

# { bytes in brief }

LAW AND TECHNOLOGY NEWS MONTHLY

EDITORS: Sharon D. Nelson, Esq. and John W. Simek  
ASSOCIATE EDITOR: Jason R. Foltin EDITOR EMERITUS: G. V. Nelson



© 2009 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

## Issue 148 - September 2009

**PLEASE NOTE:** The URLs referenced in Bytes frequently link to newspapers and other current news sources. These links may fail over time. [Click here to visit Sensei's home page at www.senseient.com](http://www.senseient.com)

---

### DEFAMATION LAWSUIT FOR US TWEETER

On July 29th, BBC News highlighted a recent lawsuit filed by Horizon Group Management against a former tenant who complained about mold in her apartment on Twitter. The complaint accused Amanda Bonnen of defaming the company when she posted a tweet saying "Who said sleeping in a mouldy apartment was bad for you? Horizon really thinks it's okay." The company claimed that the tweet was published throughout the world and severely damaged its good name; however, Horizon's Jeffery Michael admitted that he never had a conversation about the post and never asked her to take it down. Rather, he explained that "we're a sue first, ask questions later kind of organization." In damage control mode, Mr. Michael later apologized for the remark and explained that no mold was ever found in the apartment and that, save for this one instance, all other tenant grievances have been quickly and amicably resolved. While in its complaint Horizon is seeking \$50,000 in damages, the unwanted publicity might have the company reconsidering whether this lawsuit is really worth it. Once word of the lawsuit broke, floods of comments came pouring in; many either bashing the company or proclaiming that Twitter is free speech and should be protected. A copy of the story may be found at <http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/8173731.stm>

---

### REPORT: SPAM AND MALWARE AT ALL-TIME HIGHS

On July 29th, CNET News reported that the spam and malware pandemic has reached all-time highs. Even after last year's shutdown of the McColo ISP, McAfee estimates that spam still accounts for 92 percent of all e-mail. The most likely source for spam production is still the United States, even though the amount of worldwide spam originating from the U.S. has dropped steadily over the last three quarters. Other major producers include Brazil, Turkey, India, and Poland — all of which have seen sizable increases in producing spam. Zombies and botnets are also on the rise, thanks in large part to all the unprotected home computers. In fact, McAfee reported that there were almost 14 million new zombies in action over the second quarter alone, a rise of more than 150,000 new threats each day. Another major threat on the rise is AutoRun malware, which is triggered automatically when a person plugs in a USB stick, memory card, or other external device. Alarmingly, McAfee reported that in one 30-day period, it uncovered AutoRun malware in more than 27 million infected files. Finally, the report noted that the new hot spot for cyber criminals is social networking sites. On Facebook, people freely access different applications that require a username and password, so those apps can easily tap into their accounts. Twitter too has seen its share of threats. A recent attack by a JavaScript worm exploited a hole to infect users' profiles and a French hacker was able to gain access to the account of a Twitter product director. McAfee's second quarter threat report may be found at [http://www.mcafee.com/us/local\\_content/reports/6623rpt\\_avert\\_threat\\_0709.pdf](http://www.mcafee.com/us/local_content/reports/6623rpt_avert_threat_0709.pdf)

---

### SOCIAL-NETWORKING BAN FOR SEX OFFENDERS: BAD CALL?

On August 13th, Illinois Governor Pat Quinn signed a law effectively banning registered sex offenders from using social networking sites and, with the way the law defines social networking services, quite possibly any site that allows visitors to register and leave comments. While Illinois' attempt to prevent sex offenders from turning these sites into hunting grounds is virtuous, many believe that the law will do more harm than good. First and foremost, opponents of this type of legislation have argued that reports show the risk of online predators is greatly exaggerated. They point to a January 2009 analysis of Pennsylvania cases which found, during a four year period, that "only eight incidents involved actual teen victims with whom the Internet was used to form a relationship,

compared to 9,934 children who were sexually abused in a single year in that state.” Another problem highlighted by the opposition has been the classification of sex offenders. In their opinion, not everyone on every state sex offender list is a danger to children. Opponents have also explained that these kinds of laws may further lull social network users into a false sense of security. The law only prevents registered sex offenders from using social networking sites, but it cannot prevent those who have yet to be caught and convicted from logging on. Finally, there are many other problems that people may lose sight of — bullying, harassment, and impersonation — if the focus is solely on predation. A copy of the story may be found at [http://news.cnet.com/8301-13578\\_3-10309431-38.html](http://news.cnet.com/8301-13578_3-10309431-38.html)

---

## **IPHONE VULNERABLE TO ATTACK**

On July 29th, researchers demonstrated how an attacker can take complete control of a victim's iPhone simply by sending special SMS control messages — which are different than your everyday SMS text message — to the person's device. The attack is enabled by a serious memory corruption bug in the way the iPhone handles SMS messages and effectively allows an attacker to make calls, steal data, send text messages, and do more or less anything a person can do on their iPhone. This attack is much different than previous attacks which required an attacker to either lure iPhone users to a malicious website or open a malicious file because an attacker only needs to have the victim's phone number. Making matters worse, once inside the phone, an attacker can spread the attack from phone to phone by sending an SMS to anyone in the individual's address book. This problem is not unique to the iPhone as both Android-based phones and Window Mobile devices have been found to be similarly susceptible to an SMS attack. For Android-based phones, an attacker could temporarily knock the phone off the cell network whereas Windows Mobile devices could also be exploited via the SMS messages to create a situation where there are no buttons to push, so the phone cannot be used. However, in both of these types of phones, the attacker cannot take complete control over the phone itself. Google has since patched the hole, but Apple, though notified of the problem several weeks ago, has yet to fix the problem. An interview with the researchers who discovered the flaw may be found at [http://www.forbes.com/2007/08/04/iphone-apple-mac-tech-cx\\_ag\\_0804miller.html](http://www.forbes.com/2007/08/04/iphone-apple-mac-tech-cx_ag_0804miller.html)

---

## **APPLE: IPHONE JAILBREAKING COULD KNOCK OUT TRANSMISSION TOWERS**

On July 29th, a macworld.com blog post reported that Apple has told the U.S. Copyright office that any modification of the iPhone's software, a popular process known as jailbreaking, could crash a mobile phone network's transmission tower or allow people to avoid paying for phone calls. These remarks come in light of arguments made by the Electronic Frontier Foundation (EFF) that Apple's lock on the iPhone is unmerited from a copyright protection perspective and aims to "suppress competition from independent iPhone application vendors." Each party has been providing their own comments to the Copyright Office's regular review of the U.S. Digital Millennium Copyright Act (DMCA), a law that forbids the circumvention of copy control mechanisms. Rebutting EFF's claims, Apple has argued that jailbreaking violates the DMCA because it is, basically, copyright infringement. To support its position, Apple has put forth all of the potentially severe technical problems operators could face with jailbroken phones. Apple explained that jailbreaking affords an avenue for hackers to do a number of undesirable things on the networks. For starters, hackers could change the phone's exclusive chip identification (ECID), which in turn can allow them to make anonymous phone calls. Further, a hacker could manipulate a jailbroken phone to conduct a denial-of-service attack and crash the tower. The U.S. Copyright Office holds hearings every three years to consider requests to make exceptions to the nation's copyright law and is expected to make a decision in this case later this year. EFF's comments may be found at [http://www.eff.org/files/filenode/dmca\\_2009/EFF2009replycomment\\_0.pdf](http://www.eff.org/files/filenode/dmca_2009/EFF2009replycomment_0.pdf)

Apple's arguments may be found at [http://www.copyright.gov/1201/2008/answers/7\\_13\\_responses/apple%27s-response-to-copyright-office-questions-of-6-23-09.pdf](http://www.copyright.gov/1201/2008/answers/7_13_responses/apple%27s-response-to-copyright-office-questions-of-6-23-09.pdf)

---

## **SOLDIERS WARNED ABOUT ID THEFT AFTER LAPTOP STOLEN**

On August 4th, The Army National Guard reported that an unsecured personal laptop was stolen from a federal contractor. What makes this occurrence noteworthy is that the laptop contained the names, addresses, Social Security numbers, and payment data of 131,000 current and former soldiers. The Army National Guard has been

investigating the theft and is in the process of sending letters to those affected, warning them to protect themselves from identity theft. The Guard has also been in contact with its state affiliates to assist in the notification of the affected soldiers. As to the Guard's internal investigation, a spokesman for the organization stated that the organization has been looking into what security policies were breached in the contractor's handling of the data. The spokesman went on to say that while the contractor was simply trying to do his job, the fact that the data was on a personal laptop means that some security protocols were, in fact, violated. Computer security experts have agreed that employees should never have that much data on their personal laptops, noting that up to 600,000 laptops are lost annually at airports alone. Information on what to do if identity theft happens to you may be found at <http://www.privacyrights.org/fs/fs17a.htm>

---

### **MARINES, NFL IN ASSAULT ON TWITTER, FACEBOOK?**

On August 4th, CNET News reported that both the Marines and the NFL have begun to ban the use of Twitter and Facebook. The Marines have explained that its ban, which will supposedly last one year, was designed to prevent worms, Trojans and other malware from infecting its space. However, some have wondered whether the ban has actually been enacted yet and whether high ranking officials will fall under the Marine's ban if it becomes military-wide. On the other side of the coin, the NFL has taken a unique approach to its social networking ban. The Green Bay Packers have told its players that they would be fined \$1,701 for texting or tweeting during any team function. While the Miami Dolphins have their own Twitter page, coach Tony Sparano has told players to lay off the tweets so as not to create any additional distractions. To some, these bans have highlighted the fact that organizations based on values such as discipline and secrecy, like the NFL and the Marines, are not exactly well-suited to social networking. Further information may be found at [http://news.cnet.com/8301-17852\\_3-10302980-71.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-17852_3-10302980-71.html?part=rss&subj=news&tag=2547-1_3-0-20)

---

### **PUBLIC SPIED ON 1,500 TIMES A DAY IN UK, STUDY FINDS**

On August 10th, Reuters reported on the alarming number of surveillance requests, 1500 in fact, which were made every day in Britain last year. Each one of these requests allowed public bodies to access data — telephone records, e-mail and text message traffic — but not the actual content of the conversations or messages. As a Home Office spokesman explained, the requests were being used to substantiate the who, where, and when elements in directed surveillance. The Liberal Democrats have seized on the figures, complaining that the government has forgotten that George Orwell's 1984 was a warning and not a blueprint. While the Liberal Democrats agree that a majority of the requests were necessary, they believe that only a magistrate should be able to approve a request for surveillance, under the Regulation of Investigatory Powers Act (RIPA). To substantiate their claims that the act is being misused, they have pointed to some requests, which were granted to investigate trivial offenses like dog fouling. A copy of the story may be found at <http://uk.reuters.com/article/idUKTRE5791OD20090810>

---

### **HOW NOT TO DO E-DISCOVERY - ESPECIALLY IF IT'S ON PURPOSE**

On August 5th, a Byte and Switch blog post provided insight into the eDiscovery debacle in the 2002 Pershing Park case in Washington DC. As background, Plaintiffs brought suit after riot police rounded up and arrested hundreds of individuals, including non-violent protesters and simple passer-bys, in Pershing Park. These individuals were handcuffed, bussed to a processing unit, and left tied wrist-to-ankle on a gym floor for the next 12 hours. Not happy, they sued. During discovery, the city of Washington D.C. fouled up the process in epic fashion. The city managed to lose the records of everything that transpired before, during and after that police action and the 400 or so field arrest forms. Even more shocking, the tapes of the radio runs were edited down from two hours to one and e-mails requested 6 years ago are just now being turned over sans their attachments. After severely scolding the district attorney, Judge Emmet G. Sullivan made sure he was aware that some hefty sanctions were on the way. In fact, Judge Sullivan went so far as to say, "You know what, look, there are going to be sanctions in this case and there's going to be an award of attorney fees, and you know, those sanctions -- and there'll be additional sanctions, and I'll tell you right now those sanctions are going to be painful." Further information be found at <http://www.byteandswitch.com/storage/e-discovery/how-not-to-do-ediscovery---especially-if-its-on-purpose.php>

---

## **RESEARCHERS: XML SECURITY FLAWS ARE PERVASIVE**

On August 5th, security researchers unveiled details about a little-known but prevalent class of vulnerabilities that may reside in a multitude of Internet components, from Web applications to mobile and cloud computing platforms to documents, images and instant messaging products. The problem stems from the way hardware and software makers handle data from an open standard called eXtensible Markup Language (XML). XML has been used as a fast and efficient way to transport, store and structure information across a wide range of applications and has been used in a variety of document formats (docx, openoffice, playlists, configuration files and RSS feeds, to name a few). With so many different uses, XML can be attacked in a variety of ways. The critical flaw may allow successful attackers to remotely install malicious software or send the application into an infinite loop, thereby rendering it temporarily inaccessible. So far there have yet to be any public exploits for these vulnerabilities, but some software manufacturers aren't taking any chances. Several have stated that they will be releasing updates to address the vulnerabilities, but due to the widespread use of XML, it is likely that similar problems may emerge in the future. CERT-FI's advisory report may be found at <https://www.cert.fi/en/reports/2009/vulnerability2009085.html>

---

## **GETTING ELECTRONICS INTO THE COURTROOM**

On August 11th, The National Law Journal reported on the impact that the Web 2.0 craze has on courts and some of the possible solutions to combat this growing problem. More and more frequently, stories have surfaced about a juror tweeting in court or a witness texting on the stand. In one particularly egregious situation, a witness was found text-messaging a company executive at the counsel table while the judge and the attorneys were engaged in a sidebar conference. Calling the incident a fraud on the justice system, the Florida judge declared a mistrial. With situations like these an almost every-day occurrence, it begs the question "what is the legal system to do?" Some have argued that solutions such as simply ignoring the problem altogether, issuing special jury instructions, or barring communication devices don't manage the problem effectively. Instead, one solution they believe that courts should adopt is to allow preauthorized counsel to bring electronic devices into the courtroom and make all others check their devices in the lobby. Advocates for this type of restriction have argued that it would solve the constitutional defense question, many of the jurors-gone-wild scenarios and the witness going rogue on the stand situation. It is also believed that enforcement of such a rule would reduce courtroom disturbances and address security concerns that the press or public could be recording court proceeding or photographing jurors or witnesses. A sample of this rule may be found at <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202432737644>

---

## **FTC DELAYS ENFORCEMENT OF IDENTITY THEFT RULES THAT WOULD AFFECT LAWYERS**

On July 29th, the Federal Trade Commission stated that it would be delaying enforcement of new rules designed to prevent identity theft, called the Red Flag Rules, until November 1st. The new identity-theft rules would require businesses that act as "creditors" to set up programs to minimize the risk of identity theft. Even though the FTC emphasized that it is unlikely to bring actions against entities that know their clients individually, perform services in or around their clients' homes, or operate in sections rarely hit by identity theft. Lawyers, doctors and other professionals have protested the FTC's broad interpretation of "creditors" to include businesses that bill clients some time after providing services. The American Bar Association has explained that the FTC's assertions that lawyers can be regulated under this law are not only troubling but completely unacceptable. To the ABA, the rule has also been viewed as undercutting a long history of regulation of state bars and supreme courts and threatening the independence of the profession from federal controls. The organization has said that it will continue to lobby Congress to exempt lawyers from the rule permanently and has recently filed suit against the FTC. A statement issued by the outgoing ABA President H. Thomas Wells Jr. may be found at <http://www.abanet.org/abanet/media/statement/statement.cfm?releaseid=731>

Additionally, the FTC statement may be found at <http://www.ftc.gov/opa/2009/07/redflag.shtm>

---

## **MICROSOFT WORD SALES BANNED IN 60 DAYS**

On August 11th, a judge ordered Microsoft to stop selling its popular Word document creation application in the United States in 60 days, after finding that certain portions of the software contain technology that violates a patent

held by i4i, Inc. Specifically, Judge Davis said that Microsoft was enjoined from selling any versions of Word that can open documents saved in the .XML, .DOCX, or .DOCM formats that contain custom XML - typically used by businesses to link their corporate data to Word documents. Adding salt to the wound, the court also said the software maker must pay \$240 million in patent-violation damages. Beyond the \$240 million dollars, the potential losses from the decision could be even more devastating. In the most recent fiscal year alone, Microsoft Office, which includes Word, accounted for more than \$3 billion in worldwide sales. Investors have yet to flinch however, as Microsoft shares actually posted gains in early trading after the decision. The judge went on to say that the injunction does not apply to versions of Word that open an XML file as plain text or which apply a transformer that removes all custom XML elementsâ€”possibly paving the way for Microsoft to issue a patch that rectifies the problem. Microsoft has stated that it plans to appeal the decision. A copy of the decision may be found at <http://blog.seattlepi.com/microsoft/library/20090811i4ijudgment.pdf>

A copy of i4i's complaint can be found at <http://blog.seattlepi.com/microsoft/library/20090811i4icomplaint.pdf>

---

## **CAN MICROSOFT, YAHOO AND AMAZON HELP SCUTTLE GOOGLE'S BOOK SETTLEMENT?**

On August 21st, ZDNet.com reported that Microsoft, Yahoo, and Amazon are reportedly joining forces with the Internet Archive and other non-profit groups to dismantle Google's book settlement with publishers and authors. As for the deal itself, Google and The Authors Guild, as well as the Association of American Publishers reached a settlement under which Google gets to scan books as long as it offers the ability to purchase them, provides institutional subscriptions and gives authors and publishers control over access to their works. Google has asserted it is simply trying to make print books available to the masses, but its rivals have argued that the company is getting too much power over copyrighted works in the \$125 million dollar deal. Additionally, the Department of Justice has an inquiry into the settlement, which still needs court approval. Some have reasoned that this situation seems eerily similar to the Microsoft fiasco of the 1990's. The settlement agreement between Google and The Authors Guild may be found at [http://www.googlebooksettlement.com/r/view\\_settlement\\_agreement](http://www.googlebooksettlement.com/r/view_settlement_agreement)

---

## **HACKER MITNICK MAY SUE AT&T OVER DATA BREACH**

On August 20th, CNET News reported on an ironic series of events - the AT&T wireless account of famed hacker Kevin Mitnick was breached and his personal information was leaked to the Web. Whoever was responsible for the attack likely used social engineering to do so — a technique Mitnick himself was known to frequently employ in his hacking days. Apparently not seeing the humor in the irony, Mitnick called the company and requested that AT&T compensate him for damages to his reputation and property rights; however, AT&T denied his requests after determining that they were without foundation and even threatened to cancel his service. Following a conversation with an attorney, Mitnick hinted at possibly filing a lawsuit for invasion of privacy for the failure to adequately protect his information. Due to his rock-star status in many hackers' mind, Mitnick has been a popular target for individuals out to make a name for themselves. Not only has his website been attacked numerous times through the years, but this isn't the first time Mitnick's AT&T account information has been breached. About a year ago he suffered a similar attack while on a trip to Bogota, Columbia. When asked about the most recent break-in, Mitnick explained that the bigger issue is that this ineffective security affects all AT&T customers and that the company needs to start shoring up its defenses. The story may be found at [http://news.cnet.com/8301-27080\\_3-10314576-245.html](http://news.cnet.com/8301-27080_3-10314576-245.html)

---

## **FACEBOOK DISABLES 6 ROGUE PHISHING APPS, BUT 5 MORE APPEAR**

On August 20th, Facebook said it had disabled six rogue apps that were stealing Facebook users' login credentials and spamming people, but within hours five more appeared. The five new apps were called "Friends," "Friends Gifts," "Matching," "Poki," and "Your Photos." By the end of the night however, these new rogue apps were disabled as well. The apps would send their victims a notification that someone had just commented on a post of theirs. The notification contained a link to a phishing site where users were then prompted to provide their Facebook login credential and asked to install one of the rogue apps. If the victim fell for the trap, his or her friends were then spammed. Facebook faced the same problem earlier in the week and removed those apps as well. A spokeswoman for the company has assured Facebook users that the company will continue to ensure that all

applications on Facebook Platform comply with Facebook policies. A blog post discussing this latest cyber scam may be found at <http://countermeasures.trendmicro.eu/two-more-rogue-facebook-apps-linked-to-fucabook-scam/>

---

## **SYMANTEC IDENTIFIES 'DIRTIEST WEB SITES OF SUMMER'**

On August 19th, Symantec released its Dirtiest Web Sites of Summer 2009 list, which documents the worst of the worst when it comes to websites that host malware threats. Number one on the list with a whopping 48 percent of the total number of sites were those that featured adult content. The other 50 percent covered a wide range of categories including legal services, catering, figure skating, and electronic shopping. On average, sites on the list have 18,000 threats per site, but 40 of the sites have in excess of 20,000 threats. With so many threats, the number of web attacks that can occur is off the charts. One method used to infect a computer with malware is "drive by downloads," which can exploit a vulnerability in your browser or operating system by "leveraging little security holes" and injecting code into your machine simply by virtue of your visiting the site. Another technique employed is social engineering where someone tricks a user into installing malware that is masquerading as a safe program. If a victim falls for any of these ploys, the malware can turn your machine into a "spambot" or use your computer to carry out attacks on other systems. Several programs are now available to let users know if a site is known to have malware. The list of dirtiest Web sites may be found at <http://safeweb.norton.com/dirtysites>

---

## **A LAWSUIT TRIES TO GET HACKERS THROUGH THE BANKS THEY ATTACK**

On August 19th, Unspam Technologies filed a lawsuit against gangs of Internet criminals known to break into business computers, steal banking passwords and transfer themselves money. While the lawyer for the company has conceded that the lawsuit will not likely produce the names of the hackers, he hopes that it will provide details of the thefts, the names of the victims and other information from the compromised banks that can be used to improve security and maybe identify the hackers. The technique employed by Unspam's attorney has been used successfully in the past — he used it previously on behalf of AOL and Verizon to identify people sending spam to their customers. However, banks might prove to be a harder nut to crack for information purposes. Not only do a number of laws protect the confidentiality of bank customers, but the banking industry has historically avoided much discussion about fraud cases. Banks have argued against disclosure because they believe it could give away the techniques used to break in and may potentially cause customers to lose confidence in the banking system. Additionally, banks may fight the subpoenas to protect themselves from liability for losses by their corporate customers. While everyday customers are generally reimbursed when money is lost to hackers, business accounts are not afforded the same protection. No matter what the outcome, Unspam's lawyer has said that he hoped his lawsuit would encourage banks to improve their electronic defenses. In his opinion, unless people want to go back to using their mattress as a bank, more needs to be done. A copy of the complaint filed by Unspam Technologies may be found at <http://graphics8.nytimes.com/packages/pdf/technology/onlinebanking.pdf>

---

## **D.C. APPEALS COURT ADOPTS FIVE-STEP INQUIRY FOR UNMASKING ANONYMOUS INTERNET SPEAKERS**

On August 13th, the District of Columbia Court of Appeals held that a defamation plaintiff seeking to identify an anonymous defendant must first submit sufficient evidence to establish a genuine issue of material fact for all claim elements within its control. Given the novelty of the issue, the court surveyed case law from other jurisdictions and ultimately adopted a five-part test similar to the summary judgment standard set forth in *Doe v. Cahill*. In *Cahill*, the court explained that a defamation plaintiff should be required to present evidence sufficient to survive a motion for summary judgment before he can obtain the identity of an anonymous defendant. Looking toward this reasoning, the D.C. court adopted the following five-part test. First, a defamation plaintiff must plead all elements of his or her claim. Failure to do so will likely result in a dismissal and no additional inquiry into the matter. Second, the party must make a reasonable attempt to notify the defendant. The court said courts should determine whether reasonable efforts have been made on a case-by-case basis. Third, the defendant should be given a reasonable amount of time to respond to the request being unmasked. Fourth, the plaintiff must provide evidence to show that he or she has a viable claim of defamation. And finally, the plaintiff must show that the information sought is important. Applying that test, the court vacated a district court order quashing a subpoena that sought the identity of an individual who sent an e-mail to a software piracy watchdog group reporting that the plaintiff engaged in

software piracy. Even though the plaintiff had failed to satisfy the test in its complaint, the court gave the company the opportunity to do so because the standard was not then clear. A copy of the decision may be found at [http://pub.bna.com/eclr/07cv159\\_081309.pdf](http://pub.bna.com/eclr/07cv159_081309.pdf)

---

### THREE MEN INDICTED IN LARGEST U.S. DATA BREACH

On August 17th, two Russians and a Florida man, Albert Gonzalez, were charged with the largest data breach in U.S. history. All are charged with conspiracy to gain unauthorized access to computers, commit fraud in connection with computers and damage computers, as well as conspiracy to commit wire fraud. The three men have been accused of hacking into Heartland Payment Systems, 7-Eleven, and the Hannaford Brothers supermarket chain, and stealing data related to more than 130 million credit and debit cards. Specifically, the trio allegedly found their victims on a list of Fortune 500 companies and, after determining what type of checkout systems they used, used a SQL injection attack to steal the data, utilizing computers from multiple states and foreign countries to launch the attacks, store malware and the stolen data obtained. A SQL injection inserts a small malicious script, which in turn exploits vulnerabilities in the database layer of an application that feeds information to the website. The three also allegedly installed backdoors and sniffers to intercept data in real time as it was processed by the victims and tried to hide their actions by accessing the victim networks through proxy computers, modifying their software to evade detection and programming it to delete all traces of their activities. After obtaining the purloined information, the men then tried to sell the data to others. Gonzalez has been in the legal spotlight quite a bit lately. He was charged in May 2008 in New York with hacking the computer network of the Dave & Buster's restaurant chain. Moreover, Gonzalez has already been charged with stealing data related to 40 million credit cards from eight major retailers. If convicted for their most recent criminal exploits, each man faces up to 35 years in prison as well as a fine of up to \$1.25 million. A blog post on the issue may be found at <http://bits.blogs.nytimes.com/2009/08/19/accused-hackers-lawyer-criticizes-federal-prosecutors/?partner=MOREOVERNEWS&ei=5040>

---

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

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

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

Subscribe to *Bytes in Brief*

Email:

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

---

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