

# { 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



© 2010 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

## ISSUE 153 – FEBRUARY 2010

**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)

---

### SOCIAL NETWORKING AMONG JURORS IS TRYING JUDGES' PATIENCE

On January 9th, *The Washington Post* reported on how modern technology and an information-saturated culture are testing notions of how juries and judges mete out justice. One aspect particularly troubling to judges and legal experts is how easy it can be for technology and culture to affect jurors and a Defendant's right to a fair trial. While jurors of the past faced hurdles that restricted their ability to conduct their own investigations or discuss the case with others, technology has wiped out those barriers. The Internet has provided easy and instant access to a variety of information and social networks have provided users the ability to instantly post updates about the everyday aspects of their daily lives, or even the juicy tidbits of an intriguing trial. Making matters worse, legal scholars and lawyers can't seem to agree on how to handle the problem. Some argue that judges should warn jurors expressly about the Internet, while others advocate giving jurors more information during trials. And still others throw up their hands, many contending that no matter what is done, jurors will continue to "Google" and "tweet." One thing that may drive reform – or at least bring the issue to the forefront – is the recent outbreak of cases that have popped into public view because the jury misconduct was egregious enough that judges were forced to decide whether to grant new trials. Although courts have sometimes found that a new trial wasn't warranted because the juror's conduct didn't actually harm the Defendant's right to a fair trial, this isn't always the case. For example, in May, a Maryland appeals court ordered a new trial for a man accused of raping his teen daughter after it became apparent that a juror had researched "oppositional defiant disorder" on the Internet and communicated to other jurors. According to the court, this conduct improperly and irreparably influenced the jury's deliberative process. In July, a New Jersey appeals court granted three cousins convicted of aggravated manslaughter a new trial after a juror had done research about the victim, the defendants and the amount of prison time they faced and had told her colleagues about it. Finally, in one of the more high profile cases, defense attorneys for Baltimore Mayor Shelia Dixon accused five jurors of improperly becoming friends and chatting about the case on Facebook. The attorneys argued that the jurors, called the "Facebook Friends," could have bullied other jurors into finding Ms. Dixon guilty. Although Judge Sweeny wasn't forced to consider the alleged misconduct because a surprise plea deal ended her appeals, it is certain that this issue isn't going to go away. More information may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/08/AR2010010803694.html>

---

### DDOS ATTACK ON DNS HITS AMAZON AND OTHERS

On December 24th, *Infoworld.com* reported that Internet users in Northern California were unable to reach Amazon.com and Amazon Web Services as their DNS provider was targeted by a DDOS (distributed denial of service attack). First to recognize the problem was Neustar, the owner of Amazon's DNS provider, UltraDNS. Allen Goldberg, Vice President of Corporate Communications at Neustar, said that his company was able to analyze the attack pattern and take steps to limit its effects within minutes of identifying the problem. Likewise, Amazon Web Services (AWS) was able to quickly detect that something was wrong. Its status page indicated that its staff was investigating reports from customers trying to reach its S3 cloud storage service. The outage affected the e-commerce servers of parent company Amazon.com too, and many others: "Tons of sites are offline," wrote Jeff Barr, Amazon Web Services strategist, in a Twitter message. A copy of the story may be found at <http://www.infoworld.com/d/security-central/ddos-attack-dns-hits-amazon-and-others-523>

---

## **AS ATTACKS INCREASE, U.S. STRUGGLES TO RECRUIT COMPUTER SECURITY EXPERTS**

On December 23rd, *The Washington Post* reported that the federal government is fighting and losing the battle to fill a growing demand for skilled computer-security workers, from technicians to policymakers, at a time when network attacks are rising in frequency and sophistication. In fact, demand is so intense that it has sparked a bidding war among agencies and contractors for the small pool of skilled technicians with security clearances, driving up salaries, depriving agencies of skills, and in some cases affecting project quality. According to several national security experts, the lack of trained defenders for the country's critical computer networks is leading – if it has not already – to serious gaps in protection and significant losses of intelligence. Further, as evidenced by the government's response to recent cyberattacks, most governmental agencies and private companies lack the skills and resources to muster a robust containment effort when cybercriminals strike. As adamantly stated by Alan Paller of the SANS Institute, skilled technicians are much more important than hardware. One of the primary problems facing the government is the fact that it is often outbid by the private sector in recruiting cyber-warriors. While the federal government has attempted to draw in talent by offering individuals the National Science Foundation's Scholarship for Service, which pays for up to two years of college in exchange for an equal number of years of federal service, this program has placed fewer than 1,000 students since its inception in 2001. Often, recipients of the scholarship will work for a governmental agency for the required two years, but will then be lured away to a private company by a lucrative pay raise. Philip Reiting, deputy undersecretary of Homeland Security's National Protection and Programs Directorate, conceded that the government generally cannot match industry pay scales. But he noted that, in the government, you can have a bigger ability to make a difference at an earlier place in your career than anywhere else – and your country needs you. Like computer security workers, cybersecurity lawyers, researchers and policymakers are also in short supply. For instance, the Pentagon lacks a career path to develop expert decision-making in the cyber field. Robert D. Gourley, a former Defense Intelligence Agency chief technology officer has explained that the great cyber-generals are few and far between. More information may be found at <http://www.washingtonpost.com/wp-dyn/content/article/2009/12/22/AR2009122203789.html>

---

## **OBAMA NAMES HOWARD SCHMIDT AS CYBERSECURITY COORDINATOR**

On December 29th, the White House named a former Bush administration official, Howard A. Schmidt, as the man to orchestrate the government's strategy for protecting the nation's computer systems. Schmidt carries a resume that reflects his experience in the private sector, law enforcement and government. He served as special adviser for cyberspace security from 2001 to 2003, worked as chief security officer at Microsoft and eBay, served in both the Air Force and FBI, and was president of the Information Security Forum, a nonprofit consortium of corporations and public-sector organizations working to resolve cybercrime and cybersecurity issues. The appointment comes after President Obama declared the nation's digital networks a strategic national asset and said protecting them would be a national security priority. In the President's opinion, creating a White House cybersecurity office with a senior White House officer running it was central to the effort, noting that he would depend on this official in all matters relating to cybersecurity, and that this official would have his full support and regular access to him as they work to combat all challenges. However, the President's remarks were undercut by internal tension over how much authority Schmidt would have and to whom he would report. According to White House economic adviser Lawrence H. Summers, Schmidt should be required to report to him as well because cybersecurity is also a matter of national economic security. Perhaps quelling the concern, an administration official has explained that Schmidt will be required to report to deputy national security adviser John O. Brennan, but he will work closely with and collaborate with the economic council on cyber-issues too. A White House blog post on the topic may be found at <http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator>

---

## **FBI PROBES CYBER ATTACK ON CITIGROUP: REPORT**

On December 22nd, *Reuters* reported that the FBI is investigating a computer attack targeting Citigroup, Inc. and resulting in the theft of tens of millions of dollars. The attack was aimed at Citigroup's Citibank subsidiary. Those responsible for the attack are thought to be linked to a Russian gang and may have been able to gain access to the bank's systems through third parties. This latest attack highlights the growing concern that surrounds the issue of computer hacking of financial institutions. Scott Vernick, a lawyer at Fox Rothschild LLP, whose practice includes electronic data security matters, has explained that while most financial institutions are working extremely hard to harden their defenses against such attacks, the problem is that the criminals are

working even harder. Citigroup stated that the attacks are directed against companies globally, and while there had been attempts to interfere with the bank's systems, none have been successful. Yet, Fred Cate, director of the Center for Applied Cybersecurity Research at Indiana University, paints a different picture. He believes that the evidence demonstrates that attacks such as the one against Citibank are successful in many instances, particularly socially engineered attacks. A copy of the story may be found at <http://www.reuters.com/article/idUSTRE5BL01320091222>

---

## **AS PHONES DO MORE, THEY BECOME TARGETS OF HACKING**

On December 21st, *The New York Times* reported that as mobile phones become ever more like personal computers, they are also becoming more vulnerable to traditional computer menaces like hackers and viruses. Earlier this year, Kaspersky Lab, an antivirus company, reported that a new malicious program could take over a Nokia phone and make small charges to the owners' wireless account. Just last month, an experimental worm was able to infiltrate jailbroken iPhones, which are phones altered to run software Apple has not authorized. While the worm did not cause any damage – it just installed a photo of the '80s pop star Rick Astley – it suggests that pernicious attacks on iPhones are possible. As the number of security threats grows, individuals have attempted to capitalize on this fledgling market and build profitable businesses. One of the new kids on the block is called Lookout, a mobile phone security vender that has recently begun testing security software for phones running the Windows Mobile and Android operating systems and will soon introduce security applications for the BlackBerry and iPhone. The company's software is designed to protect phones against rogue programs and gives phone owners the ability to remotely back up and erase the data on their phones. For instance, a small business could install the Lookout software on many different types of devices, back up all the data and remotely erase a phone if an employee leaves it in a cab. Further, Lookout had claimed that its software can address the unique challenges of protecting cellphones, like preserving battery life. While the company will not give details, it says it has figured out how to get its software to work on the iPhone, which does not allow non-Apple programs to operate in the background, as security software typically does. A basic version of the software is free, while the company plans to charge a monthly subscription for a version with more features. Other companies like Research In Motion, maker of the BlackBerry, and Good Technology, a Silicon Valley-based mobile messaging firm, already offer mobile security tools, but their systems are aimed at businesses. Other companies, like security firms Symantec and Trust Digital, have their sights set on this market too. Although for now snoops and bad guys pose much less of a threat to cellphones than to PCs, as people continue to do more and more with their phones, they become a valuable target for hackers. A copy of the story may be found at <http://www.nytimes.com/2009/12/21/technology/21cell.html>.

---

## **HACKERS CLAIM TO CRACK KINDLE COPYRIGHT ARMOR**

On December 23rd, *CNET News* reported that hackers have stated that they've successfully cracked the copyright protections on Amazon's Kindle e-reader, making it possible to export e-books to other devices. One hack was allegedly the result of a Kindle DRM (Digital Rights Management) challenge issued on an Israeli forum called Hacking.org. On the site, one hacker known as Labba boasted that he created a crack that allows e-books stored on the Kindle to be transferred to other devices as PDF files. Similarly, U.S. hackers have also jumped into the Kindle cracking foray. One U.S. hacker has written a program that is reportedly able to crack copyright protections on the Kindle for PC application while another hacker, who goes by the name "i♥cabbages," has created a program called Unswindle that promises to convert books stored in the Kindle for PC application into a different file format. The program's creator recently posted two updates on the program, one noting that Amazon has demonstrated that it takes its digital rights management, or DRM, seriously and has already pushed out a new version of K4PC, which breaks this particular script. In the second update, the hacker explained that while the K4PC update may not actually have been targeted at Unswindle, he had nonetheless updated his creation to handle the 20091222 version of the executable. Those using the program have given it mixed reviews; some have stated that it worked flawlessly while others have highlighted various bugs. A blog post on the topic by i♥cabbages may be found at <http://i-u2665-cabbages.blogspot.com/2009/12/circumventing-kindle-for-pc-drm.html>.

---

## **JUSTICES TO REVIEW PLAN FOR WEBCASTS OF A TRIAL**

On January 11th, the Supreme Court indicated that it might chime in regarding whether and when video

coverage of federal trials is appropriate. This comes after the trial judge presiding over the same-sex marriage trial in San Francisco announced the intent to allow streaming video to several federal courthouses around the nation and had planned to post it after the end of each day's proceedings on YouTube. The Supreme Court temporarily blocked the judge's plan to broadcast the trial on the Internet, saying they needed more time to consider the issues. The order did, however, permit the trial to be streamed to other rooms within the San Francisco courthouse. In dissent, Justice Stephen G. Breyer agreed that further consideration of the issues was warranted, but he would have considered the issues without a stay, in part because the Defendants had not shown they were likely to suffer irreparable harm without one. Generally speaking, the Supreme Court does not allow video coverage of arguments in its courtroom, and cameras are routinely banned from most federal courtrooms, but in an experiment begun last month, the United States Court of Appeals for the Ninth Circuit, which includes the Federal District Court in San Francisco, agreed to allow federal judges to permit cameras in civil cases. Attorneys representing those opposing same-sex marriages have argued that a stay was needed to prevent harassment, economic reprisal, threats and even physical violence against witnesses prepared to testify in favor of Proposition 8. In response, lawyers representing proponents of same-sex marriages have argued that the case warranted broadcast coverage given its ramifications on hundreds of thousands of gay men and lesbians in California. Not surprisingly, a coalition of news organizations also urged the Supreme Court not to grant a stay, noting that the case did not involve criminal fair-trial rights and would not be heard by a jury. A copy of the temporary injunction may be found at <http://www.supremecourtus.gov/orders/courtorders/011110zr.pdf>.

---

## **ADOBE TO SURPASS MICROSOFT AS HACKER TARGET**

On December 29th, McAfee reported that Adobe products, Adobe Reader and Flash, have supplanted Microsoft Office applications as the target of choice for cybercriminals; a result driven largely by the growing popularity of these products. For the most part, this surge in attractiveness should come as no surprise. Security experts have warned for quite some time of the potential risk posed by Flash and in November, another Internet security vendor identified a flaw in the way web browsers handle Flash files that could be used to compromise websites that have users submit content. Beyond Adobe, cybercriminals have also ramped up their attacks against social networking sites, as well as third-party applications in general. In fact, according to senior VP of McAfee labs Jeff Green, society is now facing emerging threats from the explosive growth of social networking sites, the exploitation of popular applications, and more advanced techniques used by cybercriminals. More specifically, Facebook, Twitter, and the third-party applications that incorporate the social networks have given criminals new technologies to target and exploit, including "rogue apps" distributed by criminals and abbreviated URLs on sites like Twitter that make it easier for cybercriminals to mask and direct users to malicious websites. Along these same lines, more sophisticated Trojans have made it possible to make unauthorized withdrawals from online banking accounts that stay below transaction limits, thereby making those withdrawals more difficult for banks to spot. McAfee pointed out that e-mail attachments are expected to remain the most widely used Trojan distribution method, so users can avoid infection by checking on the safety of an attachment before clicking it. Finally, McAfee reported that it expects attacks incorporating botnets to incorporate peer-to-peer control, a distributed and resilient botnet infrastructure, rather than the centralized hosting model seen today. As McAfee's report demonstrates, hackers are adapting to the changing Web culture and are incorporating new techniques to circumvent new security measures. McAfee's report may be found at [http://www.mcafee.com/us/local\\_content/white\\_papers/7985rpt\\_labs\\_threat\\_predict\\_1209\\_v2.pdf](http://www.mcafee.com/us/local_content/white_papers/7985rpt_labs_threat_predict_1209_v2.pdf).

---

## **INDIANAPOLIS MAN 1ST TO BE PROSECUTED UNDER COMPUTER-EXTORTION LAW**

On January 13th, Kevin M. Stewart, a resident of Indianapolis, was the first individual to be successfully prosecuted under a law that makes it a crime to commit extortion with material from a protected computer system. The two year prison sentence comes after Stewart stole a computer server from the Indianapolis office of AIG Medical Excess. The server contained the names of over 900,000 insured persons, their personal identification information, and confidential medical information and private e-mail communications. Stewart then delivered a package to the insurance company, which included a letter stating that he possessed the stolen materials and that he intended to disseminate the information unless he received \$1,000 a week for four years. Luckily, the FBI and others were able to locate him, resulting in his prosecution. A blog post on the topic may be found at [http://indianalawblog.com/archives/2010/01/courts\\_indianap.html](http://indianalawblog.com/archives/2010/01/courts_indianap.html).

---

## **FORRESTER SAYS TECH RECESSION IS OVER**

On January 12th, the research firm Forrester released a report documenting what it believes is the end of the tech recession. Forrester's principal analyst Andrew Bartels explained that this belief stems from the fact that all the pieces to the puzzle are in place for a 2010 tech spending rebound. Specifically, Bartels highlighted increased spending on hardware and software as factors that led to the firm's predictions. According to the firm, tech spending in the U.S. is expected to grow 6.6% this year, to \$568 billion, after being down 8.2% in 2009. Additionally, Forrester predicts worldwide spending to jump 8.1% to more than \$1.6 trillion, following a decline of 8.9% last year. Software will enjoy the greatest uptick in sales, according to Forrester, which sees worldwide spending on software growing by 9.7%. Some of that could be driven by key new products from Microsoft and other vendors. Microsoft launched Windows 7 in October of 2009, and is slated to ship Office 2010 in the middle of this year. Forrester also sees a strong rebound in the hardware sector in 2010, with spending on computer equipment expected to increase by 8.2%. The firm also predicted that communications equipment sales will grow 7.6%, sales of IT outsourcing services will climb 7.1%, and sales of consulting and integration services will increase 6.8%. Further, Forrester believes that the IT industry is on the verge of a six to seven year cycle of growth and innovation that will be driven by smart computing, which represents a marriage of advanced hardware and software technologies that can drive new levels of automation and efficiency. In Bartels' mind, 2010 marks the beginning of this next phase of technology advancement. Further information is available at <http://www.ebizq.net/news/12118.html?rss>

---

## **INTERNET USERS NOW SPENDING AN AVERAGE OF 13 HOURS A WEEK ONLINE**

On December 23rd, a new Harris Poll reported that adult Internet users are now spending an average of 13 hours per week online although usage varies greatly. In fact, one in five adult Internet users are online for only two hours or less a week while one in seven are spending 24 or more hours a week online. Over the years, this number has steadily increased from 7 hours (in 1999, 2000, 2001, and 2002) to between 8 and 9 hours (2003, 2004, 2005, and 2006) to 11 hours in 2007. While last year Internet users were online for 14 hours per week, the poll noted that this number could have been inflated due to the financial crisis and the presidential election. Additionally, the Poll highlighted that those aged 30-39 (18 hours) spend the most time online, with those aged 25-29 and 40-49 coming in a close second at 17 hours per week. Another interesting finding was that half of those surveyed reported that they had purchased something via Internet shopping within the last month. Interestingly, the number of adults online, now 184 million (80%), has not changed significantly since 2008 and 2007. This includes those online at work, at home, at school or any other locations. However, the Harris Poll pointed out that the number of adults who are online at home has increased to 76% this year, and 75% last year, compared to 70% in 2006, and 66% in 2005. Some have viewed the results of this poll as reflecting a growing ability to use the Internet, an increase in Web sites and applications, increased TV watching online, and increased purchasing online. Also, many believe that the number of hours spent online may have increased because of the recession. Going online is free; going out usually costs money. The poll may be found online at <http://news.harrisinteractive.com/profiles/investor/NewsPDF.asp?b=1963&ID=35164&m=r>

---

## **VERIZON ENDS SERVICE OF ALLEGED ILLEGAL DOWNLOADERS**

On January 20th, *ZDNet.com* reported that Verizon Communications acknowledged that multiple file sharing offenses could result in a service interruption. According to the company's spokeswoman, Bobbi Henson, Verizon has cut some people off, but it has refused to throttle bandwidth as Comcast has done in the past. This approach is viewed by many as very similar to the one promoted and pushed heavily by the music industry. The music industry's approach, which was put forward by the Recording Industry Association of America (RIAA) in December 2008, moved away from filing lawsuits against individuals accused of file sharing, utilizing instead a graduated response to copyright infringement. The approach calls for an initial warning which would inform a customer that he or she had been accused of illegal file sharing. If an individual chooses to continue, the approach calls for a more strongly worded warning. The final response for chronic offenders is suspending or terminating service. While Verizon has declined to comment as to whether it has adopted RIAA's plan to combat copyright infringement, one thing is for certain, issuing warning letters that threaten termination of service have proved to be quite effective. According to Henson, the company has found that often, after the first warning, most people stop, or at least tell whoever is doing it to stop. Additionally, Henson was quick to point out that Verizon isn't actually monitoring what its customers download on the Internet. Instead, copyright

owners are capturing IP addresses and then requesting that the company send out e-mail warnings. Further, Henson also explained that Verizon was not simply handing over information about its users to the copyright owners, requiring first that the copyright owners procure a court order. A copy of the e-mail an individual receives when suspected of downloading copyrighted material may be found at <http://www.zdnetasia.com/news/internet/0,39044908,62060699,00.htm>.

---

## **MICROSOFT URGES CLOUD-COMPUTING PRIVACY BILL**

On January 20th, Microsoft's general counsel, Brad Smith, urged Congress to introduce a bill that would address privacy and security issues associated with cloud computing. The bill, called the Cloud Computing Advancement Act, would, at least according to Smith, improve privacy protection, modernize the Computer Fraud and Abuse Act to allow law enforcement to go after hackers and deter online crime, contain truth in cloud-computing principles, and contain a new multilateral framework to address data access issues globally. Speaking at the Brookings Institute in Washington D.C., Smith explained that the PC revolution empowered individuals and democratized technology in new and profoundly important ways. As we move to embrace the cloud, we should build on that success and preserve the personalization of technology by making sure privacy rights are preserved, data security is strengthened and an international understanding is developed about the governance of data when it crosses national borders. To support the company's belief that a bill was desperately needed, Smith also unveiled a report that said an overwhelming majority of people are concerned about the security of their data in the cloud. More specifically, the study, which polled 700 members of the general population, 200 senior IT business makers, and 200 senior business decision makers during a five-day period in December, found that 58 percent of the general population and 86 percent of senior business leaders are excited about the potential of cloud computing, but 90 percent still have concerns. While it remains to be seen if Congress will actually introduce Smith's proposed legislation, it appears that other organizations support the bill and will likely back it. Randy Skoglund, executive director of Americans for Technology Leadership, applauded the proposal and stated that his organization supported Microsoft's efforts to modernize these important laws to make sure they reflect today's technologies. In Skoglund's mind, laws need to impose stiff penalties on the criminals who hack into financial and corporate networks putting our data, our finances and our identities at risk. A copy of the story may be found at [http://www.microsoft.com/presspass/press/2010/jan/10/1-20BrookingsPR.mspx?rss\\_fdn=Press%20Releases](http://www.microsoft.com/presspass/press/2010/jan/10/1-20BrookingsPR.mspx?rss_fdn=Press%20Releases)

---

## **ALLEGED CHINA ATTACKS COULD SHAPE U.S. CYBERSECURITY POLICY**

On January 14th, *Infoworld.com* reported that the recent attacks on Google and more than 30 other Silicon Valley companies by those allegedly working for China has focused attention on the issue of state-sponsored cyber attacks and the best way for the U.S. government to respond to them. To date, the U.S. has no formal policy for dealing with foreign government-led threats against U.S. interests in cyberspace, but the recent attack has fueled efforts to develop such a policy and to do so quickly. For the most part, the U.S. response to the attacks has been little more than expressions of outrage and protest by lawmakers. According to Ira Winkler, president of the Internet Security Advisors Group, there really is nothing the U.S. can do. As he puts it, the reality of the situation is that we are screwed. The political reality is that China, in large part, is funding the U.S. deficit and we can't just cut China off. Making matters worse is the fact that articulating a response to government-led cyber attacks is never easy. Not only is there often a lack of certainty as to the true culprit of the crime, but even if the evidence clearly pointed to a particular foreign country, it's futile to launch any kind of cyber-retaliation. However, that doesn't mean that nothing can be done. Amit Yoran, the former director of the U.S. Department of Homeland Security's National Cyber Security Division, said that the first thing to do is to bolster our defenses. Specifically, Yoran called for a security approach that focuses on continuous monitoring of networks and data, not one based solely on prevention. What else is needed, and needed badly, is manpower. According to Alan Paller, director of research for the SANS Institute, the federal government has less than 1,000 people with the advanced skills needed to fight in cyber space at world-class levels. What's needed, in his opinion, are between 20,000 and 30,000 cybersecurity warriors. Senator Joseph Lieberman's comments on the cyber attacks and his opinion on what must be done may be found at [http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord\\_id=28946e2c-5056-8059-76b5-32a0c5690735](http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=28946e2c-5056-8059-76b5-32a0c5690735)

---

## **U.S. V. WILLIAMS: SEARCH AND SEIZURE OF CHILD PORNOGRAPHY FALLS WITHIN THE SCOPE OF POLICE WARRANT**

On January 21st, the Fourth Circuit affirmed Curtis Williams' conviction for, inter alia, possession of child pornography after the police searched his home and found a DVD containing child pornography. In September 2007, the Fairfax Baptist Temple in Fairfax Station, Virginia, began receiving threatening e-mail messages from an individual identifying himself as "Franklin Pugh." These messages soon became sexually explicit, with the sender proclaiming that he was a pedophile. The messages stated that he previously had sexual encounters with several young boys in the congregation and that he wanted to continue these sexual encounters in the future. Upon investigation, the Fairfax County Police determined that at least one of the e-mail accounts used to transmit received e-mails had been accessed repeatedly by an Internet account registered to Karol Williams, in Clifton, Virginia, who is the wife of the defendant, Curtis Williams. The Fairfax County magistrate then issued a search warrant which commanded the officers to search for and seize from the home of Karol and Curtis Williams, among other things "any and all computer systems and digital storage media, videotapes, videotape recorders, documents, and photographs." In collecting these items, one officer opened a DVD that had been seized and observed over a thousand images in "thumbnail view" of minor boys, some of which were sexually suggestive and some of which were sexually explicit. Williams then filed a motion to suppress the evidence, including the child pornography; however, the district court denied the motion, explaining, with respect to the child pornography, "The fact that a person who's already under suspicion for threatening to do bodily harm to minors would have imagery within his computer or within his home showing significant mistreatment of minors in my view is sufficiently within the ambit of those concerns to permit the agents to search for that [under the warrant]." The court concluded that the child pornography images were "instrumentalities of criminal activity" and therefore that its seizure was authorized by the warrant. In upholding the district court's decision to admit the child pornography as evidence, the appellate court reiterated the lower court's finding that the child pornography fell squarely within the scope of the search warrant. Alternatively, the appellate court held that, even if the officers exceeded the limits of the warrant, the seizure of the child pornography was justified under the plain-view exception to the warrant requirement. A copy of the opinion may be found at <http://pacer.ca4.uscourts.gov/opinion.pdf/085000.P.pdf>

---

## **MICROSOFT PUTS A TIME LIMIT ON BING DATA**

On January 19th, Microsoft announced that it would comply with European regulators and discard all data collected on users of its Bing search engine after 6 months. Like other search engines, Bing had been keeping user data for more than 18 months. In its announcement, Microsoft said it would delete I.P. addresses after six months but would retain cookies and other session identifiers for 18 months. The decision comes after a European advisory group had been critical of how search engines collect and retain data on individuals for advertising purposes. In 2008, a panel of national privacy regulators from each European Union country asked the big three – Microsoft, Google, and Yahoo – to eliminate all online query data, like a computer's unique identification number, location, and the text typed into search fields after six months. Previously, Microsoft had said it would change its protocols, but only if its major competitors did too. Hendrik Speck, a professor of computer science in Germany, believes that Microsoft's change of heart came after it realized that consumers around the world are placing an increasing value on privacy and that can have business consequences. Speck believes that Microsoft's competitors will likely follow suit, driven largely by the same concerns that likely caused Microsoft to change its policy. In fact, Yahoo, which had been deleting only a portion of individual I.P. addresses, said it would now delete the entire address after 90 days and make anonymous the log of a user's activities. Google, however, has yet to indicate whether it would accept the European Union's demands. For now, the company's global privacy counsel, Peter Fleischer, has made it clear that the company believes its policy of making user data anonymous after nine months strikes the proper balance between ensuring user privacy and refining the functioning of its leading search engine. A copy of the story may be found at <http://www.nytimes.com/2010/01/20/technology/companies/20search.html>

---


*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 © 2010 Sensei Enterprises, Inc. All rights reserved.**