



## Issue 136 September 2008

The URLs referenced in Bytes frequently link to newspapers and other current news sources. Be aware that these links may fail over time.

---

### **ABA RECOMMENDS STATES NOT REQUIRE COMPUTER FORENSICS TECHNOLOGISTS TO HAVE PRIVATE INVESTIGATOR LICENSES**

In late August, the American Bar Association approved a resolution by the Section for Science and Technology law recommending that states should not require those performing computer forensics services to procure a private investigator license. The recommendation includes computer forensics services involving the review of computer information, whether it is for court purposes or providing expert testimony, and the testing and securing of computer networks. The recommendation also supports establishing a separate set of professional standards for the computer forensics industry. The report lays out reasons for the recommendations, most notably that computer forensics is distinctly different than what most private investigators do, and that most private investigators do not possess the science and technology background that is necessary to conduct computer forensic examinations. Further, many computer forensic experts would be excluded from the trial process because they are not licensed as private investigators, though the computer forensic experts have many other professional certifications that make them qualified to testify in court. The report also notes that licensing requirements are not one of the factors laid out by the Supreme Court in determining the reliability of evidence. The recommendation and report may be found at <http://www.abanet.org/leadership/2008/annual/recommendations/ThreeHundredOne.doc>

### **SENATE PASSES LEAHY CYBER CRIME MEASURE**

On July 31st, the Senate unanimously passed legislation to fight identity theft and cyber crime. Vermont Senator Patrick Leahy introduced the bill, entitled the Identity Theft Enforcement and Restitution Act, to protect the privacy of American citizens. Key provisions of the bill expand the law to allow prosecution of identity thieves when the identity thief is impersonating a business, and when the thief is stealing data from a computer in the same state. Prior law allowed prosecution only if the identity thief targeted an individual or committed identity theft through an interstate communication. The law also makes it a felony to employ spyware to damage more than ten computers. Threatening to steal or release information from a computer is also a felony under the new law. Leahy said that the bill is intended to decrease identity theft by strengthening the cyber crime laws and enacting harsher penalties. Senator Leahy's press release may be found at <http://leahy.senate.gov/press/200807/073108a.html>

### **RSA CONFERENCE SURVEY FINDS THAT SECURITY BREACHES GO UNREPORTED**

On July 28th, the RSA Conference announced the results of its survey of about 300 attendees that found more than 89% of security incidents went unreported in 2007. The survey defined a security incident as "an unexpected activity that brought sudden risk to the organization and took one or more security personnel to address." The survey went further and asked for specific types of security incidents, and found that 69% of firms experienced e-mail borne malware and phishing, 44% experienced web-borne malware, 29% experienced data leakage, 28% experienced insider threats/theft, and 16% experienced intellectual property theft. Tim Mather, a security strategist for the RSA Conference, found the results disturbing because only 11% of breaches were reported, and 29% of firms experienced data leakage that included employee or consumer data. Mather pointed out that failure to report these problems could violate federal or state law. The RSA Conference press release on the survey may be found at [http://www.rsaconference.com/security\\_topics/business\\_trends\\_and\\_impact/blog.asp?x?blogId=17053](http://www.rsaconference.com/security_topics/business_trends_and_impact/blog.asp?x?blogId=17053)

## **RESEARCHERS REPORT PHOTO COULD STEAL ONLINE CREDENTIALS**

On August 1st, presenters at the Black Hat computer security conference announced that they would explain a new type of hybrid photo file that could steal credentials from users of popular websites like Google and Facebook. The hybrid file is called GIFAR, for the two types of files it combines: GIF and JAR. The hybrid file works because to the web server it looks like a GIF photo file, but it is also a Java applet. The web browser recognizes the malicious applet as if it were written by the website developer, when it really allows the bad guys to access users' Facebook or other accounts where users may upload images. The researchers also indicated ways to prevent such an attack, including through better filtering tools that would allow a website to spot the hybrid file or through a fix developed by Sun, owner of the Java programming language. Presenter John Heasman's blog post on the topic may be found at <http://heasman.blogspot.com/2008/08/on-gifars.html>

## **JUDGE FINDS SPRINT EARLY TERMINATION FEES ILLEGAL**

On July 28th, California Judge Bonnie Sabraw, of the Alameda County Superior Court, issued a tentative ruling against Sprint Nextel in its early termination fee lawsuit. Judge Sabraw ruled that the early termination fees are illegal and that Sprint Nextel should pay back \$18.2 million in collected fees from customers. In addition, Sprint Nextel also was ordered to stop trying to collect \$54.7 million from customers who did not pay the early termination fee. Initially, a jury found that customers had broken their contracts with Sprint Nextel, but the judge held that the contracts were illegal from the start. A news article on the decision may be found at [http://news.cnet.com/8301-1035\\_3-10004049-94.html](http://news.cnet.com/8301-1035_3-10004049-94.html)

## **LAPTOPS MAY BE DETAINED AT BORDER WITHOUT REASONABLE SUSPICION**

On July 16th, two Department of Homeland Security Agencies, U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement, posted policies on their websites stating that federal officers may examine documents, including laptops and other electronic devices, and detain the devices to do a complete search. While the devices may initially be detained without cause, in order to detain the devices indefinitely there must be probable cause. The policies apply to anyone entering the country, including U.S. citizens, and have been in effect for some time. The policies state that it is necessary to combat terrorism, child pornography, and to prevent other contraband from getting into the country. Senator Russ Feingold expressed concerns about the privacy implications of the practice, and stated that he intends to introduce legislation that would require reasonable suspicion to conduct border searches. The *Washington Post* article that broke the story may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2008/08/01/AR2008080103030.html>

The Customs policy may be found at [http://www.cbp.gov/linkhandler/cgov/travel/admissability/search\\_authority.ctt/se\\_arch\\_authority.pdf](http://www.cbp.gov/linkhandler/cgov/travel/admissability/search_authority.ctt/se_arch_authority.pdf)

## **FCC DECLARES COMCAST ILLEGALLY INTERFERED WITH FILE SHARING TRAFFIC, COMCAST STILL PLANS TO DELAY TRAFFIC FOR HEAVY USERS**

On August 1st, the Federal Communications Commission voted 3-2 that Comcast illegally interfered with Internet users' right to access the Internet. The Commission found that Comcast violated federal Open Internet Policy when it blocked peer-to-peer traffic for some subscribers. Chairman Kevin Martin was particularly critical of Comcast's actions, stating that Comcast "arbitrarily picked an application and blocked their subscribers' access to it." Martin also criticized Comcast for not notifying customers of the practice. Comcast was not fined, but instead must disclose the details of its discriminatory network management, submit a plan of how it will stop the practice, and disclose new network management plans to customers and the FCC. The decision indicates that other network operators could be subject to FCC scrutiny and that the FCC could issue fines for future violations. In response, Comcast revealed that it still plans to slow Internet service during periods of high congestion for heavy Internet users. Comcast's senior vice president, Mitch Bowling, laid out

the new plan in an interview with Bloomberg News and stated that Comcast would determine in real time when a user is causing congestion, and take action with respect to that user for the good of all users. The FCC press release may be found at

[http://hraunfoss.fcc.gov/edocs\\_public/attachmatch/DOC-284286A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-284286A1.pdf)

The *Bloomberg News* article may be found at <http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a7.3IMtqzEKc>

## **STUDY FINDS MALICIOUS CODE COMES FROM LEGITIMATE WEBSITES**

On July 29th, security vendor Websense announced the results of its research on Internet Security for the first and second quarters of 2008. The report found that 75% of websites with malicious code are legitimate websites that have been hacked, a 50% increase in a six-month period. Further, the legitimate websites are not small websites, as 60% of top 100 sites are either involved in or had malicious content in the first half of 2008. Most of the top 100 sites are either social networking sites or search engines. Websense manager Stephan Chenette stated that the problem with these sites is they let users upload content but do not filter it carefully, which results in the sites hosting a lot of malware. The report also notes the increase in web applications that contribute to malicious attacks and data loss because they allow hackers to target particular Internet users. Where e-mail communications are concerned, the report found that 87% of all e-mail messages sent are spam, holding steady from the end of 2007. But there was an increase of 47% in the amount of phishing attacks in spam, as 9% of all spam contains a phishing attack. The full report may be found at [http://www.websense.com/securitylabs/docs/WSL\\_Report\\_1H08\\_FINAL.pdf](http://www.websense.com/securitylabs/docs/WSL_Report_1H08_FINAL.pdf)

## **DOJ CHARGES ELEVEN IN THEFT OF OVER 40 MILLION CREDIT CARD NUMBERS**

On August 5th, the U.S. Department of Justice charged eleven perpetrators in the theft and sale of over 40 million credit and debit card numbers. The ring allegedly hacked nine different U.S. retailers – including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 and DSW - in what may be the largest identity theft and hacking scheme the DOJ has prosecuted to date. The perpetrators executed the scheme by installing "sniffer" programs to capture credit and debit card numbers after hacking into the various companies' networks. The perpetrators then sold the information to other criminals and used debit cards to withdraw large amounts of cash. Payments received from selling the stolen information were deposited in Eastern European bank accounts. The eleven face various charges including conspiracy, computer intrusion, fraud and identity theft. The defendants are from all over the world, with three from the U.S., one from Estonia, three from Ukraine, two from China, one from Belarus, and one who is identified only by an online alias. The perpetrators are being prosecuted in various U.S. District Courts. The DOJ press release may be found at <http://www.usdoj.gov/opa/pr/2008/August/08-ag-689.html>

## **COURT TO HEAR E-MAIL HACKING APPEAL**

On August 6th, the Washington Post reported that the U.S. Court of Appeals for the 9th Circuit plans to hear the appeal of *Bunnell v. Motion Picture Association of America*. The decision could transform online privacy law, as it deals with the question of what constitutes an "interception" online. The case stems from a 2005 incident in which a hacker broke into the server for a file sharing company and obtained copies of company e-mails as they were transmitted. The hacker then sent the e-mails to the MPAA, who paid the hacker for the e-mails, allegedly to be used in litigation against the file sharing company. The District Court found that the e-mails were not intercepted in violation of the 1968 Wiretap Act because they were not technically in transmission when the hacker intercepted them, because the interception did not stop transmission of the e-mail. The decision has huge implications, because it could mean that other entities, such as law enforcement, could hack into e-mails without compliance with the Wiretap Act. Privacy advocates, including the Electronic Frontier Foundation, filed amicus briefs against the District Court ruling. The story may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2008/08/05/AR2008080503421.html>

The EFF amicus filing may be found at  
[http://www.eff.org/files/filenode/Bunnell\\_v\\_MPAABunnellAmicus.pdf](http://www.eff.org/files/filenode/Bunnell_v_MPAABunnellAmicus.pdf)

## **COURT RULES DVR DOES NOT VIOLATE COPYRIGHT LAWS**

On August 4th, the U.S. Court of Appeals for the Second Circuit ruled that digital video recorders (DVR) do not violate copyright laws. In this case, media companies sued cable television provider Cablevision, claiming that Cablevision's DVR capabilities constituted copyright infringement. Cablevision's DVR is not yet in use, but it differs from other providers' DVR systems because the technology relies on a centralized server instead of an individual hard drive. The media companies sued after Cablevision announced its technology but before Cablevision could put the DVR system in place. The District Court ruled in favor of the media companies, and said that playback should be licensed. But the Second Circuit overturned the decision, stating that the DVR did not directly infringe copyrights, as it merely provided customers with a service. The decision explained that the people who record items on the DVR are responsible for the copy, and that the copies must be permanent to be considered copies under copyright law. The decision may be found at [http://www.ca2.uscourts.gov:8080/isysnative/RDpcT3BpbnNcT1BOXDA3LTE00DAtY3Zfb3BuLnBkZg==/07-1480cv\\_opn.pdf#xml=http://www.ca2.uscourts.gov:8080/isysquery/irlb26e/29/hilite](http://www.ca2.uscourts.gov:8080/isysnative/RDpcT3BpbnNcT1BOXDA3LTE00DAtY3Zfb3BuLnBkZg==/07-1480cv_opn.pdf#xml=http://www.ca2.uscourts.gov:8080/isysquery/irlb26e/29/hilite)

## **UK SURVEY REVEALS THAT COMPANIES CANNOT KEEP E-MAIL SAFE**

On July 29th, e-mail management company Mimecast announced the results of a survey that found 94% of companies admit they are powerless to prevent the leak of confidential information by e-mail. The survey was conducted of 125 IT managers in the United Kingdom. Only 6% of those IT managers were confident that anyone would be prevented from sending confidential e-mail. An alarming 32% of companies admitted they would not even be aware if confidential information had been leaked, leaving the companies helpless to remedy the situation. But 62% of firms said they would be able to do damage control after the e-mail had been sent, even though they could not prevent the disclosure. Bob Tarzey, security analyst at Quo Circa, attributes the disclosures not to maliciousness, but to employee carelessness. The Mimecast press release may be found at <http://www.mimecast.com/events-press/press-releases/article/view/new-survey-reveals-94-of-companies-are-powerless-to-prevent-confidential-data-from-leaving-the-ir-co/222/>

## **JUDGE SANCTIONS CLIENTS FOR HIDING SOURCE CODE DURING DISCOVERY**

On August 12th, in the U.S. District Court for the Northern District of California, Magistrate Judge Elizabeth LaPorte issued sanctions against Homestore, Inc., the National Association for Home Builders of the United States, and the National Association of Realtors for discovery abuses. Kevin Keithley sued the three companies for patent infringement on his software patent for displaying real estate information online. Judge LaPorte sanctioned the three defendants for destroying evidence, claiming they did not have documents essential to the case, and producing the documents only after sanctions were threatened. Homestore failed to preserve their source code on their websites, even after litigation had been threatened and Homestore should have been preserving documents. The chief IT officer at Homestore stated that an old database with the source code was replaced and a computer failure had also wiped out the code. Contrary to the testimony, Homestore later found backed up source code. The judge did not impose a default judgment because she stated that the destruction of evidence was not intentional, though Homestore recklessly disregarded its discovery obligation. The sanctions included an adverse inference instruction for not retaining the source code, and \$250,000 in monetary sanctions to Keithley's attorneys. The sanctions order may be found at <http://pdfserver.amlaw.com/ca/sanctions0815.pdf>

## **APPEALS COURT RULES THAT OPEN SOURCE COPYRIGHTS ARE ENFORCEABLE**

On August 14th, the U.S. Court of Appeals for the Federal Circuit ruled that open source users may be sued for copyright infringement if they do not comply with the licensing terms of the software, even if the software is free. The lawsuit was filed by Robert Jacobsen, copyright owner for computer programming code available under an open source license on his website. Jacobsen accused

Matthew Katzer of using the copyrighted code in his software package without giving credit to Jacobsen, in violation of the terms of the license. The District Court found that Jacobsen could not sue because the open source license was intentionally broad. The appellate court overturned this ruling, finding that open source copyright holders have the right to lay out the terms under which their product can be used. The court also found that Jacobsen may sue for monetary damages even though his product is free, because there is still an economic consideration. The decision may be found at <http://www.ca9.uscourts.gov/opinions/08-1001.pdf>

### **CYBERWARFARE: PART OF GEORGIA/RUSSIA CONFLICT OR EXCITED KIDS?**

On August 12th, various news sources indicated that Georgia government websites were attacked to coincide with Russia's attack of Georgia. Two Georgian websites were victimized, as were the president's website and a popular television station's website. Though the Russian government did not appear to be involved, many experts were skeptical. The *Wall Street Journal* claimed that the Russian Business Network (RBN) was behind the attacks, but stated that the RBN probably was acting for someone else, whose identity was hidden. Others claimed Russian criminals were performing the attacks as a tradeoff with the government for lighter sentences. One researcher reported that kids were behind the attacks on the Georgian websites. Since the attack consisted only of botnet attacks on websites, not an attack on the Internet infrastructure, the researcher said that the attacks were probably overexcited kids. The researcher blamed the Georgia government for being ill prepared to handle such an attack. Regardless of the source, the conflict brought to light the dangerous possibility of cyberwarfare in the future. An initial news story may be found at <http://government.zdnet.com/?p=3935>

The news story about the researcher crediting kids with the attack may be found at [http://news.cnet.com/8301-1009\\_3-10016152-83.html](http://news.cnet.com/8301-1009_3-10016152-83.html)

### **POLICE USE GPS DEVICE TO CAPTURE SUSPECTS**

On August 13th, the *Washington Post* reported that GPS tracking systems are becoming an invaluable tool to help police catch suspects. One example of GPS use was in Fairfax County, Virginia against David Lee Foltz, a suspect in a series of attacks on women in Fairfax and Alexandria. Foltz was arrested after dragging a female victim into a wooded area. The police had been tracking him with a GPS device placed on his van four days earlier. While police do not want to reveal how they catch criminals, tools such as the GPS come to light when challenged in court in cases like Foltz's. Privacy advocates are concerned that using the GPS violates the Fourth Amendment search and seizure provision when GPS is used without a search warrant. Advocates supporting use of GPS claim that police do not need a warrant for GPS since it gives the same information as physical tracking. Police did not seek a warrant in the Foltz case because Foltz's van was parked on a public street. Courts are split on the issue, with the Washington State Supreme Court holding a search warrant is necessary, and courts in New York, Maryland and Wisconsin holding a search warrant is not necessary. The article may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2008/08/12/AR2008081203275.html>

### **JUDGE PUTS GAG ORDER ON SUBWAY HACKING SPEECH**

On August 9th, Federal Judge Douglas Woodlock ordered a halt to a speech at the Defcon conference in Las Vegas to prevent three MIT students from giving a presentation on how to hack smartcards used for the Boston subway. The Massachusetts Bay Transportation Authority moved for an injunction to prevent the students from giving the speech, which Judge Woodlock granted after a short hearing. The Electronic Frontier Foundation represented the students and claimed the order violated the students' First Amendment Rights. Though the order was in effect, everyone who signed up for the Defcon conference received a copy of the students' presentation in advance. The presentations also were posted on various websites. The project revealed many flaws in the MBTA's transportation system, including flawed network security and social engineering weaknesses. Though the presentation contained much of this information, the students said they withheld information that would allow people to hack the MBTA's farecards. Ten days after the gag order was implemented, the judge lifted the temporary injunction, and rejected the MBTA's request

for a five-month injunction so the security flaws could be fixed. Though the injunction was lifted, the lawsuit against the students alleging violations of the Computer Fraud and Abuse Act remains. Information on the case, including links to the court orders, may be found at <http://www.eff.org/cases/mbta-v-anderson>

## **DHS TRACKS U.S. CITIZEN'S BORDER CROSSINGS**

On July 25th, the Department of Homeland Security announced in the Federal Register that the federal government has been collecting information on all U.S. citizens crossing borders by land. The government compiles the data in the Border Crossing Information database, and keeps the records for fifteen years in case it needs to be used in an investigation. According to the notice, the information that is collected includes some biographical information, a photograph, and any information about a person's trip that he or she decides to give up. The notice justifies the program by stating it will be used to fight terrorism. While information was always gathered on those traveling by air, collecting information on those traveling by land proved difficult until recently. New travel documents must have the capability to be scanned, which speeds up the information collection process. Critics are concerned about invasions of privacy and the amount of information the government is keeping in storage on U.S. citizens. The DHS notice may be found at <http://edocket.access.gpo.gov/2008/E8-17123.htm>

## **UCRIME ONLINE MAP LISTS CAMPUS CRIME INCIDENTS**

On August 4th, a new website launched that is trying to keep college campuses a little bit safer. UCrime provides maps and automated alerts in real time for crimes that occur on college campuses. The service is not only for students, as parents, prospective students, administrators, faculty, or those who live near a university may use it. Alerts are available through many means, including e-mail, cell phones and Facebook. In addition to alerts, the campus maps on the website give information on what type of crime occurred and when it happened. It also allows users to comment on crimes and share safety tips, all with the goal of making campus communities safer. The UCrime press release may be found at <http://ucrime.blogspot.com/2008/08/ucrime-press-release.html>

## **INDIAN FIRM MOVES TO DISMISS ANTI-OUTSOURCING LAWSUIT**

On August 14th, Indian company Acumen Legal Services filed a motion to dismiss in a case filed by a law firm concerned about the consequences of outsourcing legal services. The lawsuit seeks declaratory and injunctive relief concerning whether transmitting data to outsourcing companies waives Fourth Amendment protection for the transmitted data. The motion to dismiss claims that there is no personal jurisdiction in the case because there was no contact between Acumen and the forum jurisdiction. Also, Acumen claims there is no subject matter jurisdiction because the law firm made no monetary value claim, which does not satisfy the amount in controversy requirement. The motion further states that the costs of the decision would have far reaching effects beyond legal outsourcing. The Acumen press release may be found at [http://www.klgates.com/files/upload/eDAT\\_Acumen\\_Press\\_Release.doc](http://www.klgates.com/files/upload/eDAT_Acumen_Press_Release.doc)

The motion to dismiss may be found at [http://www.klgates.com/files/upload/eDAT\\_Acumen\\_Motion\\_Dismiss.pdf](http://www.klgates.com/files/upload/eDAT_Acumen_Motion_Dismiss.pdf)

## **COURT ORDERS RE-PRODUCTION OF ESI IN NATIVE FORMAT**

On August 7th, U.S. District Court for the District of Kansas decided that production of electronically stored information in paper format did not comply with Federal Rule of Civil Procedure 34, which requires a party to produce ESI in a reasonably useable format. In this employment discrimination case, defendant Graceland College Center produced the ESI by converting the relevant e-mails and documents to PDF format, printed the documents and turned them over to plaintiff Julie White. The court held that the conversion of documents violated Rule 34, and relied on the advisory committee notes to the Federal Rules. The committee notes explained, "the option to produce in a reasonably useable form does not mean a responding party is free to convert electronically stored information

from the form in which it is ordinarily maintained to a different form that makes it more difficult or burdensome for the requesting party to use the information effectively in the litigation." The committee notes also stated that if the ordinary form is searchable, it should not be modified so it is no longer searchable. The court found that conversion of the files from electronic form to paper form made the documents no longer searchable and cut out relevant metadata. For those reasons the court ordered re-production of the documents in native electronically stored format. The decision may be found at [http://www.klgates.com/files/upload/eDAT\\_Westlaw\\_Document\\_White.doc](http://www.klgates.com/files/upload/eDAT_Westlaw_Document_White.doc)

### **QUALCOMM ATTORNEYS' APPEAL DISMISSED BY FEDERAL CIRCUIT**

On August 18th, the Federal Circuit Court of Appeals dismissed the appeal of Qualcomm in its patent infringement dispute against Broadcom. In the case the Magistrate Judge issued sanctions against Qualcomm and its attorneys for discovery abuses, including failing to turn over hundreds of thousands of documents. The court declined to hear the appeal because of a lack of jurisdiction. The court explained that it could only hear an appeal of a final order, and that the order Qualcomm was appealing was not a final order, as it was an order implementing sanctions and remanding the case to the District court. The court noted that both sides knew that proceedings regarding the sanctions were still ongoing, therefore the court could not review the case. The order may be found at [http://www.klgates.com/files/upload/eDAT\\_Qualcomm\\_August\\_18\\_Order.pdf](http://www.klgates.com/files/upload/eDAT_Qualcomm_August_18_Order.pdf)

### **GOVERNMENTS FILTER WHAT WE SEE ON THE INTERNET**

On August 21st, CNN reported that governments across the globe are filtering what users see on the Internet. Filtering, as defined by the article, is "restricting access, blocking, or taking down Web sites." Governments may use filtering in different ways, including censoring websites or filtering search results. The use of these tools is also more widespread than one may think. In 2007, a survey of 40 countries found that two-thirds had used Internet filtering technologies, though most democracies such as the U.S. and India had unrestricted Internet. Some countries used filtering tools for a specific purpose, such as blocking child pornography or access to sites about a rival country. Filtering also has been used as a form of cyberwarfare, as was seen recently in the conflict between Russia and Georgia. The full story may be found at <http://www.cnn.com/2008/TECH/08/21/internet.filtering/index.html>

### **CASE USES "HASH" TECHNOLOGY TO CATCH CHILD PORN PERP**

On July 24th, Magistrate Judge David D. Noce in the U.S. District Court for the Eastern District of Missouri issued an opinion upholding the use of evidence that was identified by police using hash algorithms. According to Ralph Losey's blog post on the topic, hash "reveals the unique mathematical fingerprint of every computer file that allows for perfect identification and authentication of electronic evidence." Hash values are assigned to every file on a computer, and the police can use these values to identify child pornography on a particular computer. An example of hashing is seen in *U.S. v. Warren*. The judge found probable cause for a search warrant for Warren's computer based on police reports of the hash values of Warren's computer that indicated there was child pornography on it. The judge upheld the use of the video computer file as evidence, and endorsed the use of a simpler way to identify hash values. The usual hash value system uses values between 32 and 40 places for identification, whereas the truncated value used by the court contains only six places as a labeling system. The decision may be found at [https://ecf.moed.uscourts.gov/documents/opinions/USA\\_v\\_Warren-RWS-34.pdf](https://ecf.moed.uscourts.gov/documents/opinions/USA_v_Warren-RWS-34.pdf)

Losey's blog post may be found at <http://ralphlosey.wordpress.com/2008/08/17/new-case-where-police-use-hash-to-catch-a-perp-and-my-favored-truncated-hash-labeling-system-to-identify-the-evidence/>

### **CASE SHOWS HOW ADVERSARIAL E-DISCOVERY MAY BE COSTLY**

On May 27th, in U.S. District Court for the Northern District of Indiana, *Perfect Barrier, LLC v. Woodsmart Solutions, Inc.*, was decided concerning overbroad search terms and the results one party did not anticipate. In this case, plaintiff Perfect Barrier requested defendant Woodsmart

search for e-mails by using seventy-seven search terms that Perfect Barrier's attorney came up with to try to bury Woodsmart with document review. Woodsmart responded by saying that the search terms were overly broad, and offered to compromise on the issue by coming up with a list of keywords together. Perfect Barrier rejected the compromise, and insisted that Woodsmart do the search. Woodsmart did the search, which pulled up over 75,000 pages of documents that Woodsmart produced in native format. Woodsmart did the search under a protective order that allowed it to designate all responsive documents as confidential, so only Perfect Barrier's attorneys could review them, thus shifting the burden of review from Woodsmart to Perfect Barrier. Perfect Barrier tried to object, but Magistrate Judge Christopher A. Nuechterlein concluded that Perfect Barrier had tried to bury Woodsmart with an overbroad discovery request. The judge denied the motion for sanctions against Woodsmart, and noted that Perfect Barrier could have used more limited search terms from the beginning. The judge also held that since Perfect Barrier failed to indicate a method of production, Woodsmart's production of the documents in native format was perfectly acceptable. The decision may be found at [http://www.klgates.com/files/upload/eDAT\\_Westlaw\\_Document\\_Perfect.doc](http://www.klgates.com/files/upload/eDAT_Westlaw_Document_Perfect.doc)

---

"*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, [click here](#) and enter your real name, company name, and e-mail address.

---

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