

{ 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 141 - February 2009

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

INTERNET SURPASSES NEWSPAPERS AS NEWS SOURCE

On December 23rd, the Pew Research Center for the People & the Press reported that more people get news from the Internet than newspapers, as 40% of people surveyed received news online while only 35% read newspapers. Television continued to be the most prevalent source of news, as 70% of those surveyed said they got their news from television. But 59% of Americans younger than 30 said their news source was the Internet, with an identical number getting their news from television. The number of young television news viewers was down from 68% in September. While that number changed, there was little change in the source of news, as 23% watch CNN and 17% watch Fox News.

The story may be found at <http://people-press.org/report/479/internet-overtakes-newspapers-as-news-outlet>

NEW TOOL PREVENTS TEENS FROM USING CELL PHONES WHILE DRIVING

On December 11th, University of Utah researchers released a new device to prevent teens from talking or texting on cell phones while driving. The device, called the Key2SafeDriving, disables cell phones when a special car key is inserted in the ignition. The key then wirelessly disables the cell phone through Bluetooth or RIFD. The only calls allowed through would be 911 calls, or calls to specifically programmed numbers, for instance, so the teen could call home. Any other calls or text messages will receive a message that says, "I am driving now." The university licensed the invention to a private company that hopes to make the device available through insurance companies and cell phone service providers within six months. An estimated cost was \$50 per key plus an undetermined monthly service charge. Note from the editors: There are all kinds of articles on how to bypass this. The simplest is to disable Bluetooth on the phone.

The university press release may be found at <http://www.unews.utah.edu/p/?r=120808-1>

MICROSOFT EXTENDS XP CUTOFF - AGAIN

On December 19th, *Channel Web* reported that Microsoft's cutoff date for XP would be extended four months, from January 31st to May 30th for custom computer builders. System builders are smaller build to order vendors, compared to larger companies like Dell and HP. The deadline for the larger vendors was already extended to July 31st. The extension comes from growing dissatisfaction with Windows Vista, as few large businesses have upgraded to Vista because of the system requirements and lack of compatibility with older software. Most companies are still using seven year old XP instead of Vista, and the latest XP extension is another indication of Vista's failure with businesses.

The story may be found at <http://www.crn.com/software/212501445>

FAKE “CLASS OF 2013” FACEBOOK GROUPS STARTED BY SPAM MARKETERS

On December 18th, a Butler University admissions official reported that many of the “Class of 2013” Facebook groups for various universities may have been started by a spam company. Patrick Kelly, who was not on the admissions rolls to the university, started the group for Butler. The official, Brad Ward, dug further and discovered that administrators who started the groups had common names, and urged university officials across the country to start “official” Facebook groups for incoming students. A company called “College Prowler” may have been the source of the groups, as chief executive Luke Skurman admitted that his company had been involved in making the groups. The supposed purpose was to inform students about a free guide on the College Prowler website, and no messages or wall posts were sent by College Prowler administrators. Skurman also tried to blame the groups on an unnamed company working with College Prowler. Incoming college students beware – that Facebook group may not be the best place to meet your new “classmates.”

The blog post may be found at <http://squaredpeg.com/index.php/2008/12/18/facebook-pay-attention/>

GOOGLE RELEASES BROWSER SECURITY HANDBOOK

On December 11th, Google released its Browser Security Handbook, a guide for web developers that highlights the key security features of the major web browsers. The browsers include Internet Explorer 6 and 7, Firefox 2 and 3, Apple Safari, Opera and Google’s Chrome and Android. The handbook has three parts, dealing with general features of browsers, security features, and weaknesses. Google developer Michal Zalewski stated that the handbook was developed because most security vulnerabilities exist as a result of misunderstandings surrounding browser vulnerabilities.

The handbook may be found at <http://code.google.com/p/browsersec/wiki/Main>

VERIZON GETS \$33 MILLION JUDGMENT AGAINST CYBERSQUATTERS

On December 24th, Verizon announced that it received a \$33.15 million judgment in what it deemed the largest cybersquatting judgment to date. Cybersquatting is the practice of using similar domain names for a major brand that link to spam or junk websites. The judgment was against OnlineNIC, a domain registrar based in San Francisco, who did not show up to court. The company registered at least 663 domain names identical or similar to Verizon’s trademark, and the judge awarded \$50,000 per domain name. While Verizon received a large award, it may have trouble collecting as OnlineNIC has concealed its employees’ identities through shell entities, fictitious names, and deceptive contact information. Regardless of whether it collects, Verizon hoped that the judgment would deter other cybersquatters, who may be punished through the 1999 U.S. Anti-Cybersquatting Consumer Protection Act.

The Verizon press release may be found at <http://newscenter.verizon.com/press-releases/verizon/2008/court-awards-verizon.html>

RESEARCHERS DISCOVER UNDETECTABLE PHISHING ATTACK

On December 30th, security researchers released a paper detailing an undetectable phishing attack by exploiting the algorithms used to protect secure websites. Hash values are unique numbers given to website certificates that identify the document and ensure that it is not modified in transit. But a hashing algorithm called MD5 has a vulnerability that makes it possible to have one legitimate website and one phishing website with the same hash value for their SSL (Secure Socket Layer) certificate. The researchers used about 300 Sony Playstation 3s to build a “rogue certificate authority” that could issue bogus hash values. The researchers admitted that it would be hard for the attack to take place in the real world because the phishing attack must trick the victim into going to the malicious website hosting the fake certificate. The researchers said that the MD5 algorithms should be replaced with more secure algorithms.

The researchers’ paper may be found at <http://www.win.tue.nl/hashclash/rogue-ca/>

CALIFORNIA OUTLAWS DRIVING WHILE TEXTING

On January 1st, California drivers will no longer be able to text message while driving. The state legislature passed, and Governor Arnold Schwarzenegger signed, a law expanding the ban on talking on a cell phone while driving without a hands free device. Violators will be fined from \$20 to \$50. The bill authored by state senator Joe Simitian "closes the loophole" left open by the previous law.

The story may be found at http://www.senatorsimitian.com/news/entry/new_year_means_new_laws_taking_effect/

DATA BREACH TOTALS ROSE SIGNIFICANTLY IN 2008

On January 5th, the Identity Theft Resource Center announced its year-end statistics for data breaches, including a 50% increase in data breaches from 2007. 656 breaches were reported in 2008, up from 445 in 2007. Divided between industries, 37% of the breaches came from businesses, 20% from schools, 16% from government, 15% from the health/medical field, and 12% from the financial/billing industries. The threat from prior employees more than doubled from 7% in 2007 to 16% in 2008, which the ITRC stated could be due to the economy, an increase in organized crime rings using company insiders, or better protection against hackers that led to less insider threat detection.

The ITRC press release may be found at http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml

FISA APPEALS COURT SAYS WARRANTLESS WIRETAPPING OK

On January 15th, the Foreign Intelligence Surveillance Court of Review released a redacted opinion of an August 2008 decision that ruled that federal agencies could conduct warrantless surveillance for national security purposes. The case arose after a telecommunications company filed suit challenging the surveillance law. The court dealt with whether the Fourth Amendment prohibition on unreasonable searches and seizures applied to intelligence agencies compelling telecommunications companies to open their networks for surveillance purposes. The court found that the Fourth Amendment was no bar as long as the executive branch had safeguards in place to protect individuals against unwarranted surveillance. The court also stated that courts should not frustrate executive branch efforts to protect national security.

The redacted opinion may be found at http://www.uscourts.gov/newsroom/2009/FISCR_Opinion.pdf

HOUSE PUTS NET NEUTRALITY IN STIMULUS PACKAGE

On January 15th, the House of Representatives released its economic stimulus package which included Net neutrality rules. Democrats are using the urgency of the stimulus package to sneak in Net neutrality rules, as the bill allocates billions of dollars in grants for broadband and wireless development in "unserved" and "underdeserved" areas. The grants go to various parties, including telecommunications companies, state and local governments, and other businesses that may be interested, but have Net neutrality strings attached. The recipients must adhere to the FCC's 2005 broadband policy statement and operate the broadband and high speed wireless networks on an "open access basis." The move is sneaky considering the controversy surrounding Net neutrality, and since the Senate is planning to address the issue soon. Critics stated that there was no need for such a contentious issue to be crammed into an emergency stimulus package, and that the requirements could be imposed retroactively if necessary.

The 258-page legislation (see p. 38-58 for the Net neutrality provisions) may be found at <http://appropriations.house.gov/pdf/RecoveryBill01-15-09.pdf>

WHITE HOUSE ORDERED TO MAKE LAST MINUTE ATTEMPT TO SAVE E-MAILS

On January 14th, U.S. District Judge Henry H. Kennedy issued an emergency order requiring the White House to search staff workstations, personal storage table files, and to turn over any media devices such as CDs, DVDs, memory sticks, or external hard drives that may have e-mails from the period from March 2003 to October 2005. The order was in connection with a lawsuit filed in September 2007 by the National Security Archive to compel the White House to preserve its e-mails. The Archive was concerned that the Bush e-mails will be lost when the Obama Administration takes over. The order was issued in response to a hearing at which the White House admitted that it had done little to nothing to recover e-mail files from computer workstations and external media devices. But the White House lawyers also stated at the hearing that they located about fourteen million missing e-mails and that a major restoration project was underway to recover missing e-mail from backup tapes. On January 15th, Magistrate Judge John Facciola, who is overseeing the White House e-mail litigation, enforced Judge Kennedy's emergency order.

The Archive press release, with links to the orders may be found at <http://www.gwu.edu/~nsarchiv/news/20090115/index.htm>

NEW YORK COURT SAYS AMAZON MUST COLLECT SALES TAX

On January 12th, New York Supreme Court Justice Ellen Bransten ruled that Amazon.com and other online retailers should continue to collect sales tax on shipments into New York. Amazon was collecting the tax as its legal challenge was pending. Typical sales tax laws require the taxes only to be collected in states where they have a physical operation. Amazon and other online retailers such as Overstock.com do not have physical operations in New York but ship items there. Bransten found that Amazon should not be able to escape sales tax by collecting indirectly, as Amazon has affiliates and partners in the state.

The decision may be found at <http://graphics8.nytimes.com/packages/pdf/technology/amazon.pdf>

INTERNET RISK TO CHILDREN LOWER THAN EXPECTED

On December 31st, the Internet Safety Technical Task Force issued its long-awaited report indicating that children and teens are less vulnerable to online predators than many had feared. The group was formed last year as a result of an agreement between MySpace and 49 state attorneys general. The report found that the most salient threat faced by minors online was bullying and harassment, because as many as 49% of youths said they were bullied or harassed. While adult predators were a concern, a majority of youths were not in danger of being harmed by an adult they met online. In fact, most youths interacting with adults were not victims of deception, as they knew that they were interacting with adults. Most importantly, the task force found that the risks online were not any different from the risks to youths found offline, and that minors that are at risk offline are often at risk online as well. The study also looked at age verification technologies and concluded that age verification technologies could be used for adults, but did not have the same viability for minors because of the few public records for minors. No technology provided a complete solution, and the report indicated that ultimately, a combination would probably be necessary but not foolproof.

The report may be found at <http://cyber.law.harvard.edu/pubrelease/isttf/>

TEEN CONVICTED OF MURDER OVER VIDEO GAME

On January 12th, a judge convicted seventeen year old Daniel Petric of murder after the teen shot both his parents, killing his mother, after they took the video game Halo 3 away from him. His father survived the attack, which occurred after weeks of planning by the teen. The teen tried to implicate his father by placing the gun in his father's hand, and fled the scene with nothing but the game. Defense attorneys argued that the teen was not guilty by reason of insanity, as he was dangerously addicted to Halo 3. Judge James Burge rejected the insanity plea, though he found that the teen probably did not know that his parents would be gone forever if he shot them. The judge found that while the teen was addicted, he also had planned the crime for weeks. The teen was tried as an adult and faces life in prison without possibility of parole.

The story may be found at http://news.yahoo.com/s/ap/20090113/ap_on_re_us/pastor_s_wife_slain/a>

NEW PROGRAM REQUIRES NON-U.S. VISITORS TO REGISTER ONLINE

On January 12th, the Department of Homeland Security will require travelers from 35 countries including the United Kingdom, Germany, Japan, Australia, and others to register online before they can travel to the United States. The registration takes place through the Electronic System of Travel Authorization (ESTA), where the traveler fills out an online form that is checked against DHS databases to determine whether the person poses a security risk. Information required includes: biographical data, data on communicable diseases, arrests & convictions for certain crimes, and mental disorders that could be a threat to others. The program lets the traveler know within minutes whether he or she has been approved. If the application is not approved, the traveler can still apply for a visa to travel to the U.S. If a traveler does not have Internet access, a third party may file the application on the traveler's behalf. DHS Secretary Michael Chertoff stated that the program gives authorities more time to screen for threats and that many travelers used the system during the voluntary trial period without issue.

The DHS press release may be found at http://www.dhs.gov/xnews/releases/pr_123177155521.shtm/a>

JUDGES TAKE DIFFERENT VIEWS ON WHETHER SEARCH OF HANDHELD DEVICE DURING ARREST IS LEGAL

Two recent court decisions by the Southern District of Georgia and the Southern District of Florida came to two different conclusions on whether police should be able to search handheld devices such as mobile phones as an incident of arrest. The issue came down to whether handheld devices should be treated as traditional "containers" under the law. On December 22nd, U.S. District Judge William Zloch ruled in a case involving a drug bust where a DEA agent examined the defendant's two cell phones during the booking process. The Southern District of Florida judge found that the evidence obtained from the search should be suppressed because the search was not incident to lawful arrest, as it took place during booking. Judge Zloch also found that the DEA agent lied when he said that he conducted the search to ensure the text messages would not expire, as the real reason was to find incriminating evidence. The search required a warrant because "searching through information stored on a cell phone is analogous to a search of a sealed letter, which requires a warrant." But Judge B. Avant Edenfield of the Southern District of Georgia disagreed in a similar case decided on January 5th. In that case, police responded to a call about a parked car and scrolled through the photos on the cell phone of the driver and found images of what appeared to be a fourteen-year-old girl in lewd poses. The driver was charged with possession of child pornography. Judge Edenfield ruled that the evidence was admissible, because the cell phone was a container found on the driver's person, as part of a search incident to lawful arrest. The split highlights the issue of whether cell phones are like physical containers or are entitled to more protection because of the uniquely personal nature of the contents.

The story initially reported by Cnet may be found at http://news.cnet.com/8301-13578_3-10140373-38.html

JUDGE HEARS MOTION TO DISMISS MYSPACE SUICIDE CONVICTION

On January 8th, U.S. District Judge George Wu heard oral arguments in an appeal by Lori Drew, who was convicted in November of three misdemeanor counts of accessing computers without authorization. The defense argued that the computer fraud law was improperly used to convict Drew, who created a fake MySpace profile and pretended to be a teenage boy courting thirteen-year-old Megan Meir, who committed suicide after the boy broke off their relationship. If Judge Wu grants the motion, he would set aside the jury's verdict and enter in a judgment of acquittal. Judge Wu had not made a decision at the end of oral argument, and was expected to issue a written opinion, though he did not say when. If the conviction stands, Drew faces up to three years in prison and a \$300,000 fine.

The story may be found at <http://www.google.com/hostednews/ap/article/ALeqM5gg5xCtQtLBF6vJqWXStItGEOsJfwD95J8FJ80>

TEXT MESSAGES HELP CATCH CARJACKERS

On January 7th, Alan Heuss was sitting in his car at night with the engine running when a man with a gun approached him and took his car, cell phone, and some cash. Heuss and his friends filed a police report and then came up with their own scheme to outsmart the carjackers. His friends suggested they try to contact the carjackers via Heuss's stolen cell phone. They sent text messages saying that they had "hot chicks and drugs," with an address to report to. Stupidly, the carjackers went to the address in the stolen car and were met by police.

The local news report may be found at

http://www.10tv.com/live/content/local/stories/2009/01/09/story_carjacking_text.html?sid=102

GOOGLE NAMED TO TOP TEN LIST FOR SPAM ABUSES

On January 6th, *Internet News* reported that Google reached number three on the Spamhaus Project's list of worst spam problem networks. Google joined the list about a month ago and had been steadily climbing as the problems were unresolved. According to the list, Google has thirty-one unresolved issues, which include many types of fraud and spam gangs. A Google spokesperson indicated that Google is working to fix the problems. Spammers also have been using Google Docs to lure visitors to tainted websites. Gmail is also a frequent source of spam because the service is free, there is no meaningful account validation, and users tend to use weak passwords so hijacking accounts is fairly easy. Richard D.G. Cox, chief information officer at Spamhaus indicated that a company with vast resources like Google should be able to better fight these threats.

The story may be found at

<http://www.internetnews.com/security/article.php/3794591/Spammers+Help+Push+Google+to+Dubious+Milestone.htm>

FAKE LINKEDIN PROFILES LINK TO MALWARE

On January 5th, the Trend Micro Malware Blog reported that fake LinkedIn profiles were linking to malware. The fake profiles took celebrity names including Victoria Beckham, Christina Ricci, Kirsten Dunst, Salma Hayek, and Kate Hudson, and created profiles such as "Beyonce Knowles Nude." Once users were lured to the website, the links sent the user to malware sites that if clicked on would install Trojan software. Cybercriminals buy and sell pre-registered profiles on social networks to launch attacks. Previously, the attacks were limited to social networking sites such as Facebook or MySpace, but cybercriminals have branched out to professional networking sites.

The story may be found at <http://blog.trendmicro.com/bogus-linkedin-profiles-harbor-malicious-content/>

COMCAST REMOVES FILE SHARING BLOCKS AFTER FCC ORDER

On January 5th, Comcast sent a letter to the Federal Communications Commission (FCC) indicating that it no longer slows down or blocks peer-to-peer (P2P) traffic on its networks. Comcast issued the letter in response to formal complaints filed with the FCC that Comcast violated the FCC Internet Policy Statement. Comcast reiterated its commitment to provide customers with information about its services, and published its network management practices on its website. Comcast also took steps to move to a "protocol-agnostic" method of network management, which handles traffic without regard to the source, content or applications moving across the network.

The letter may be found at

<http://downloads.comcast.net/docs/comcast-nm-transition-notification.pdf>

COURT RULES IN FAVOR OF ONLINE VIDEO SHARING SITE

On December 29th, U.S. District Judge A. Howard Matz of the Central District of California ruled that the Digital Millennium Copyright Act (DCMA) protects online video sharing sites from copyright violations if they abide by takedown notices under the DCMA. Universal Music Group filed suit against Veoh claiming that Veoh violated copyright laws because it allowed users to upload and store copyrighted videos. Judge Matz found that Veoh's business model complied with the "safe harbor" provisions of the DCMA and that copyright law precluded the sites' liability for storage at site users' discretion. In August, a San Jose Magistrate Judge dismissed a similar lawsuit against Veoh filed by a pornography company.

The decision may be found at <http://blog.wired.com/27bstroke6/files/matz.pdf>

TWITTER BRINGS IN THE NEW YEAR WITH PHISHING ATTACKS AND HACKING<

On January 3rd, Twitter users were hit with a phishing attack. Direct messages were sent to Twitter accounts telling users to visit a website with a "funny blog about you." The URL then redirected users to a login page that looked like the Twitter homepage, but was actually an imposter called twitter.access-logins.com that pretended to be Twitter in an attempt to steal login information. Affected accounts sent messages to other accounts with the same phishing messages. As many people use the same username and password for multiple accounts, this phishing attack is another example of why using the same username and password is not smart. Twitter received more bad news on January 5th when it learned that CNN anchor Rick Sanchez's account had been hacked. Sanchez's account displayed the message "I am high on crack right now might not be coming into work today." Sanchez posted a reply message that his account had been hacked. About 33 other accounts were hacked, including the accounts for Fox News and Britney Spears. The Twitter blog indicated that the hacking was separate from the phishing attack. The hacker gained access to some of the tools the Twitter support team uses to help people change their passwords when they forget them. The Twitter blog indicated that the tools were taken offline and would be put back when secure.

The Twitter blog post about the phishing attack may be found at <http://status.twitter.com/post/68196572/dont-share-your-secret-info>

The Twitter blog post about the hacking may be found at <http://blog.twitter.com/2009/01/monday-morning-madness.html>

CALIFORNIA ENACTS LAW TO STOP CYBER-BULLYING

On January 8th, the Washington Post reported that a California law went into effect that would allow schools to suspend or expel students who commit cyber-bullying. Cyber-bullying has become a major concern, as children are using the Internet, cell phones, or other electronic devices to harass each other. The worst cases have ended up with children committing suicide over the harassing messages. According to a study, four in ten teenagers had experienced some form of cyber-bullying. At least 12 other states have passed cyber-bullying laws, including Arkansas, Delaware, Idaho, Iowa, Michigan, Minnesota, Nebraska, New Jersey, Oklahoma, Oregon, South Carolina and Washington. The laws do not proscribe their own solutions, but notify schools that cyber-bullying is an issue that needs to be addressed. But trying to contain cyber-bullying is problematic for schools, as it is difficult to investigate, educators may not understand the technology, and there are First Amendment concerns attached to controlling what students say outside of school.

The story may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2008/12/31/AR2008123103067.html>

METADATA RAISES ETHICAL ISSUES FOR ATTORNEYS

On January 5th, LLRX.com published an article by Jim Calloway explaining what metadata is and detailing an attorney's ethical obligations when dealing with metadata. Metadata is information about a digital document that is not immediately visible to the naked eye, such as the dates it was edited, who edited it, the changes made to the

document, and comments that the editing party made about the document. One concern for attorneys is that metadata could reflect the other side's strategy, legal issues, or legal advice. The major issues raised by the article are whether an attorney can look at metadata sent by opposing counsel, and if a document contains revealing metadata, what should be done in response? The article goes through the various state ethics opinions dealing with metadata, which conclude that an attorney has an ethical obligation to exercise care in transmitting electronic documents to ensure that the document does not contain metadata. According to some opinions, there also is an ethical duty on the receiving attorney not to look for metadata that may contain confidential information. Ultimately, it is essential for an attorney to understand how metadata works and its implications, to avoid inadvertently sending information that would damage his or her client.

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

SUPREME COURT REFUSES TO HEAR ANTI-PORN LAW CASE

On January 21st, the Supreme Court effectively killed the Child Online Protection Act (COPA), by refusing to hear the government's appeal of an appeals court ruling that declared the law unconstitutional. The American Civil Liberties Union filed suit claiming that the law was so overly broad and vague that ordinary publishers would be affected. The Supreme Court issued two preliminary rulings in the case in 2002 and 2004, sending the case back to the appeals court the first time, and the second time issuing a temporary injunction preventing prosecutors from enforcing COPA. But the Court refused to hear the case a third time without providing an explanation. Critics of COPA hailed the decision not to hear the case as a victory for First Amendment rights, as children can be protected online without compromising First Amendment principles.

The story may be found at http://news.cnet.com/8301-13578_3-10147171-38.html

MAN MURDERS WIFE OVER HER FACEBOOK STATUS

On January 23rd, the BBC reported that a man was convicted of killing his estranged wife over her Facebook status. Forty-one year old Edward Richardson, of the United Kingdom was "enraged" after he saw that his estranged wife, Sarah, changed her Facebook marital status from "married" to "single." He decided to see Sarah since she was not responding to his messages, and stabbed her to death after breaking into her house. Richardson tried to take his own life after he took Sarah's. Richardson was sentenced to life with a minimum of seventeen years in prison.

The story may be found at <http://news.bbc.co.uk/1/hi/england/staffordshire/7845946.stm>

HEARTLAND DATA BREACH COULD BE BIGGER THAN TJX'S

On January 20th, Heartland Payment Systems, a company that processes credit and debit card transactions, announced that its credit card systems had been compromised sometime last year. Hackers placed malicious software on the system to steal card data on the company's networks. Visa and Mastercard alerted Heartland of suspicious activity, which caused the company to conduct a forensic investigation and discover the breach. Apparently no merchant data, cardholder social security numbers, unencrypted PIN numbers, addresses, or phone numbers were compromised. But it appeared that the hackers obtained the Track 2 data from the magnetic strip on the back of the cards, which is all that is needed to make counterfeit cards. Heartland processes at least 100 million credit card records per month, meaning that many cards, if not more, could have been compromised. The TJX data breach, the largest to date, compromised 45 million cards.

The story may be found at http://www.infoworld.com/article/09/01/21/Heartland_data_breach_could_be_bigger_than_TJXs_1.html

OHIO SUPREME COURT ORDERS PUBLIC BOARD TO PAY TO RECOVER ITS DELETED E-MAILS

On December 9th, the Ohio Supreme Court ordered the Seneca County Board of Commissioners to pay for forensic recovery of its deleted e-mails. The case stemmed from a records request from the *Toledo Blade* for e-mails concerning the Board's decision to demolish the county courthouse. The Board could not produce the e-mails because the e-mails were deleted, and the *Blade* filed a writ of mandamus to compel the Board to forensically restore the e-mail. The court granted the writ, finding that the Board deleted e-mail in violation of its own retention policy. The *Blade* produced sufficient evidence to show that the e-mails still existed on the Board's computers even though they were deleted, and that the e-mails had significant value to the litigation. The court considered shifting the cost of the forensic analysis to the *Blade*, but decided against it because the requesters of information under the Ohio statute are not required to pay for the costs of their requests.

The court opinion may be found at

http://www.sconet.state.oh.us/Communications_Office/summaries/2008/1209/071694.asp

ARIZONA COURT HOLDS METADATA NOT A PUBLIC RECORD UNDER AZ LAW

On January 13th, the Arizona Court of Appeals held that metadata is not a public record under Arizona law. The case arose out of an Equal Employment Opportunity Commission complaint against the City of Phoenix. The plaintiff made public records requests, and the city replied with paper documents that had been backdated. The plaintiff then filed a motion to compel the production of metadata connected with the documents, and the city refused, arguing that metadata was not a public record. The court agreed with the city, and went through the three definitions of a public record recognized by the Arizona courts. The court found that metadata did not fit into any of the three definitions, as the metadata was generated by a computer automatically, not by an officer manually. While there was normally a presumption for production of public records, since the court found that metadata was not a public record, the presumption did not apply.

The opinion may be found at

http://www.ediscoverylaw.com/uploads/file/Westlaw_Document_Lake.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
