastructure in the U.S. and Canada is vulnerable to cyberattack. The survey interviewed 199 “industry insiders” from utilities, oil and gas, financial services, government, telecommunications, transportation and other critical infrastructure industries. Those surveyed were asked about the readiness of eight different industries to deal with a cyberattack. More than 50 percent said utilities, oil and gas, transportation, telecommunications, chemical, emergency services and postal/shipping industries were not prepared. For the postal/shipping industry, the results were worse, as 3/4 said it was not ready for an attack. The energy sector was indicated as the biggest target, most vulnerable to attack and the most detrimental if breached. The biggest bottleneck to prevention was the cost of security, followed by apathy.

The Secure Computing press releases may be found at

[http://www.securecomputing.com/press\\_releases.cfm?ID=1224414](http://www.securecomputing.com/press_releases.cfm?ID=1224414)



## **VERIZON EMPLOYEES ACCESSED OBAMA'S CELL PHONE ACCOUNT**

On November 20th, Verizon Wireless announced that some of its employees had accessed President-Elect

Obama's cell phone account without authorization. The statement indicated that the account had been inactive for several months and was only a regular flip phone, not a smart-phone with e-mail capability. Employees that accessed the account were placed on immediate leave with pay. The sanction applied to all employees that accessed the account, whether authorized or not. Once Verizon determines who had authorized access and who did not, it will take appropriate action. Verizon offered its sincere apology to President-Elect Obama.

The Verizon statement may be found at  
<http://news.vzw.com/news/2008/11/pr2008-11-20b.html>

---

## **TENNESSEE PASSES NEW LAW FORCING COLLEGES TO POLICE ILLEGAL DOWNLOADS**

On November 12th, Tennessee passed a new law requiring both public and private colleges in the state to police their computer networks to detect illegal downloads. In an apparent victory for the Recording Industry Association of America (RIAA), the law is aimed at reducing the large number of illegal downloads coming from college campuses. According to a survey, more than half of college students download movies and music illegally. Under the law, universities must implement "technological support and develop and enforce a computer network usage policy to effectively limit the number of unauthorized transmissions of copyrighted works." The Electronic Frontier Foundation (EFF) said the law is ridiculous and would initially cost Tennessee over \$9 million to enforce and more than \$1.5 million annually thereafter. The EFF also explained that the law will not stop piracy on college campuses because there are other, low cost ways for students to exchange music, utilizing DVDs and USB drives.

The RIAA press release may be found at  
<http://www.riaa.com/newsitem.php?id=72240403-D51A-209F-142F-98DC98F7AE18>

The EFF blog post may be found at  
<http://www.eff.org/deeplinks/2008/11/riaa-wins-campus-lose-tennessee-governor-signs-c>

---

## **ARMY BANS USB DRIVES AFTER WORM ATTACK**

On November 19th, *Wired.com* reported that the Army suspended the use of portable data storage after a worm attack invaded its network. According to internal Army e-mail, the attack was on both the classified and unclassified networks, and the ban was supposed to take effect immediately. The ban applied to all devices until the devices could be scanned for malware. Eventually, some secure government devices will be available for use in critical situations. The worm at issue spreads by copying itself onto USB drives and other portable storage devices. When the device is plugged into another computer, the worm invades that PC as well. Though a major inconvenience, the Army's security firm believed that the ban would be effective in stopping the worm.

The story may be found at  
<http://blog.wired.com/defense/2008/11/army-bans-usb-d.html>

---

## **FTC GETS COURT ORDER TO STOP SPYWARE COMPANY SALES**

On November 17th, the Federal Trade Commission announced that a U.S. District Court in Florida had issued a temporary injunction preventing company CyberSpy Software, LLC, from selling its spyware program, RemoteSpy. The program works as follows: clients who ordered the software were given instructions on how to disguise the program as an innocuous attachment to an e-mail. When a victim clicked on the file, the spyware was installed on the victim's computer and recorded every keystroke, including passwords. The program also collected images of the computer screen and websites visited by the victim. Software customers could then log into a company database to access all information collected by the program. The FTC complaint alleges that the company collected personal information without authorization and made that information available to its users. The FTC seeks a permanent injunction and for the company to give up any ill-gotten gains. The temporary restraining order also requires the company to take the servers that store the unauthorized information offline.

The FTC press release may be found at  
<http://www.ftc.gov/opa/2008/11/cyberspy.shtm>

---

## **MICROSOFT OFFERS FREE SECURITY SUITE FOR CUSTOMERS**

On November 18th, Microsoft announced that it would offer a free security system for PCs called "Morro" focused on fighting malware. While the suite will not be available until the second half of 2009, it is supposed to "provide comprehensive protection from malware including viruses, spyware, rootkits and trojans." Morro will be better suited for lower bandwidth PCs, as it uses fewer resources than the current Windows Live One Care system, which Microsoft will stop selling when the new system comes out. Morro also will not have One Care's non-security features like printer sharing and automated PC tune-ups. Microsoft switched to a free product because it determined that many PCs are without anti-virus software or their users do not keep their anti-virus software up to date.

The Microsoft press release may be found at  
<http://www.microsoft.com/Presspass/press/2008/nov08/11-18NoCostSecurityPR.mspx>

---

## **NEW PRIVACY GROUP TO WORK ON DATA COLLECTION ISSUES**

On October 16th, a new privacy group called the Future of Privacy Forum was formed. The group plans to focus on online privacy and plans to help shape standards for collection and use of consumer information online. The group is sponsored by AT&T and will be led by Jules Polonetsky, who until this month was in charge of AOL's privacy policy, and Chris Wolf, a privacy lawyer for law firm Proskauer Rose. Privacy issues have come into the limelight recently as collection of user data increases. The group plans to help the new administration deal with these types of issues. One issue the group could fight for is for companies to have consumers "opt in" before a company can collect data, instead of the current practice of having consumers "opt out" if they do not want their data collected.

The Future of Privacy Forum Mission may be found at  
<http://www.futureofprivacy.org/2008/11/15/the-future-of-privacy/>

---

## **AMERICAN AIRLINES INTRODUCES MOBILE BOARDING PASSES**

On November 13th, American Airlines announced its introduction of mobile boarding passes sent to a traveler's cell phone or PDA, but only at selected airports. The airline partnered with the Transportation Security Administration to test the new system, which e-mails a two-dimensional barcode to a traveler's cell phone or PDA. When the traveler gets to the airport, he or she can go directly to security, which will scan the phone instead of a regular boarding pass. Travelers may check bags with the online boarding pass by scanning the bar code at one of the self-service counters. The new system does not eliminate the paper option, as travelers who would still like to receive a paper boarding pass may do so. Other airlines have been testing similar systems, but American's is the first to be active.

The American Airlines press release may be found at  
[http://www.aa.com/content/amrcorp/pressReleases/2008\\_11/13\\_barcode.jhtml](http://www.aa.com/content/amrcorp/pressReleases/2008_11/13_barcode.jhtml)

---


*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.**