

{ 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 140 - January 2009

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

SPYWARE CAUSED PORN ON TEACHER'S COMPUTER

On November 21st, prosecutors dropped felony charges against a Connecticut teacher accused of showing students porn on a classroom computer. Julie Amero pled guilty to a misdemeanor charge of disorderly conduct, paid a \$100 fine and surrendered her teaching license. Computer forensic experts found that spyware was responsible for the pornography on the computer. The spyware was on the computer because the school did not keep its computers software updated. Connecticut Superior Court Judge Hillary B. Stackbein said the conviction was based on false information. Prosecutor Michael Regan said that he was not convinced by the spyware evidence, was convinced of Amero's guilt, and would take the case to trial again. Computer experts across the country were appalled at Regan's ignorance, as the state never inspected the computer's hard drive and relied on testimony from a detective with limited computer experience.

The story from the *Hartford Courant* may be found at
http://blogs.courant.com/rick_green/2008/11/connecticut-drops-felony-charge.html

FACEBOOK GETS \$873 MILLION JUDGEMENT AGAINST SPAMMER

On November 21st, a Federal Judge in San Jose awarded Facebook \$873 million against spammer Adam Guerbuez of Montreal, Canada and his business, Atlantic Blue Capital. Guerbuez was responsible for over four million spam messages sent to Facebook users. The scheme tricked Facebook users into turning over their usernames and passwords, and used computer programs to send out spam messages about drugs and penis enlargement products. The judgment is the largest ever awarded under the CAN-SPAM Act. While Facebook did not expect to collect the entire judgment, it hoped it would deter other spammers.

The story on the Facebook Blog may be found at
<http://blog.facebook.com/blog.php?post=40218392130>

REPORT FINDS CHINA CONDUCTING CYBER ESPIONAGE AGAINST THE U.S.

On November 20th, the U.S.-China Economic and Security Review Commission report to Congress indicated that the U.S. is vulnerable to cyber espionage by China. According to the report, Chinese cyber operations are so advanced that the U.S. may not be able to counteract them. The report found that China could access an unclassified U.S. military network, which could be used to delay or disrupt U.S. forces. The report also warned that computer parts manufactured in China may be vulnerable to tampering, as counterfeit routers made in China were found in the Defense Department. The Chinese government is also training citizens in cyber operations at military academies.

The Commission's press release on the report may be found at
http://www.uscc.gov/pressreleases/2008/08_11_20pr.php

TEENAGER BROADCASTS SUICIDE ONLINE, WATCHERS MAY BE PROSECUTED

On November 18th, a Florida nineteen year old posted on a message board that he was going to commit suicide and then broadcast it on Justin.tv, which allows users to broadcast live videos on the Internet. Some viewers encouraged the teen, and some discouraged him, and many watched while the teen overdosed on narcotics and collapsed. Some viewers alerted the authorities after the teenager didn't get up. The video kept streaming until authorities arrived, broke down the door and surveyed the scene. Florida authorities are trying to figure out if any of those who encouraged the suicide can be charged under Florida law. The Florida manslaughter law may give prosecutors room to charge people, as it allows people to be charged for "assisting" with suicide or death because of negligence. But it is questionable whether communicating with someone over the Internet rises to the level of culpable conduct necessary to file charges. It would be hard for prosecutors to prove that the watchers knew the teen was going to commit suicide and that this was not an Internet hoax. According to one federal criminal lawyer, proving that state of mind would be nearly impossible.

An initial story on the suicide may be found at

<http://www.guardian.co.uk/technology/2008/nov/22/internet-live-suicide>

A story on the criminal charges may be found at http://news.cnet.com/8301-1023_3-10107351-93.html

HOW TO KEEP LAPTOPS SAFE FOR HOLIDAY TRAVEL

On November 24th, *InfoWorld* published a helpful guide to help keep laptops safe during holiday travel. Airports have become a black hole for laptops, as many are lost or stolen in the rush to catch flights and go through security checkpoints. The article includes ten tips to avoid laptop and data loss. Some of the tips include backing up data before traveling, not checking baggage with a laptop, labeling your laptop so it may be easily identified, putting your laptop in a hotel safe, and not accessing insecure wireless networks.

The full list of tips to keep your laptop safe may be found at

http://www.infoworld.com/article/08/11/24/Ways_to_keep_your_laptop_privacy_safe_during_holiday_travel_1.html

JUDGE ORDERS BALLMER TO TESTIFY IN VISTA CAPABLE LAWSUIT

On November 21st, U.S. District Judge Marsha Pechman ordered Microsoft CEO Steve Ballmer to testify in the "Vista Capable" class action lawsuit. The lawsuit claims that Microsoft labeled some computers as "Vista Capable" when the machines could not support Vista's more advanced features. Microsoft sought to limit depositions in the case to other executives, but the court found that the plaintiffs showed Ballmer had unique knowledge, and ordered him deposed for no more than three hours in the following month. Judge Pechman found that Ballmer's busy schedule did not protect him from the discovery process.

The order may be found at <http://blog.seattlepi.nwsourc.com/microsoft/library/fridaydocument.pdf>

MYSFACE SUICIDE CASE RESULTS IN MISDEMEANOR CHARGES

On November 26th, a federal jury reached a verdict in the country's first cyberbullying case. The accused, Lori Drew, created a falsified MySpace account and pretended to be a boy courting a teenager who committed suicide after "the boy" broke up with her. The jury convicted Drew of three misdemeanor charges, but deadlocked on the fourth conspiracy charge, which was declared a mistrial. Under sentencing guidelines, Drew could face up to three years in prison and a \$300,000 fine, although no sentencing date was set and her lawyer asked for a new trial. The verdict was significant because it was the first time a federal computer fraud statute was used to prosecute someone for essentially breaking the MySpace user agreement.

The story may be found at <http://www.nytimes.com/2008/11/27/us/27myspace.html?ref=todayspaper>

HACKERS ACCESSED ONLINE BILL PAYMENT COMPANY CHECKFREE

On December 2nd, hackers took control of the CheckFree website used for online bill payment. The hackers accessed the website by stealing the username and password used to make account changes at CheckFree's domain registrar. The hackers then redirected the website to a server in the Ukraine that tried to install malicious software on the user's computer. It was unclear how many customers were affected, as the hacking took place during off-peak hours. CheckFree sent an e-mail notice to its customers that stated anyone who accessed their account during a certain window of time and received a blank screen instead of a payment screen may have been affected. The notice also said that CheckFree would provide free versions of McAfee software to remove the threat.

The story may be found at http://voices.washingtonpost.com/securityfix/2008/12/hackers_hijacked_large_e-bill.html

FINES SOUGHT AGAINST MISSOURI GOVERNOR FOR DENYING E-MAIL ACCESS

On December 3rd, investigators filed a revised lawsuit against Missouri governor Matt Blunt accusing him of "knowingly and purposely" violating Missouri's public records law. Allegedly, Blunt and his attorneys denied access to e-mails requested by investigators. According to the lawsuit, the governor and his team raised objections, refused to produce documents and demanded excessive amounts of money for some documents. The lawsuit is part of an ongoing scandal over Blunt's e-mail preservation, and seeks fines and penalties against the governor's office. Blunt claimed that his office had no obligation to save e-mails and could delete them at will. But under state law, e-mails are public records. Some may be deleted, depending on the topic, but some must be saved for three years and some must be saved for the state archives. Blunt did not seek reelection after the scandal, and his term expires within a month.

The story may be found at <http://www.time.com/time/nation/article/0,8599,1864522,00.html>

MAN CHARGED WITH CRIMINAL LIBEL FOR CRAIGSLIST RANT

In October, a Colorado prosecutor charged a man with two counts of criminal libel over posts made in the Craigslist "Rants and Raves" section about his former lover. The posts alleged that she traded sexual acts for legal services and that there was a visit from child services because of an injury to her child. The victim reported the posts to police, and the police charged the writer with criminal libel. Colorado passed its criminal libel law in 1963, which bans statements that "impeach the honesty, integrity, virtue, or reputation or expose the natural defects of one who is alive." Criminal libel statutes are rarely used, as most libel lawsuits are civil. The defendant had not entered a plea, but said that he was "just venting."

The story may be found at <http://abcnews.go.com/US/wireStory?id=6373122>

PRESIDENT BUSH SIGNS CHILD SAFE VIEWING ACT

On December 2nd, President Bush signed the Child Safe Viewing Act, which requires the Federal Communications Commission to research technologies that allow parents to censor what their children watch. The FCC has 270 days to file a report with Congress on the types of technology available, and how to encourage the technologies without affecting communications prices. The Senate passed the bill unanimously and the House passed it without objection.

The text of the bill may be found at <http://thomas.loc.gov/cgi-bin/query/z?c110:S.602>:

TERRORISM IN THE DIGITAL AGE: TECHNOLOGY UTILIZED IN MUMBAI ATTACKS

On December 2nd, the Washington Post reported terrorists in the recent Mumbai attacks utilized technology to carry out the attacks. The attackers used GPS devices and high resolution maps to sail to India from Pakistan. Indian investigators also found that attackers used BlackBerrys and cell phones with switchable SIM cards to make

tracking more difficult. But technology is a two-way street, as victims kept the outside world updated through text messages and Twitter updates to friends and relatives. The technology is also being used to trace the attacks to Pakistan, as an e-mail sent by the organization claiming responsibility for the attacks was traced from a computer server in Moscow and to Pakistan. The attacks show the increasing role of technology in our daily lives, and how it can be utilized in disconcerting ways.

The story may be found at

http://www.washingtonpost.com/wpdyn/content/article/2008/12/02/AR2008120203519_pf.html

SPAM INCREASES AS SPAMMERS FIND NEW HOSTS

On November 26th, security researchers reported that the amount of spam was increasing as spammers found new hosts following the shutdown of a large hosting company weeks before. On November 11th, spam hosting company McColo was shut down, which hosted up to 75% of all spam. In the meantime, the spam levels were fairly flat and only started climbing about two weeks after the initial shutdown. Some botnets that came back online were coming from ISPs outside the United States, which will be harder to shut down in the future. Security experts are hopeful that the shutdown, though temporary, may put some spammers out of business or at least increase their costs.

The story may be found at http://news.cnet.com/8301-1009_3-10109148-83.html

EU FORMS PLAN TO SEARCH FOR CYBER CRIMINALS

On November 27th, the European Union announced a new plan to fight cybercrime. The five year plan includes measures such as cyber patrols, joint investigation teams, and remote searches to help track down and prosecute cyber criminals. According to the EU press release, cyber crime greatly increased in recent years, with particular concern expressed over the increase in child pornography. The new strategy provides for better information sharing between European police forces and the private sector with alerts about cyber crime sprees. The commission allocated 300,000 euros (around \$425,000 US) to the program.

The EU press release may be found at

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827&format=HTML&aged=0&language=EN&guiLanguage=en>

NEW SOFTWARE TO HUNT DOWN BOTNETS

On November 19th, a new software program, BotHunter, was released to help fight botnets that infect users' computers in order to send spam and steal information. The software was funded by a grant from the U.S. Army Research Office, and developed by SRI International. The program is free and available for Mac OS X, Linux/Unix and Windows XP. A Vista version is not available on the website but is coming soon. The program looks for patterns that indicate malware in both incoming and outgoing data on a computer. Several thousand downloads are being used in the U.S. military. About 250 users had reported finding their PCs were being used as participants in botnets.

The BotHunter press release and ongoing news may be found at <http://www.bothunter.net/doc/news.html>

COURT USES FEDERAL RULE OF EVIDENCE 502 TO DETERMINE NO WAIVER

On November 14th, a U.S. District Judge in Pennsylvania applied new Federal Rule of Evidence 502 and found that inadvertent disclosure of over 800 documents did not constitute a waiver. Since inadvertent disclosure was involved, the court applied Rule 502. The court first looked at the three factors laid out in the rule, which are that the waiver was inadvertent, the party took reasonable steps to prevent disclosure and the party attempted to rectify the

error. The court then determined the heart of the dispute was the reasonableness of the precautions, so it looked to five factors laid out in the Advisory Committee Notes, including: 1) the reasonableness of the precautions taken to prevent inadvertent disclosure in view of the extent of the document production, 2) the number of inadvertent disclosures, 3) the extent of the disclosure, 4) any delay in measures taken to rectify the disclosure, and 5) whether the overriding interests of justice would be served by relieving the party of its errors. Here, the court found that the first four factors favored waiver, but that overriding interests of justice for the producing party outweighed the other four. While the producing party did not adequately prepare for litigation, the severity of waiver as a sanction would be unjust. But the court did order that documents that were not entered into a privilege log by a court-specified date should be produced.

The case is *Rhoads Industries, Inc. v. Building Materials Corp.*, and may be found at http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_Rhoads.doc

STUDY FINDS CYBERCRIMINALS PROFITING FROM RECESSION

On December 9th, security firm McAfee published a new report that indicated that cybercriminals are benefiting from lax law enforcement and the economic recession as people may be more gullible to online scams. The report is entitled "Virtual Criminology Report – Cybercrime vs. Cyberlaw," and compiles opinions of professionals in the legal, technology, and research fields. One problem facing law enforcement is that they are not prepared to deal with changing technology, and those trained in technology are lured away from public service to the private sector. Some new schemes intended to exploit vulnerabilities from the economic crisis are phishing e-mails pretending to be resume sites to collect personal details, and fake e-mails from banks claiming to be notices about a bank failure. The report also showed that some countries are more adamant about prosecuting cybercrime than others, and places such as China and Russia have become a safe haven for cybercriminals. According to the report, Russia is the source of the best designed malware.

The report (free with registration) may be found at <http://resources.mcafee.com/content/NAMcAfeeCriminologyReport>

COMPUTER USERS SPREAD MALWARE

On December 17th, security firm Trend Micro announced that most malicious attacks on computers come from a user going to a malicious website and accepting a download. From January to November, the top 100 attack programs infected 53% of victims by getting them to download something, with another 12% coming from e-mail attachments. Only 5% of attacks came from software vulnerabilities, but considering the amount of malware, the number is still large. In North America the chances of being duped into downloading increased, as 63% of the infections from the top 100 pieces of malware were caused by downloading, and only 1.7% came from software bugs. Trend Micro indicated that a solution may be education to prevent users from infecting themselves.

The press release may be found at <http://trendmicro.mediaroom.com/index.php?s=43&item=683>

VIRGINIA ATTORNEY GENERAL APPEALS SPAM CASE TO U.S. SUPREME COURT

On December 11th, Virginia Attorney General Bob McConnell appealed the Virginia Supreme Court's decision overturning the first felony spam conviction in the country to the U.S. Supreme Court. McConnell asked the Supreme Court to reinstate the spam law, which the Virginia Supreme Court struck down on First Amendment grounds. In doing so, the Virginia Supreme Court overturned the conviction of one of the worlds' worst spammers, Jeremy Jaynes. The Virginia law was held overbroad because it was not limited to commercial e-mails, and could include political or religious messages. McConnell claimed that the situation where an imaginary spammer is prosecuted for sending religious e-mails is rare to nonexistent. Jayne's lawyer said it was unlikely that the Supreme Court would hear the case, and if it did, the decision would likely be upheld.

McConnell's press release may be found at http://www.oag.state.va.us/PRESS_RELEASES/NewsArchive/121108_Spam_Supreme_Court.html

COMMISSION RECOMMENDS NEW CYBERSECURITY MEASURES

On December 8th, the Center for Strategic and International Studies Commission on Cybersecurity released a report with recommendations on how to handle cybersecurity. The report calls for a Center for Cybersecurity Operations (CCO) headed by an appointed White House advisor. The CCO would regulate computer security for the public and private sectors, form new rules for cybersecurity, and test computers for vulnerabilities. The Commission found coordination necessary because information about computer threats is not shared throughout the public and private sectors. President-elect Obama seems to be on board with the initiative, as five of the Commission members are part of his transition team. Obama may also appoint a national cybersecurity czar who would report to the President.

The report may be found at http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf

SONY TO PAY CIVIL PENALTY FOR VIOLATING PRIVACY ACT

On December 11th, the Federal Trade Commission (FTC) announced that Sony BMG Music Entertainment would pay \$1 million to settle charges that it improperly collected and disclosed information on children under 13 without parental consent. The penalty matches the largest ever for a civil violation of the Children's Online Privacy Protection Act. Sony operates websites for music fans that require them to register with personal information allowing them to make their own fan page, post to message boards, and engage in private messaging. The FTC press release stated that Sony did this without parental consent, allowing children to interact with adult fans. Under the statute, websites with social networking features such as Sony's are required to get parental consent before collecting, using or disclosing children's personal information. The FTC order also requires Sony to delete any information obtained in violation of the Act, and provides provisions for future compliance.

The FTC press release may be found at <http://www.ftc.gov/opa/2008/12/sonymusic.shtm>

MICROSOFT SAYS IT WILL ANONYMIZE DATA SOONER IF OTHERS FOLLOW

On December 9th, Microsoft endorsed European guidelines that suggest search engines should not keep sensitive information longer than six months without anonymizing the data. While it endorsed the standard, Microsoft said it would not change its own practices unless everyone in the industry agreed to it. Currently, Microsoft retains its data for 18 months before anonymizing it. Privacy advocates warned against keeping data such as IP addresses and tracking cookie information because it can reveal personal information and is kept longer than necessary. It is unclear whether the guidelines can be turned into enforceable law. Current European data protection law has no time limit on data retention time.

The press release may be found at http://www.microsoft.com/emea/presscentre/pressreleases/TrustworthyComputingPR_081208.mspx

FEWER LATE FEES FOR THOSE WHO PAY BILLS ONLINE

On December 8th, online bill payment company Billeo released a survey that found more than half of people who pay bills online never pay late fees. Other findings from the survey included that 75% of those who pay bills online do so for convenience, and most customers save electronic receipts from the bill paying. Credit cards topped the list of types of bills paid online, followed by utilities, telephone services, cable, satellite, wireless, and insurance. The survey indicates the growing comfort and convenience for consumers to conduct transactions online.

The press release identifying the survey results may be found at http://www.billeo.com/images/pdf/Billeo_12-08-2008.pdf

'KOOBFACE' VIRUS FOUND ON FACEBOOK

On December 3rd, McAfee's Avert Labs blog warned that a virus called "Koobface" was targeting Facebook. The virus uses the Facebook messaging system to infect computers, and tries to gather sensitive information. The virus would send a message to friends of someone with an infected computer that would direct the friend to a link where they are asked to download an update to Adobe's Flash Player, which infects the person's computer if downloaded. The infected computer takes the user to infected websites. Users tend to be less suspicious of messages from "friends" on Facebook, making the attack especially potent. Facebook security told members to delete contaminated e-mails and posted directions on how to clean infected computers.

The blog post may be found at

<http://www.avertlabs.com/research/blog/index.php/2008/12/03/koobface-remains-active-on-facebook/>

WEBSITES SHOULD BE TREATED LIKE OTHER ELECTRONIC DOCUMENTS

On October 1st, a U.S. Magistrate Judge for the District of New Jersey ruled that websites should be treated the same as other electronic files, and sanctioned the defendant for failing to maintain its website's content when the dispute arose. In the contract action, when defendants did not produce the website, plaintiff filed a motion for an adverse inference instruction. The court granted the adverse inference instruction because defendants had reason to know that the website could be essential to the litigation after plaintiff filed suit and did not preserve it. The court found that a website was no different than any other electronic file, as defendants had control over the content. Since defendant either willfully withheld or deleted the documents, the court granted the adverse inference instruction.

The opinion may be found at <http://ediscovery.quarles.com/uploads/file/Arteria%20Decision.pdf>

MORE STATES ADD E-DISCOVERY RULES

More states are adding e-discovery rules to their court procedures, with most of them effective sometime next year. Arkansas and Kansas added e-discovery rules for the first time, with Arkansas adding a rule covering inadvertent disclosure of privileged materials and Kansas amending its Rules of Civil Procedure to echo the Federal Rules. Iowa, New York, and North Carolina were other states who updated their e-discovery rules.

The list, with links to the rules, may be found at

<http://www.ediscoverylaw.com/2008/12/articles/news-updates/new-additions-to-the-growing-list-of-state-ediscovery-rules-arkansas-and-kansas-added-for-the-first-time/>

RIAA ANNOUNCES CHANGE IN STRATEGY TO STOP ILLEGAL FILE SHARING

On December 19th, the Recording Industry Association of America announced a drastic change in strategy: it no longer will prosecute individuals for illegal file sharing. Instead, the RIAA will rely on Internet Service Providers to stop the illegal downloads. When the RIAA thinks a user is downloading illegally, it will contact the ISP and the ISP will send e-mail notices to the user. If the illegal downloading continues, the user's Internet service could be watered down or shut off. The RIAA also preserved the right to prosecute the most egregious illegal file sharing offenders. Some privacy concerns are alleviated because the RIAA will not request information - it will just forward its threatening e-mails to the ISP. Some civil liberties groups are concerned that cutting off Internet access could raise First Amendment problems since it interferes with a person's right to communicate.

The story may be found at http://news.cnet.com/8301-1023_3-10126914-93.html?tag=mncol;txt

A copy of the notices from the ISP may be found at http://news.cnet.com/8301-1023_3-10127050-93.html

Comments from the RIAA President may be found at http://news.cnet.com/8301-1023_3-10127313-93.html

PERSONALIZED SPAM MORE PREVALENT IN 2008

On December 15th, Cisco announced in its 2008 Security Report that the amount of personalized spam rose over the past year. For personalized spam, online identity thieves use lists of stolen e-mail addresses or other information about the victims to send personalized e-mails. Unlike traditional spam, which is mostly blocked by filters, personalized spam is not blocked as often because it appears to come from reputable e-mail services. Many of the personalized attacks link to bogus websites that look real or websites that install malicious programs. The study also found that the volume of spam is almost double what it was in 2007, with nearly 200 billion spam e-mails sent each day. New forms of spam include text message spam, e-mails trying to trick administrators into revealing passwords, and e-mails saying there are problems with a personal bank account.

The press release and link to the full study may be found at http://newsroom.cisco.com/dlls/2008/prod_121508.html

YAHOO LIMITS RETENTION OF SEARCH DATA TO 90 DAYS

On December 17th, Yahoo announced that it would limit the time it holds personal information, including search log data, page views, ad views, and ad clicks to 90 days, the lowest among search engines in the United States. To do so, Yahoo will delete the last 8 bits of the IP address associated with a search after 90 days, and will hide cookie data and any other personal information like names, phone numbers, etc. from the query as well. Yahoo said it would have some limited exceptions for fraud, security and legal purposes. The move puts pressure on industry rivals Google and Microsoft, who have retention times of 9 months and 18 months, respectively. Yahoo made the move to make its search engine more attractive to users concerned about privacy.

The Yahoo press release may be found at <http://yhoo.client.shareholder.com/press/releasedetail.cfm?ReleaseID=354703>

HACKERS FINALLY UNLOCK IPHONE 3G

On December 31st, the iPhone Dev-Team will release instructions on how to unlock the iPhone so it can run on networks other than AT&T. The unlock requires that an iPhone 3G be running version 2.11.07 or earlier baseband, which is the software that controls the cell phone part of the iPhone. The team also intends to release an unlocking software program that can be run by most iPhone users. Unlocking the iPhone has been a never-ending struggle between Apple and hackers. Apple continues to put obstacles in the way of hackers trying to unlock the iPhone, but to no avail.

The story may be found at <http://blog.iphone-dev.org/post/65126957/tis-the-season-to-be-jolly>

NEW YORK CONSIDERS TAXING ITUNES DOWNLOADS

On December 16th, the *New York Daily News* reported that New York state could soon impose a tax on iTunes downloads. New York has a \$15.4 billion deficit, so Governor David Patterson proposed the "iPod tax" to bring in extra revenue. The tax technically is for "digitally delivered entertainment services," which would include other media besides iTunes, such as e-books downloaded from Amazon.com for the Kindle. The tax would also apply to sporting events, movie tickets, taxis, and satellite TV and radio. In taxing downloads, New York would be joining 17 other states that already tax downloads, including New Jersey, Alabama, Arizona, Colorado, Hawaii, New Mexico, Texas and Washington. Other states such as California and Wisconsin considered taxing downloads but the proposals were defeated.

The story may be found at http://www.nydailynews.com/ny_local/2008/12/16/2008-12-16_gov_david_paterson_unveils_dire_new_york.html

SURVEY ANNOUNCES TOP 20 COMPANIES FOR PRIVACY IN 2008

On December 15th, the Ponemon Institute and TRUSTe announced the results of their annual survey of the most trusted companies for privacy. The study surveyed 6,486 adults about the most trustworthy companies and those that best safeguarded personal information. American Express topped the list, followed by eBay, IBM, Amazon, Johnson & Johnson, Hewlett Packard, U.S. Postal Service, Procter & Gamble, Apply, Nationwide, and Charles Schwab to round out the top ten. Most of those companies were on the list before, but Apple, Yahoo, Facebook, Verizon, and FedEx were new to the top 20. Google dropped from the top 20, as it was ranked number 10 last year, but other technology companies such as Apple, Yahoo and Facebook improved their rankings. The press release noted that Facebook's appearance on the list was especially significant as it indicated increased trust in social networking.

The TRUSTe press release may be found at http://truste.org/about/press_release/12_15_08.php

COURT ADDRESSES METADATA PRODUCTION IN DETAIL

On November 21st, the U.S. District Court for the Southern District of New York considered a discovery dispute over metadata production. In this class action lawsuit concerning unlawful searches and seizures of plaintiffs' homes, the issue of metadata production arose after the defendants had already produced its electronic discovery and the parties could not reach an agreement over what metadata should be produced. The court recognized that metadata production is not specifically mentioned in the Federal Rules of Civil Procedure, but is subject to general discovery rules. The court found that metadata must be produced if it is relevant to the claim or defense of any party and is also subject to the balancing test of Rule 26(b)(2)(C) that requires a court to balance the probative value against the burden of production. The court then took these general principles and applied them to the specific types of metadata plaintiffs requested. The court denied production of metadata from e-mail on backup tapes, as the burden of production was too high and the likely benefit low, but the court ordered that defendants' produce metadata for e-mail with metadata already intact. The court granted plaintiffs' request for metadata from Word and PowerPoint documents, but ordered that plaintiffs pay all costs for producing this metadata. The court also denied production of metadata from Excel spreadsheets, as plaintiffs did not show any indication of fraudulent modification and the metadata was likely irrelevant, but the court did order defendants to produce the spreadsheets in native format since defendants were willing to do so. Finally, the court ordered defendants to provide a live demonstration of one of its databases where plaintiffs sought to see how and when incident reports were modified.

The case is *Aguilar v. Immigration and Customs Enforcement of the U.S. Department of Homeland Security*, and the opinion may be found at http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_Aguilar.doc

Bytes in Brief[®] is a FREE monthly digest of Internet law and technology news delivered to you by e-mail. For members of the legal and business community interested in Internet law and technology developments, *Bytes in Brief* provides a synopsis of related news and links to sources with more expanded coverage. In the time it takes to drink a cup of coffee, *Bytes in Brief* is designed to make sure you are tracking major developments in this fast moving area.

If staying current in this field is important to you and you find yourself buried under unread magazines, newspapers and journals, *Bytes in Brief* can help you stay in touch without a major outlay of time or expense.

To subscribe, enter your e-mail address into the sign-up box below. It will take you offsite to the *Constant Contact* website, where our opt-in only list is maintained and updated. After you confirm your e-mail address, you will receive an e-mail asking for confirmation that you do wish to become a *Bytes In Brief* subscriber. Once you reply to that e-mail, you will be added to the subscription list.

Subscribe to *Bytes in Brief*

Email:

Privacy by  SafeSubscribeSM
For Email Marketing you can trust

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