**News Highlights in This Issue:**

- 44 Attorneys General Settle with ChoicePoint
- Remote Search of Computer is Constitutional
- Don’t Miss Free Spyware/Phishing Training
- Internet Fraud in U.S. at New High
- Iowa Senate Votes to Tax Download Products
- Report on Combating ID Theft Available
- Online Auction Insufficient for Jurisdiction
- Teen Behavior on Internet Profiled by Pew
- Washington Outlaws Driving While Texting
- Cyber Guide for Decision Makers Published
- No Privacy in Personal Computer at Work
- Committees Pass New York Net Neutrality Bill
- Web Site May Be Liable for User Input
- Delaware Strengthens Sex Offender Reporting
- Thumbnail Images Do Not Infringe Copyright
- U.S. Puts 12 Nations on Piracy List
- Oklahoma to Allow Internet Ban for Offenders
- Anti-Spam Technique Approved by Board
- House Approves Two Preemptive Spyware Bills
- Study Finds Internet Censorship on the Rise

**Table of Contents**

**Features**
- Search Incident to Arrest, Digital Devices
- Register for Spyware/Phishing Training
- Cyber Guide for Decision Makers Published

**AGs Fighting Cyber Crimes**
- 44 AGs Settle With ChoicePoint
- Florida, Kentucky AGs Stop Net Pharmacy
- AG Goddard Says Porn Possession Charged
- Connecticut AG Asks Firm to Protect Data
- AG McCallum Says 126 Caught in Sting
- Hawaii AG’s Agents Arrest Predator
- AG Madigan Seeks Sex Offenders’ Status
- Kansas AG Applauds Passage of Predator Bill
- AG Foti Forms Southwest ICAC Unit
- Maryland AG Launches Cyber Safety Program
- AG Coakley Launches Cyber Initiative
- Michigan AG Arrests Internet Predator
- AG Hood Says Child Pornographer Sentenced
- New Hampshire AG Gives Cyber Safety Talk
- AG King Asks Schools to Join Net Safety Plan
- New York AG Stops Internet Auction Scheme
- AG Cooper Testifies on Penalties for Predators
- Pennsylvania AG Arrests Child Predator
- AG McMaster Says Net Predator Arrested
- Texas AG Says Predator Got 70 Years
- AG Shurtleff Says Pornographer Arrested
- Washington AG Settles With Deceptive Sites

**In the Courts**
- Remote Search of Computer Constitutional
- No Privacy in Personal Computer at Work
- EBAY Transaction Insufficient for Jurisdiction
- Multiple Porn Counts Require Multiple Transactions
- Web Site May Be Liable for User Comments
- Out-of-State Internet Pharmacist Can Be Charged
- Thumbnail Images Do Not Infringe Copyright

**News You Can Use**
- Internet Fraud at All Time High
- Report: 2007 Will Be Good for Cyber Crooks
- Copyright Boards Rejects Net Radio Appeal
- Paw Profiles Teen Behavior on Internet
- Cyberiquetion is Biggest Threat to Brands
- U.S. Puts 12 Countries on Piracy List
- Cost of Piracy to Businesses Rising Yearly
- FCC Issues Privacy Rules for Wireless
- Survey Finds Internet Censorship Rising
- Anti-Spam Technique Approved by Key Body

**Legislation Update**
- Iowa Senate Votes to Tax Downloaded Products
- Oklahoma to Allow Internet Ban for Offenders
- Anti-Spam Technique Approved by Board
- House Approves Two Preemptive Spyware Bills
- Study Finds Internet Censorship on the Rise

**Tools You Can Use**
- Combating ID Theft Report Available
- Digital Data Acquisition Tool Tested
SEARCH INCIDENT TO ARREST AND DIGITAL DEVICES

By Marc M. Harrold*  

Search incident to a lawful arrest is a broad, well-settled exception to the Fourth Amendment that allows arresting officers to perform such a search without a warrant. Further, not only is the search incident to arrest doctrine an exception to the Fourth Amendment’s warrant requirement, it has been deemed a “reasonable” search under that Amendment as well.1 The search extends both to the arrestee’s person and to containers, whether opened or closed,2 within the arrestee’s reach or “area within his immediate control.”3  

In United States v. Robinson,4 the U.S. Supreme Court upheld the validity of a warrantless search incident to a lawful arrest where a police officer, after arresting an individual for driving while his license was revoked, inspected a crumpled cigarette package and discovered that it contained heroin. It did not appear that the officer was searching for weapons or instruments of escape when he inspected the package of cigarettes. It was also highly unlikely that the officer was inspecting the crumpled package of cigarettes specifically to uncover evidence related to Robinson’s arrest for driving on a revoked license.  

Are cell phones, PDAs and laptop computers types of “containers” that can be searched incident to a lawful arrest?  

Suppose that, instead of a crumpled cigarette package, Robinson had a cell phone or PDA in his shirt pocket when he was subject to a full custodial arrest for driving on a revoked license? What if, clearly within his reach and subject to his control, was a laptop computer?  

When I have presented this scenario to law students, attorneys and even judges, there is an intuitive backlash that this type of search should violate the Fourth Amendment. Most individuals begin to perform some type of balancing to determine if this search would be “reasonable.” Most often, the main factors in this balancing are the role the electronic device might play in the underlying criminal activity and the probability the police will discover relevant digital evidence by searching the particular electronic device.  

Arguably, this type of reasonableness balancing is unnecessary as the U.S. Supreme Court has already deemed this type of search to be reasonable, not based on any specific facts or individualized suspicion, but based solely on the...
fact that the individual is subject to a lawful, custodial arrest:

A CUSTODIAL ARREST OF A SUSPECT BASED ON PROBABLE CAUSE IS A REASONABLE INTRUSION UNDER THE FOURTH AMENDMENT; THAT INTRUSION BEING LAWFUL, A SEARCH INCIDENT TO THE ARREST REQUIRES NO ADDITIONAL JUSTIFICATION. IT IS THE FACT OF THE LAWFUL ARREST WHICH ESTABLISHES THE AUTHORITY TO SEARCH, AND WE HOLD THAT IN THE CASE OF A LAWFUL CUSTODIAL ARREST A FULL SEARCH OF THE PERSON IS NOT ONLY AN EXCEPTION TO THE WARRANT REQUIREMENT OF THE FOURTH AMENDMENT, BUT IS ALSO A “REASONABLE” SEARCH UNDER THAT AMENDMENT.5

As such, it seems that a digital device (cell phone, PDA, laptop) can be treated as an ordinary open or closed container for analysis under the search incident to a lawful arrest doctrine. This assertion is based entirely on federal Fourth Amendment jurisprudence. A state constitution could provide for more protection against this type of search than the federal constitution, and state legislators and even individual law enforcement agencies are free to create legislation, regulations, and operating procedures that do not permit this type of search.6 Further, it may be forensically unsound to perform such a search. I only seek to answer the question: can police perform such a search without violating the Fourth Amendment? (Not whether they, in fact, should.)

United States v. Finley

A recent Fifth Circuit Court of Appeals case, United States v. Finley,7 addresses this question with regards to cell phones. Finley was arrested at the scene of a traffic stop made pursuant to a narcotics investigation. The custodial arrest was lawful and was not in dispute. Incident to his arrest,8 police seized a cell phone from Finley’s person. The Fifth Circuit applied standard search incident to arrest analysis and held that the police did not violate the Fourth Amendment when they retrieved “call records and text messages” from his cell phone.9

Although the court in Finley does indicate that the police officers were likely searching the cell phone for specific evidence of narcotics activity10 (the crime prompting the arrest), this language is contextual and should not be read to limit the search incident to arrest doctrine only to situations where additional suspicion or justification is present. Specifically, the court cites to the very section of Robinson where the U.S. Supreme Court expressly rejects this type of additional suspicion requirement from the search incident to lawful arrest:

A POLICE OFFICER’S DETERMINATION AS TO HOW AND WHERE TO SEARCH THE PERSON OF A SUSPECT WHOM HE HAS ARRESTED IS NECESSARILY A QUICK AD HOC JUDGMENT WHICH THE FOURTH AMENDMENT DOES NOT REQUIRE TO BE BROKEN DOWN IN EACH INSTANCE INTO AN ANALYSIS OF EACH STEP IN THE SEARCH. THE AUTHORITY TO SEARCH THE PERSON INCIDENT TO A LAWFUL CUSTODIAL ARREST, WHILE BASED UPON THE NEED TO DISARM AND DISCOVER EVIDENCE, DOES NOT DEPEND ON WHAT A COURT MAY LATER DECIDE WAS THE PROBABILITY IN A PARTICULAR ARREST SITUATION THAT WEAPONS OR EVIDENCE WOULD IN FACT BE FOUND UPON THE PERSON OF THE SUSPECT.

In 1973, in the passage above, the Court spoke specifically to the search of “the person.”11 However, as previously stated, the doctrine has been expanded to include containers, whether opened or closed, within the arrestee’s reach.12
Conclusion

Were the U.S. Supreme Court to revisit this issue of scope, it would not be the first time. Initially, in *Chimel v. California:* 13

[T]he Supreme Court attempted to tie strictly the scope of the search to “the circumstances which rendered its initiation permissible,” but the Court subsequently rejected that position in *United States v. Robinson.* The majority in *Robinson* was unwilling to place on the arresting officer the burden of deciding in each case “whether or not there [is] present one of the reasons supporting the authority for the search of the person incident to a lawful arrest”14

Regardless, the Court could hold that digital devices are somehow different than every other container encountered and searched by police incident to a lawful arrest. The Court would not only have to limit the scope of a particular exception to the warrant requirement of the Fourth Amendment, but also hold that a search incident to arrest is not *per se* “reasonable,” as has been well-settled jurisprudence for over three decades.15 By doing this, the Court would complicate a well-settled, practical search and seizure doctrine and would, at least in the realm of ever-changing and evolving digital devices, necessitate the need for the very type of “*ad hoc*”16 reasonableness balancing it expressly and wisely rejected and abandoned in *Robinson.*

---

* Senior Counsel, National Center for Justice and the Rule of Law; Visiting Professor of Law, University of Mississippi School of Law.

1 *United States v. Robinson,* 414 U.S. 218, 235 (1973)


5 Id. at 235.

6 This refers only to permitting a search incident to arrest of the digital device. During a custodial arrest, the device would inevitably be seized / inventoried and placed into police property. Police would, of course, be free to obtain a search warrant if probable cause existed and search the item at that time.

7 477 F.3d 250 (5th Cir. 2007).

8 Finley had actually been transported to a residence at the time the cell phone was seized. This fact did not alter the court’s holding as it deemed the search to be “substantially contemporaneous.” *Finley,* 477 at 260 n. 7 (“The fact that the search took place after the police transported Finley to Brown’s residence does not alter our conclusion.”)

9 *Finley,* 477 F.3d at 260.

10 *Finley,* 477 F.3d at 259-60

11 *Robinson,* 414 U.S. at 235.

12 *Belton,* 453 U.S. at 460-61; *Finley,* 477 F.3d at 259-60.


14 *Mary Beth G. v. City of Chicago,* 723 F.2d 1263, 1269 (7th Cir. 1983) (Internal citations omitted)

15 There is text and a footnote in *United States v. Edwards,* a 1974 U.S. Supreme Court ruling (only one year after *Robinson*) that appears inconsistent with the *Robinson* opinion. *United States v. Edwards,* 415 U.S. 809 (1974) (“In upholding this search and seizure, we do not conclude that the Warrant Clause of the Fourth Amendment is never applicable to postarrest seizures of the effects of an arrestee.”). *See also Edwards,* 415 U.S. at 809 n. 9. Factually, the arrestee in *Edwards* had been transported and was incarcerated in a correctional facility at the time of the search so it seems to blur the line between search incident to arrest and an administrative search performed at a jail. However, the specific doctrine discussed throughout *Edwards* is “warrantless searches incident to custodial arrests,” (*Edwards,* 415 U.S. at 802) and later the Court reaffirms that it is the incident to arrest doctrine under consideration stating, “[E]ven on these terms, it seems to us that the normal processes incident to arrest and custody had not been completed when Edwards was placed in his cell…” *Id.* at 804. The Court then states that as this is “contemporaneous,” and its view that “[w]ith or without probable cause, the authorities were entitled at that point not only to search Edwards’ clothing…” *Id.* at 804-05. Given this language that comports with *Robinson,* the language placed in Footnote 9: “Holding the Warrant Clause inapplicable in the circumstances present here does not leave law enforcement officials subject to no restraints. This type of police conduct must [still] be tested by the Fourth Amendment’s general proscription against unreasonable searches and seizures.” *Edwards,* 415 U.S. 808-09 n. 9 (quoting *Terry v. Ohio,* 392 U.S. 1 (1968)), seems inconsistent with the *Robinson* ruling a year earlier: “we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a ‘reasonable’ search under that Amendment.” *Robinson,* 414 U.S. at 235.

16 *Robinson,* 414 U.S. at 235.
DON’T MISS IT!
ADVANCED TRAINING ON SPYWARE/PHISHING SET FOR AUGUST

An Advanced Training on “What AAGs Need to Know About Spyware and Phishing: Approaches to Prosecution and Pitfalls to Avoid” will be held on August 28-30 at the University of Mississippi School of Law under the partnership between the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL) at the University. The course will be offered at no cost to AAGs from Attorney General offices.

The training will include sessions on state legislative approaches to spyware and phishing, privacy issues and tools and techniques for investigating these cases. Attendees will also hear from assistant attorney generals across the country who have “been there and done that” in handling these crimes.

A registration form is included on the back page of this e-newsletter. For additional information, please contact Hedda Litwin, Cyber Crime Counsel at NAAG, at hlitwin@naag.org or (202) 326-6022.

CYBER GUIDE FOR DECISION MAKERS PUBLISHED

The National Center for Justice and the Rule of Law (NCJRL) recently published Combating Cyber Crime: Essential Tools and Effective Organizational Structures—A Guide for Policy Makers and Managers (“Guide”). This Guide is intended to assist policy makers and managers by providing information about the need to combat cyber crime. It outlines the essential tools that are necessary to combat cyber crime and provides decision makers with options so that they can effectively address the complex and varied dimensions of cyber crime in their jurisdiction. This publication is part of the NCJRL’s Cyber Crime Initiative. For additional information about the Guide, please contact Marc Harrold, Senior Counsel at NCJRL, at mharrold@olemiss.edu.

AGs FIGHTING CYBER CRIMES

MULTI-STATE

The Attorneys General of 43 states and the District of Columbia entered into a settlement with ChoicePoint, Inc., a Georgia-based consumer data provider, in which the company agreed to adopt stronger security measures over allegations it failed to adequately secure consumers’ personal information related to a breach of its database. Among the measures the company will take are written certification for access to consumer reports and, in some cases, onsite visits by ChoicePoint to ensure the legitimacy of companies before they are allowed to access personally identifiable information. ChoicePoint will also conduct periodic audits to ensure that companies are using consumer data for legitimate purposes. It will pay $500,000 for the states to share for public education.

Attorneys General Bill McCollum of Florida and Greg Stumbo of Kentucky cooperated on an investigation resulting in a seizure by agents of the Kentucky Bureau of Investigation (KBI) of illegal shipments of Phentermine, a weight loss drug with potentially serious side effects, from a shipping hub where they had been shipped to state residents from an unlicensed Internet pharmacy in Florida. The bottles of drugs were suspicious because they only had the customer and prescription name and none of the information Kentucky and the Drug Enforcement Administration (DEA) require of Internet pharmacies. KBI agents worked in cooperation with the Kentucky State Police, the DEA, the U.S. Attorney’s Office, the Kentucky National Guard, the Kentucky Board of Pharmacy and the Florida Department of Law Enforcement.

ARIZONA

Attorney General Terry Goddard announced that Christopher Breiland and Marie Siegal were arraigned on multiple charges related to identity theft and possession of child pornography. The indictment alleges that the defendants knowingly had child pornography photos on their computer. Both defendants also possessed equipment capable of producing fake IDs. If convicted of all charges, Breiland faces up to 115 years in prison and Siegal faces up to 85 years. The indictment resulted from an investigation conducted by the U.S. Postal Inspection Service.

CONNECTICUT

Attorney General Richard Blumenthal, after learning of a massive security breach at Pfizer, sent a letter to the company asking them to take specific steps to protect its employees. The letter is part of Attorney General Blumenthal’s investigation into a compromise of confidential information of thousands of Pfizer employees, including 305 in Connecticut. Attorney General Blumenthal asked that Pfizer provide information on when the breach occurred, exactly what information was compromised, what steps it took after learning of the breach and its policies for handling personal information and security compromises.

FLORIDA

Attorney General Bill McCollum announced that 126 alleged child predators were arrested by a task force of local, state and federal law enforcement officials, including Attorney General McCollum’s Child Predator CyberCrime Unit. The arrests were part of “Operation Eviction,” a five-month initiative targeting individuals who prey on children over the Internet and coordinated by the Florida Department of Law Enforcement in support of the U.S. Attorney General’s Project Safe Childhood. In addition to Attorney General McCollum’s CyberCrime Unit, participants included the Florida Department of Law Enforcement’s Computer Crime Center, the North Florida and South Florida Internet Crimes Against Children task forces, the U.S. Attorney’s Office and local law enforcement agencies. During the operation, 261 investigations were initiated and 87 search warrants were executed.

HAWAII

Attorney General Mark Bennett announced that law enforcement agents of the Hawaii Internet Crimes Against Children Task Force, including his Department, arrested Thomas Puckett on two offenses of Electronic Enticement of a Child in the first degree. Puckett asked whom he thought were two 13-year-old girls, but were actually undercover investigators, to meet him at a
marketplace where he would take them to a hotel room for sex. He was arrested shortly after arriving at the meeting place. Also participating in the arrest were the Honolulu Police Department, the FBI and the U.S. Immigration and Customs Enforcement.

ILLINOIS

Attorney General Lisa Madigan’s investigators, together with the Chicago Police Department, the U.S. Marshals Service and the Illinois Department of Corrections, completed an intensive three-day operation to assess the compliance status of 70 convicted child pornographers currently registered as living in Chicago. The team checked the registered addresses of the 70 offenders and determined that six offenders were non-compliant. They left notices for 31 offenders, advising them to check in by calling the Illinois Sex Offender Registry Team (I-SORT) hotline. The team will also follow up with seven offenders who were left notices but have not yet checked in and will find the six non-compliant offenders as part of the continuing Operation Location Unknown.

KANSAS

Attorney General Paul Morrison applauded the passing of legislation, drafted by his office, aimed at protecting children from Internet predators. One law requires sex offenders to register more often and provide more identifying information, including e-mail addresses and user names. The second law mandates that all second time offenders receive a 40-year sentence.

LOUISIANA

Attorney General Charles Foti, Jr. announced the formation of the Southwest Internet Crimes Against Children (ICAC) Task Force. The new task force is part of the Louisiana ICAC Task Force and the second one of its kind in the state.

MARYLAND

Attorney General Douglas Gansler launched “C.L.I.C.K.S.,” – Community Leadership in Cyber Knowledge and Safety, a statewide Internet safety initiative to equip law enforcement and school officials with the resources to teach students and parents about Internet safety. Attorney General Gansler partnered with Netsmartz, interactive, educational safety resource developed by the National Center for Missing & Exploited Children and Boys & Girls Clubs of America. The first session will be held on July 31 at a high school in Ellicott City.

MASSACHUSETTS

Attorney General Martha Coakley launched the Massachusetts Cyber-crime Initiative, an effort to develop a comprehensive, state-wide approach to cybercrime and fraud in the Commonwealth. The first step in the Initiative, which is currently underway, is to conduct , state-wide assessment of the cybercrime resources and needs of law enforcement and prosecutors in Massachusetts. Using the data obtained through a survey, Attorney General Coakley and key stakeholders will develop and implement a strategic plan to create a coordinated, approach to the investigation and prosecution of crimes involving digital evidence. In addition to providing law enforcement and prosecution offices with extensive training in evidence identification, collection and forensic analysis, the Initiative will focus on enlisting local law enforcement as partners in education and prevention in communities throughout Massachusetts.

Ed. Note: The Editor thanks Tom Ralph, Assistant Attorney General and Chief of the Cyber Crime Division in the Office of the Attorney General of Massachusetts, for the information contained in this story.

MICHIGAN

Attorney General Mike Cox announced the arrest of Cornell educator Barry Shaffer for using the Internet to arrange a sexual encounter with a minor. Shaffer is alleged to have engaged in
graphic sexual conversation online, and propositioned for sex, with who he thought was a 15-year-old girl he met in a chat room, but was actually one of Attorney General Cox’s investigators. Shaffer was arrested when he traveled from his home in New York to an apartment complex in Michigan, allegedly to have sex with a minor. He is charged with one count each of Child Sexually Abusive Activity and Using a Computer to Communicate with Another to Commit Child Sexually Abusive Activity, both 20-year felonies, and two counts of Using a Computer to Communicate with Another to Disseminate Sexually Explicit Matter to a Minor, a four-year felony.

MISSISSIPPI

Attorney General Jim Hood announced the sentencing of Warren Gallaher, a community college professor instructor, who pled guilty to 12 counts of possession of child pornography. Gallaher was sentenced to serve 16 years with 12 years suspended and four years in the custody of the state Department of Corrections, with sentences to run concurrently. Upon release, Gallaher will be placed on five years of post-release supervision, and his Internet/computer usage will be restricted to work purposes only and will be monitored at random by Attorney General Hood’s Cyber Crime Division. Gallaher was also ordered to pay $2,000 in fines. The case originated with the Hinds Community College campus police who enlisted the Unit’s assistance. The Unit then conducted the investigation and forensic analysis of Gallaher’s computer and prosecuted the case.

NEW HAMPSHIRE

Attorney General Kelly Ayotte addressed fifth through eighth grade students at a Concord school on the potential dangers when using the Internet. She made a PowerPoint presentation and distributed her Internet Safety Guide, which offers tips on how teens can protect themselves online.

NEW MEXICO

Attorney General Gary King sent a letter to school superintendents and high school principals across the state proposing that they cooperate with his office in an Internet safety program. The program would train high school juniors and seniors on how to teach middle school students about responsible and safe use of the Internet, especially the use of chat rooms, MySpace and blogs. Students trained under the program would be permitted to give Internet safety presentations to other students in their area. Attorney General King’s office would coordinate the training and supply the materials. The program is being developed by Sam Thompson, Education and Public Outreach Coordinator for the office.

NEW YORK

Attorney General Andrew Cuomo’s office cracked down on a nationwide online auction fraud scheme that tricked consumers out of hundreds of thousands of dollars. Ezra Dweck and employees of his company, ENH Group, LLC, one of the nation’s largest jewelry auction houses, secretly placed bids on their own online auctions and illegally inflated the prices of goods they sold, a practice called shill bidding. Over the course of one year, Dweck directed his employees to place more than 232,000 shill bids worth over $5 million. Under the terms of the settlement with Attorney General Cuomo’s office, Dweck and EMH Group will pay $400,000 in restitution and penalties and are banned from the online auction industry for four years. If they choose to resume their business after that time, they will be monitored by Attorney General Cuomo’s office and must preserve all relevant records and make them available upon request.

NORTH CAROLINA

Attorney General Roy Cooper testified before the state Senate Judiciary Committee, calling for harsher penalties and more restrictions to fight child predators. He supports a bill that would increase the punishment for child exploitation,
require photo developers and computer technicians to report suspected child pornography and also require parental consent for children to use social networking web sites like MySpace.

PENNSYLVANIA

Attorney General Tom Corbett’s Child Predator Unit agents arrested Stephen Turchetta, who is accused of using an Internet chat room to sexually proposition what he believed to be a 13-year-old girl, but was actually an undercover agent from the Unit. Turchetta also sent the “girl” sexually graphic photos and videos. When agents arrested Turchetta at his home, they also seized computers and electronic equipment, which will be analyzed by Attorney General Corbett’s Computer Forensics Unit as part of an ongoing investigation. Agents also seized an assault rifle and several ounces of marijuana. Turchetta is charged with five counts each of unlawful contact with a minor and criminal use of a computer, both third-degree felonies punishable by up to seven years in prison and a $15,000 fine. The Altoona Police Department participated on the case, which will be prosecuted by Deputy Attorney General William Caye of Attorney General Corbett’s Child Predator Unit.

SOUTH CAROLINA

Attorney General Henry McMaster announced that Max Culp, an employee of a computer consulting company, was arrested in an undercover Internet sting conducted by the Spartanburg County Sheriff’s Office, a member of Attorney General McMaster’s Internet Crimes Against Children (ICAC) Task Force. Arrest warrants allege that Culp solicited sex on the Internet with an individual he believed to be a 13-year-old girl, but was actually an undercover officer. A search warrant was executed at his residence and resulted in the seizure of several computers, computer hard drives and computer-related items. Culp was charged with one count of Criminal Solicitation of a Minor, a felony offense punishable by up to 10 years imprisonment. The City of Charlestown Police Department, another member of the ICAC Task Force, assisted in the arrest.

TEXAS

Attorney General Greg Abbott announced that Dionicio Robles, Jr., a child predator arrested by his Cyber Crimes Unit, was sentenced to 70 years in state prison for using the Internet to exploit children. Robles was arrested after he e-mailed graphic images of himself to a person he believed was a 13-year-old girl and propositioned the child for sex. When he arrived at a proposed meeting place, Robles discovered that the “girl” was actually an undercover Unit investigator. Forensic analysis conducted by the Unit revealed hundreds of images of child pornography on Robles’ computer. The sentence handed down reflects the maximum terms for all three counts of online solicitation and all seven counts of possession of child pornography. The sentences will run concurrently.

UTAH

Attorney General Mark Shurtleff announced that the Utah Crimes Against Children (ICAC) Task Force arrested Jeffery Burton for allegedly sexually abusing a six-year-old boy and manufacturing and distributing child pornography. The Task Force seized Burton’s computer, computer discs, video and DVDs depicting nude children and children being sexually abused. Burton is being held on suspicion of one first degree felony count of sodomy on a child and seven second degree counts of sexual exploitation of a minor.

WASHINGTON

Attorney General Rob McKenna’s office settled with the operators of www.privasafe.com and www.surfsafeinternetservices.com under which thousands of state consumers are eligible for refunds which could ultimately cost defendants $1 million. Attorney General McKenna’s office alleged that the defendants lured state consumers with online offers in pop-up and banner ads and e-mail messages for “free” gifts, including flat screen monitors. After consumers submitted personal
information, they were billed based on a statement at the bottom of the web page that said only paying customers would receive the “free” gift. The statement also included a link to a privacy policy that waived the consumers’ rights under federal laws. Attorney General McKenna’s office also alleged that defendants sold personal information provided by state consumers to numerous third-party marketers. As a result of the settlement, defendants are no longer billing state consumers and are prohibited from selling or sharing any information collected.

IN THE COURTS

FOURTH AMENDMENT: REMOTE SEARCH OF COMPUTER

*United States v. Heckenkamp*, 2007 US App. LEXIS 7806 (9th Cir. April 5, 2007). The 9th Circuit Court of Appeals ruled that a remote search of files on the hard drive of a computer suspected of being used to hack into a university network is constitutional. Qualcomm Corporation notified the FBI that someone had hacked into their network. The FBI traced the intrusion to a computer on the University of Wisconsin’s network and asked University administrator Jeffrey Savoy to help locate it. Discovering that the University’s own system was hacked, Savoy determined the computer’s IP address and traced the computer to Jerome Hackenkamp, a computer science graduate student. Savoy and university police officers went to Heckenkamp’s room and disconnected the network cord from the computer. FBI agents later searched the room and seized the computer pursuant to a warrant. Heckenkamp was indicted in the U.S. District Court for the Northern District of California on violation of 18 U.S.C. Sec. 1030(a)(5)(B) – recklessly causing damage by intentionally accessing a protected computer without authorization. Heckenkamp moved to suppress Savoy’s warrantless remote search, which the district court denied. Heckenkamp conditionally pled, then appealed. The 9th Circuit said the remoteless search was justified under the “special needs” exception to the Fourth Amendment’s warrant requirement, which renders a warrant unnecessary when special needs make the warrant and probable cause requirement unnecessary. While finding that the University’s computer policy mandated that all computer files would be free from unauthorized access, the policy was overridden by Savoy, who was not acting for law enforcement and believed the system was in jeopardy.

EXPECTATION OF PRIVACY: PERSONAL COMPUTER AT WORK

*United States v. Barrows*, 2007 U.S. App. LEXIS 7621 (10th Cir. April 3, 2007). Michael Barrows, a city treasurer, brought his personal computer to work so he wouldn’t have to share a computer with a clerk. The computer was connected to the city network and there was no password. When Barrows was out of the office, a problem occurred on the network which was traced to Barrows’ computer. A reserve police officer noted that there was a file-sharing program running and then found several
child pornography images. He told police, who got a warrant and seized the computer. Barrows was indicted and convicted on one federal count of possessing child pornography. He appealed, arguing that he had an expectation of privacy in his computer when he took it to work. Although courts have split on warrantless workplace searches, the 10th Circuit found that Barrows took no steps to make the computer private, such as using a password or turning it off, thus the fact that the computer was personally owned lost significance. The 10th Circuit affirmed the lower court conviction.

**PERSONAL JURISDICTION:**

**EBAY TRANSACTIONS**

*Great Notions, Inc. v. Danyeur,* 2007 WL 944407 (N.D. Tex., March 28, 2007). The U.S. District Court for the Northern District of Texas fell into line with several other courts’ decisions in finding that the online auction process is insufficient to confer personal jurisdiction over an out-of-state defendant. Great Notions sued Thomas Danyeur of Arkansas for copyright infringement and unfair competition, accusing him of counterfeiting and selling Great Notions’ designs through eBay. Danyeur moved to dismiss for lack of personal jurisdiction, and the court granted the motion, dismissing the case without prejudice. The court held that conducting an eBay auction was insufficient to confer personal jurisdiction.

**PO SSESSION OF CHILD PORNOGRAPHY: MULTIPLE COUNTS**

*United States v. Buchanan,* No. 04-41364 (5th Cir., April 10, 2007). The 5th Circuit found that the government had failed to prove that the defendant’s possession of multiple pornographic images constituted multiple counts. Michael Buchanan was a park ranger for the Army Corps of Engineers, which assigns a computer with unique password to each ranger. When his station’s network experienced slow Internet access, the administrator discovered that Buchanan was using the Corps computer to view and download adult and child pornography. The administrator copied Buchanan’s files onto a disc and gave it to the FBI. An FBI agent found four large images of child pornography, and later an FBI forensic examiner found an additional 127 images. A “thorough sweep” of Buchanan’s hard drive found “hidden” files containing more than 3,000 pornographic images. Buchanan was indicted on four counts of “receipt and attempted receipt of child pornography” under 18 U.S.C. §§ 2252(a)(2) and 2252(b)(1) – one count each for the images retrieved from the CD provided by the administrator. He was charged with a fifth count for “possession of child pornography” under 18 U.S.C. § 2252(a)(4)(A) based on 11 images found on his hard drive. He was subsequently convicted of all five counts and sentenced to seven months on each of the first four counts and 60 months on the fifth count, all to be served concurrently. He also was fined a $100 “special assessment” for each count and a $5,000 fine for all counts. On appeal, Buchanan argued that the convictions obtained from the four counts were
“multiplicitous” because the indictment didn’t allege that his receipt of the four images was the result of four separate transactions. The 5th Circuit agreed, finding that the government did not establish that Buchanan received the four images on four separate occasions. It ordered the four convictions under § 2252 set aside and ordered the court below to reinstate a single count and resentence Buchanan accordingly.

**STATUTE OF LIMITATIONS: SINGLE PUBLICATION RULE**

*Canatella v. Van de Kamp*, No. 06-15186 (9th Cir., May 3, 2007). The 9th Circuit Court of Appeals ruled that under the single publication rule, the statute of limitations for a claim arising from online material begins on the date the material is first available online. Attorney Joseph Canatella sued the California State Bar in July 2005, alleging that the posting of his disciplinary sanctions summary on the Bar’s web site violated his constitutional right to privacy. Although the Bar published the summary in February 2000, Canatella claimed he did not discover the posting until later. The Bar moved to dismiss on the ground that the one year limitations period had run on his claims, and the U.S. District Court for the Northern District of California agreed. On appeal, Canatella argued that the Bar’s reposting of his summary on his member search page after August 2003 constituted a new publication and therefore a new cause of action. The 9th Circuit rejected Canatella’s argument that the single publication rule, which states that a single publication gives rise to only one cause of action, did not apply to him. Under the rule, the one-year limitations period began to run on Canatella’s claim in February 2000 and expired before the suit was brought.

**LIABILITY: USER POSTINGS ON WEB SITE**

*Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, No. 04-56916 (9th Cir., May 15, 2007). Although court decisions have been almost unanimous that a web site isn’t liable for its users’ postings, a panel of the 9th Circuit Court of Appeals found that a web site that matches roommates may be liable for what its users say about their preferences. The suit was filed by two California fair housing groups, alleging that Roommates.com was violating the Fair Housing Act by allowing and encouraging its users to post notices stating preferences for roommates based on sex, race, religion and sexual orientation. Roommates.com offered users a menu, with choices such as gender, sexual orientation and whether children were involved, by which users could post their preferences. The panel unanimously found that because Roommates.com created the menus, it could not claim immunity under the Communications Decency Act. It sent the case back to the U.S. District Court for the Central District of California to determine whether the site had violated the Fair Housing Act, which forbids publishing real estate notices with preferences based on race, religion, sex or family status.

**INTERNET PHARMACIES: UNLICENSED PRACTICE**

resident who bought his drugs from an Internet pharmacy, could be prosecuted in state court for practicing without a California license. Following an investigation by the Medical Board of California, the San Mateo District Attorney’s Office charged Christian Hageseth, a Colorado physician, with violating state law by writing a prescription for the generic version of Prozac for a California resident who ordered the drug over the Internet. Hageseth wrote the prescription based on a health questionnaire filled out by the patient which the Internet pharmacy forwarded to him. Several weeks later, the patient committed suicide, allegedly while intoxicated by alcohol and with a measurable amount of the drug in his blood. Hageseth moved to quash the arrest warrant and dismiss the case on the ground that California had no jurisdiction because he had not engaged in any criminal conduct within the state. The San Mateo Superior Court disagreed and denied the motion. The First District Court of Appeal agreed, basing its decision on the “detrimental effects” theory of extraterritorial jurisdiction which states that if an activity causes a substantial detrimental effect in California, it can be prosecuted there.

COPYRIGHT INFRINGEMENT: THUMBNAIL IMAGES

Perfect 10 Inc. v. Amazon.com, Inc., 2007 US App. LEXIS 11420 (9th Cir. May 16, 2007). A three judge panel of the 9th Circuit unanimously held that thumbnail images provided by Google and Amazon search engines do not directly infringe display rights for purposes of the Copyright Act. At issue was Google’s Image Search that provides search results as a webpage of small images called “thumbnails” that when clicked, display an image from the third party website. These images would also appear on Amazon.com search results that Google provided at the time. Perfect 10, a company that markets and sells copyrighted images of nude models, brought a preliminary injunction action against Google and Amazon complaining that they were facilitating access to unauthorized images by displaying these thumbnails. On appeal, the 9th Circuit reversed the district court’s determination that Google’s thumbnail versions of Perfect 10’s images likely constituted direct infringement. The court reasoned that for purposes of the Copyright Act, thumbnail images provided by search engines that only communicate the HTML address of the copy are not direct infringements because they are merely links to the full image and the copy is not actually stored by Google’s computers. In addition, the court held that the thumbnail versions of the images themselves, even though stored in Google’s computer, were not direct infringements of Perfect 10’s display rights either. The court, in a fact-intensive analysis, reasoned that the significantly transformative nature of Google’s search engine, particularly the great social benefit it serves, outweighed any superseding and commercial uses of the thumbnails in this case. The 9th Circuit remanded the case however to determine whether Google and Amazon could be held secondarily liable for copyright infringement, because the district court did not undertake this analysis when it erroneously held Google liable for direct infringement.

Ed. Note: This case was reported by Coleman Adams, a third year law student at the University of Mississippi School of Law and current summer intern at NAAG’s Cybercrime Project.
NEWS YOU CAN USE

U.S. INTERNET FRAUD AT ALL TIME HIGH

A report by the Internet Crime Complaint Center, a joint enterprise of the FBI and the National White Collar Crime Center, on 2006 Internet crimes finds that Americans lost a record high of $198.4 million to Internet fraud schemes last year, up eight percent from 2005 levels of $183 million and up 191 percent from 2004 levels of $68 million. Law enforcement officials believe that actual losses are higher, as many victims don’t report the crimes. Of the Internet criminals who could be traced to their location, 61 percent resided in the United States, followed by 16 percent living in the United Kingdom and six percent in Nigeria. The statistics also show that victims of the Nigerian 419 scam had an average loss of $5,100 in 2006, an increase of $100 per incident compared with 2005 and an increase of $2,100 per incident compared with 2004. Of the 86,279 fraud complaints in 2006 that the Center referred to law enforcement agencies for investigation, Internet auction fraud accounted for the greatest volume with 45 percent of complaints. Second were complaints about non-delivery of items purchased on the Internet, followed by Internet-related check and credit card fraud.

REPORT: 2007 WILL BE GOOD YEAR FOR CYBER CROOKS

Everything from spam to spyware will become more dangerous in 2007, according to security firm McAfee’s semi-annual Sage journal, a roundup of the company’s ongoing security research. Among the specific trends outlined in the report are continued growth of botnets, particularly dangerous due to group efforts by hackers to develop and refine threat code. According to the report, most botnets will continue to target flaws in Microsoft products as well as propagate through buffer overflows. McAfee also expects that this year smart phones will be targeted, beginning first with phishing attacks, spyware and other programs aimed at stealing data to commit identify fraud. The report said that there will be more threats on VoIP systems, with SPIT (spam over Internet Telephony) providing new opportunities for hackers to market end user data. Other threats outlined in the report were the vulnerability of RFID (Radio Frequency Identification) devices to eavesdropping, recording, cloning and forgery and data leakage. The report can be accessed at www.mcafee.com/us/threat_center/default.asp.

COPYRIGHT BOARD REJECTS INTERNET RADIO APPEALS

Internet radio broadcasters were dealt another setback when a panel of copyright royalty judges rejected requests to reconsider a ruling that raised the royalties they must pay to record companies and artists. The broadcasters, including National Public Radio and online sites Yahoo Inc. and AOL, had objected to the new royalties set on March 2 of this year, saying it would force a drastic cutback in services
enjoyed by more than 50 million people. In the latest ruling, the board denied all motions for rehearing and also declined to postpone a deadline by which new royalties will have to be collected. However, they did grant leniency on one point by allowing webcasters to calculate fees by average listening hours, instead of the new system of charging a royalty every time a song is heard by an online listener. That exemption would apply only for 2007 and 2008, then the new per-listener fee structure would take effect. The royalties in question only apply to digital transmissions of music and not to terrestrial radio stations.

TEEN BEHAVIOR ON NET PROFILED

Teens generally don’t think twice about including their first names and photos on their online profiles, but most avoid using their full names or making their profiles fully public, according to a new survey by the Pew Internet and American Life Project. The survey found that two-thirds of teens with profiles on blogs or social networking sites have restricted access to their profiles, such as by requiring passwords or making them available only to an approved list. According to the Pew study, less than one third of teens with profiles use their last names and e-mail addresses, and only two percent list their cell phone numbers. However, 79 percent have included their photos, with girls more likely to do so. One-half also identify their schools. The study said that 45 percent of online teens have no profiles, a figure that contradicts widespread perceptions that teens are constantly on social networking sites. Half of the teens with social networking profiles say they use the sites to stay in touch with existing friends, while the other half use the sites to make new friends.

CYBERSQUATTING GREATEST THREAT TO CORPORATE BRANDS

Cybersquatting, in which illicit sites usurp popular trademarks, poses the greatest threat to corporate brands, according to a four week survey of public web sites by MarkMonitor, a company which supplies Internet brand protection services. Phishing and domain “kiting,” which involves the rapid registering and dropping of similar-sounding web site names, are also on the rise. The study tracked 134 million public web records for the top 25 brands, as well as major brands from eight industrial categories such as autos, apparel, food and high tech from March 9 – April 6, 2007. The study found that major brands suffered 286,000 incidents of cybersquatting. Click fraud, or siphoning off consumers via fake pay-per-click ads, was identified 50,743 times, e-commerce fraud occurred 21,093 times and kiting was present 11,015 times. MarkMonitor said that media and Internet companies were the biggest cybersquatting targets, receiving 31 percent of what the company calls “brand abuse,” while banks and other financial services were most often victims of kiting and phishing. According to the survey, the number of phishing attacks increased 104 percent during this period compared to the same period last year, with more than 229 brand name companies coming under assault.
U.S. PUTS 12 COUNTRIES ON COPYRIGHT PIRACY LIST

The administration issued an annual report required by Congress placing 12 nations on a “priority watch list” for copyright piracy which will subject them to extra scrutiny and possible economic sanctions. Known as the “Special 301 Report” for the section of U.S. trade law that it covers, its list was headed by China and Russia, followed by Argentina, Chile, Egypt, India, Israel, Lebanon, Thailand, Turkey, Ukraine and Venezuela. Another 31 countries were put on lower level monitoring lists, indicating the concerns about copyright violations in those nations did not warrant the highest level of scrutiny. Those countries placed on the lower level list were Belarus, Belize, Bolivia, Brazil, Canada, Colombia, Costa Rica, Dominican Republic, Ecuador, Guatemala, Hungary, Indonesia, Italy, Jamaica, South Korea, Kuwait, Lithuania, Malaysia, Mexico, Pakistan, Peru, Philippines, Poland, Romania, Saudi Arabia, Taiwan, Tajikistan, Turkmenistan, Uzbekistan and Vietnam.

And see…

LOSSES DUE TO SOFTWARE PIRACY GROW

Although the rate of global software piracy has remained constant for three years, the cost to businesses is rising, according to a survey for the U.S. Business Software Alliance (BSA) and conducted by the U.S.-based market research firm IDC. The survey concluded that for every two dollars (Euro 1.47) spent on legitimate software, one dollar (Euro 0.73) went to pirates. It further claimed that 35 percent of all the software installed on personal computers in 2006 was obtained illegally. Based on this figure, the survey estimated that software vendors could lose about $180 billion (Euro 133 billion) to pirates over the next four years. The report identified Armenia, Moldova and Azerbaijan as among the world’s worst for software theft, saying only one in 20 programs used there was procured legally. The U.S., New Zealand and Japan are among the “most” law abiding, with one in four programs there being pirated.

Researchers examined the software market in 102 countries, comparing software sales in each of the counties with estimates of the amount of software in use. They took the difference to be the pirated amount, calculating losses based on prices for copies of those programs.

FCC ISSUES PRIVACY RULES FOR WIRELESS OPERATORS

The Federal Communications Commission (FCC) issued an order prohibiting telephone and wireless operators from releasing, either over the phone or online, sensitive personal data, such as call detail records, unless the customer provides a password. It also requires them to notify their customers of a breach of confidentiality. Phone companies, including wireless and voice over Internet (VoIP) providers, must annually certify their compliance with the regulations, inform the FCC of any actions they have taken against data brokers and provide a summary of the complaints they receive regarding the unauthorized release of personal customer information. The regulations also require carriers to notify law enforcement authorities before impacted customers when they suspect breaches have occurred. The new rules will become effective six months after the
Office of Management and Budget approves them, a process that could take 120 days or more.

STATE-LED INTERNET CENSORSHIP ON THE RISE

A study of thousands of web sites across 120 Internet service providers found that 25 of 41 countries surveyed showed evidence of content filtering. This was compared to 2002, when only a handful of countries were carrying out “state-mandated net filtering.” The study by the Open Net Initiative (ONI), which is composed of research groups at the universities of Toronto, Harvard Law School, Oxford and Cambridge, noted that a number of countries in Europe were not tested because the private sector, rather than the government, tends to carry out filtering. The survey found evidence of filtering in the following countries: Azerbaijan, Bahrain, Burma/Myanmar, China, Ethiopia, India, Iran, Jordan, Libya, Morocco, Oman, Pakistan, Saudi Arabia, Singapore, South Korea, Sudan, Syria, Tajikistan, Thailand, Tunisia, Turkmenistan, United Arab Emirates, Uzbekistan, Vietnam and Yemen. ONI is also looking at the tools people use to circumvent filtering.

ANTI-SPAM TECHNIQUE APPROVED BY STANDARDS GROUP

The Internet Engineering Task Force, a Key Internet standards body, gave preliminary approval to DomainKeys Identified Mail (DKIM), a technology designed to detect and block fake e-mail messages. DKIM works by embedding a digital signature into the headers of an outgoing e-mail message. If the cryptographically secure signature checks out, the message can be delivered as usual; otherwise, it is flagged as spam. While DKIM appears more promising than existing anti-spam and anti-phishing techniques, which rely on techniques like assembling a “blacklist” of known fraudsters or detecting such messages by trying to identify common characteristics, it is only effective if both the sender’s and recipient’s mail systems are upgraded to support the standard. Additionally, it does not flag junk e-mail sent by a legitimate company or identify spam sent from a domain name with a true DKIM record. Yahoo, Cisco Systems, Sendmail and PGP Corporation issued a joint statement of support for DKIM, and other advocates include AOL, Earthlink, IBM, Verisign, IronPort Systems, Cox Communications and Trend Micro.

LEGISLATION UPDATE

INTERNET TAXES

The Iowa Senate voted 29-20 to approve S.F. 596, a bill that would impose the state’s sales tax on digital products downloaded from the Internet. If enacted, the bill is not supposed to generate significant tax revenues for the state, but its premise is to level the playing field for small Iowa retailers. The equivalent House bill is HF 923.
**DRIVING WHILE TEXTING**

On May 11, 2007, Washington Governor Christine Gregoire signed HB 1214 into law, making Washington the first state to impose a specific ban on reading or sending text messages while driving. Violation of the law, codified as Chapter 416 and effective on January 1, 2008, could result in a $101 fine, but only if law enforcement officers have another reason to pull over a motorist. Connecticut, New Jersey, New York and Washington, D.C. all have de facto bans on “DWT” under broader laws that prohibit drivers from using a cell phone while driving, other than using a hands-free speaker device, and California will impose a similar ban in July 2008.

**NET NEUTRALITY**

The New York Assembly is considering A. 3980, a sweeping measure to regulate the telecommunications and cable industry which also seeks to establish net neutrality. The bill would prohibit networks from favoring one particular network destination or class of applications over another. The bills has been passed out of both the Consumer Affairs and Protection and Corporations, Authorities and Commissions Committee and has now been referred to the Codes Committee.

**SEX OFFENDERS**

On May 17, 2007 Delaware Governor Ruth Minner signed Senate Bill 60 into law, legislation which strengthens reporting requirements for sex offenders who have been released from prison. The bill amends Megan’s Law in order to conform to changes required under the Adam Walsh Act. Specifically, registered sex offenders will be required to verify additional information in person to the Delaware State Police. High risk offenders must appear in person every 90 days, moderate risk offenders every 6 months, and low risk offenders annually. The additional information includes Social Security numbers, name changes, vehicle description and registration, additional residences, additional workplaces and additional places of study. Sex offenders will be photographed every time they register, re-register and appear to verify information. Offenders will have three business days to report any changes of information to the State Police. The amended legislation clarifies that a failure to verify information on the date on which the verification is required constitutes a criminal offense. Community notification procedures exempt the release of certain information and shall include a warning that civil or criminal liability may attach if information is used for an unlawful purpose. The time span for offenders extends to 25 years for moderate risk offenders and 15 years for low risk offenders. These amended laws are also applicable to all persons who, after June 27, 1994, have been declared a sex offender. The legislation is codified as Chapter 75:25.

On May 31, 2007, Oklahoma Governor Brad Henry signed into law an amendment to Title 22, Section 991a regarding sentencing of sex offenders. In addition to the other sentencing powers of the court, the amendment allows the court to also prohibit a sex offender from accessing or using an Internet social networking site that has the potential of allowing the offender to have contact with any child under the age of 18 years. A court may also require the offender to register an e-mail address or instant message, chat or other Internet communication name or identify information that the offender intends to use while accessing the Internet.

*Note: The Editor thanks Julie Bays, Assistant Attorney General in the Office of the Attorney General of Oklahoma, for information about this legislation.*
On the federal side, on May 2, Representative Ben Chandler (D-KY) introduced H.R. 2106, which requires states receiving funds for certain law enforcement assistance programs to put into effect laws and policies that prohibit parole for a sexually violent predator or any person convicted of a crime against a minor. The bill would grant states three years to implement the program, with one additional two-year extension for states making a good faith effort. Any state that does not implement such a program would be ineligible for 10 percent of its funding from the assistance programs. The bill has been referred to the Judiciary Committee.

DATA SECURITY BREACHES

The Senate Judiciary Committee considered and passed two bills regarding disclosure of security breaches of personal data, and soundly defeated a third bill. S. 1202, sponsored by Senator Jeff Sessions (R-AL), was rejected on a voice vote with almost no discussion because lawmakers said it contained loopholes and did not hold businesses accountable for compromised data systems. The bill stated that notification to consumers would be made “as expeditiously as possible and without unreasonable delay.” It would have required both agencies and “persons” that collect personal information from consumers to disclose security breaches only if there exists “a reasonable basis to conclude that a significant risk of identity theft to an individual exists.”

S. 239, sponsored by Senator Dianne Feinstein (D-CA), was approved by voice vote. It requires federal agencies and businesses that engage in interstate commerce and which collect, store or use personal information to notify its clients or consumers in the event of a security breach. Companies found in violation could be subject to civil penalties of up to $1 million. The bill states that agencies or businesses should make notifications “without unreasonable delay” following a breach, and defines “reasonable delay” as “time necessary to determine the scope of the breach, prevent further disclosures and restore the integrity of the data system and provide notice to law enforcement when required.” It will fall to the companies to prove they made timely notification. The bill also specifies that notification can be made in writing, via telephone or e-mail, if permission has been given in advance. It also allows for notice via media outlets if more than 5,000 people have been affected. An exception is made in the event of a criminal investigation.

S. 495, a sweeping bill sponsored by Committee Chairman Patrick Leahy (D-VT) and ranking member Senator Arlen Spector (R-PA), cleared the committee by voice vote and was sent to the Senate floor. The measure requires that data brokers (those firms collecting and selling personal information to third parties) let consumers know what information their database contains about them. If mistakes are discovered, the companies must fix them under the terms of the legislation. Firms and agencies which hold millions of records also must take steps to ensure the databases are protected through security programs. If security breaches occur, data brokers as well as government agencies must notify affected consumers. The bill has teeth to back up its provisions with criminal penalties, including imprisonment for up to five years for concealing data breaches and civil penalties up to $1 million for each intentional or willful violation of failure to protect records. The Federal Trade Commission would enforce the civil fine provisions. Several amendments were added to the bill before passage. A manager’s amendment by Senator Leahy, adopted by voice vote, made clarifying and definitional changes regarding encryption technology. An amendment by Senator Feinstein, approved by
voice vote, requires the Secret Service to determine the merits of an agency or business claiming that revealing details of a security breach would violate national security. Two amendments by Senator Charles Schumer (D-NY) were inserted by voice vote. One would require third parties receiving sensitive information to do so only for a valid legal purpose. Another would establish an Office of Federal Identity Protection to help consumers who are identity theft victims. Senator Benjamin Cardin (D-MD) introduced an amendment, approved by voice vote, requiring third parties to reveal the names of data brokers that supplied information if an adverse action is taken against someone. Finally, an amendment by Senator Sheldon Whitehouse (D-RI) to give bankruptcy protection to victims of identity theft was accepted by voice vote.

In addition to the above, Senator Thomas Carper (D-DE) introduced S. 1260 on May 1, another bill designed to protect consumer information and require notice of security breaches. The bill has been referred to the Committee on Banking, Housing and Urban Affairs.

On the House side, on May 3, Representative Thomas Davis (R-VA) introduced H.R. 2124, a bill which instructs the Office of Management and Budget (OMB) to establish policies, procedure and standards for federal agencies to follow in the event of a breach of sensitive personal data. It specifies that such policies must include timely notification to those individuals whose personal information may be compromised, guidance on how to provide timely notice, and guidance on whether specific actions, such as data breach analysis, credit monitoring services and identity theft insurance are necessary. The bill has been referred to the Committee on Oversight and Government Reform.

BROADBAND NETWORKS

On May 8, S. Res 191, a resolution sponsored by Senator John Rockefeller (D-WV) establishing a national goal for the universal deployment of next generation broadband networks to access the Internet by 2015, and calling upon Congress and the President to develop a strategy, enact legislation and adopt policies to accomplish this objective, was referred to the Senate Committee on Commerce, Science and Transportation.

SPYWARE

On June 6, the full House passed H.R. 964, or SPY Act, which makes it unlawful to engage in unfair or deceptive acts with respect to 1) taking unsolicited control of a computer, 2) modifying computer settings, 3) collecting personal identifying information, 4) inducing an authorized user to disclose personally identifying information, 5) inducing the unsolicited installation of computer software and 6) removing or disabling anti-spyware technology. The bill, sponsored by Representative Edolphus Towns (D-NY), also bans transmitting an information collection program to a protected computer without notice and executing an information collection program without the authorized user’s consent. The bill preempts state spyware laws. The bill also authorizes the imposition of fines ranging from $1 million to $3 million for each violation. The bill has now been referred to the Senate Commerce, Science and Transportation Committee.

On May 22, the House had also passed H.R. 1525 (the I-SPY Act), sponsored by Representative Zoe Lofgren (D-CA), which amends the federal criminal code to impose a fine and/or prison term of up to five years for intentionally accessing a protected computer without authorization, or exceeding authorized access, by causing a computer program or
code to be copied onto the protected computer and intentionally using it in furtherance of another federal offense. The bill imposes a fine and/or prison term of up to two years if the unauthorized access is for the purpose of intentionally obtaining and transmitting personal information, or for intentionally destroying the security protection of a protected computer with the intent to defraud or cause damage to the computer. H.R. 1525 authorizes $10 million for each of the years 2008 through 2011 to the Justice Department to enforce the Act. It, too, preempts state spyware laws. The bill has now been referred to the Senate Judiciary Committee.

E-VOTING

On May 16, the House Administration Committee approved, by a 6-3 vote along party lines, H.R. 811, a bill that would require all U.S. voting systems to produce or make use of verifiable paper ballots in time for the election in 2008. Sponsored by Representative Rush Holt (D-NJ) and backed by 212 other members, the bill imposes several new security obligations, such as a general ban on wireless technology in the voting machines and connecting devices used to record or tabulate ballots to the Internet. In addition, only equipment preapproved by accredited test laboratories would be eligible for use in federal elections. The bill sets aside $1 billion (more than triple the amount proposed in an earlier version of the bill) to distribute to states in the 2007 fiscal year to help them make their systems compliant. The bill would automatically consider the paper version the ballot of record except in special cases, such as if there is “clear and convincing” evidence that enough paper records have been compromised to influence the race’s outcome. The bill also requires all states to conduct random hand-counted audits of select percentages of the voter-verified paper ballots cast in a race, except when a candidate ran uncontested or racked up 80 percent or more of the vote count.

INTERNET BLOGGING

Bloggers engaged in journalistic pursuits would be granted immunity from divulging confidential sources under a bill introduced in both chambers of Congress on May 2. The Senate bill, introduced by Senator Richard Lugar (R-IN) is S. 1267; the House bill is H.R. 2102 and was introduced by Representative Rick Boucher (D-VA). While draft versions of the bill based immunity eligibility on ties to specific media institutions, the introduced version offers protection to anyone engaged in journalism, although its language does not actually require that a covered person have journalism as an occupation or on a regular basis. The bill defines journalism as “gathering, preparing, collecting, photographing, recording, writing, editing, reporting or publishing of news or information that concerns local, national or international events or other matters of public interest for dissemination to the public.” Both bills have been referred to their respective Judiciary Committees.

INTERNET GAMBLING

On May 3, Representatives Shelley Berkley (D-NV) and Jon Porter (R-NV) introduced H.R. 2140, a bill which provides for a study by the National Academy of Sciences to identify the proper U.S. response to Internet gambling. The bill has been referred to the Judiciary, Financial Services and Ways and Means Committees for consideration of the issues within each committee’s jurisdiction.

Also in the House, Representative Barney Frank (D-MA) introduced H.R. 2046, a bill that would replace the current broad ban on Internet gambling with strict regulations,
including criminal background checks and financial disclosure imposed on companies that seek to offer Internet gambling. It does, however, authorize states, Indian tribes and sporting leagues to prohibit Internet gambling activities. The bill has been referred to the Energy and Commerce and Financial Services Committees.

INTERNET RADIO

A bill introduced in both houses of Congress would nullify a controversial royalty fee increase paid by Internet radio web casters. The House bill, introduced by Representative Jay Inslee (D-WA), is H.R. 2060; the Senate bill is S. 1353 and is sponsored by Senator Ron Wyden (D-OR). The new rules, established by the U.S. Copyright Royalty Board call for rate increases of .08 cents per song per listener retroactive to 2006. Rates would also climb to .19 cents per song by 2010, amounting to a 30 percent increase per year. Each station would also have to hand over a minimum $500 royalty payment (see “News You Can Use” section for more information on the Copyright Board’s decision). In addition to repealing the increases, the House bill offers a compromise by setting the rate at 7.5 percent of the web caster’s revenue “directly related to” its transmission of sound recordings, or 33 cents per hour of sound recordings transmitted to a single listener. It would be up to the web caster to decide which model to use. The bill also calls for public radio broadcasters to submit a report to Congress on how to determine rates for their class of service. S. 1353 was referred to the Judiciary Committee; the House bill was referred to the Judiciary and Energy and Commerce Committees for each to determine the issues that fall within its jurisdiction.

TOOLS YOU CAN USE

**Combating Identity Theft**

“Combating Identity Theft: A Strategic Plan” is a report by the Bureau of Justice Assistance (BJA) that contains recommendations designed to strengthen the efforts of law enforcement, educate consumers and businesses on identity theft, help law enforcement officers apprehend and prosecute identity thieves and increase safeguards with respect to the personal data with which agencies are entrusted. The report can be downloaded at [http://www.ojp.usdoj.gov/BJA/pdf/Pres_ID_Theft_Report.pdf](http://www.ojp.usdoj.gov/BJA/pdf/Pres_ID_Theft_Report.pdf).

**Digital Data Acquisition Tool**

“Test Results for Digital Data Acquisition Tool: IXimager” documents the results of IXimager, a law-enforcement-only, evidence production tool, by test assertion. The publication also describes the testing environment, provides an interpretation of the test results and includes test results summary log files for numerous test cases. It can be accessed at [http://www.ncjrs.gov/pdffiles1/nij/217678.pdf](http://www.ncjrs.gov/pdffiles1/nij/217678.pdf).
NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

WHAT PROSECUTORS NEED TO KNOW ABOUT SPYWARE AND PHISHING

August 28-30, 2007
University, MS 38677

NOMINATION FORM - RETURN BY AUGUST 3, 2007

**PLEASE NOTE: THIS FORM IS NOT AN AUTOMATIC APPROVAL TO ATTEND THE TRAINING. APPROVAL NOTICE WILL BE SENT UNDER SEPARATE COVER**

MEETING ID NO. # 346

Please use one form per registrant/nominee. Complete all sections.

Please return form to: National Association of Attorneys General, Attn: Marland Holloway, Cyber Crime Project Assistant, 2030 M Street, N.W., 8th Floor, Washington, DC 20036 or Fax to (202) 331-1427.

<table>
<thead>
<tr>
<th>Name (as it should appear on badge):</th>
<th>Full Mailing Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title:</th>
<th>Full Mailing Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phone Number:</th>
<th>Full Mailing Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fax Number:</th>
<th>Full Mailing Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>E-mail:</th>
<th>Full Mailing Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attorney General Office:</th>
<th>Full Mailing Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Travel By (Check one): Air_____ Rail _____ Car_____</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>State Bar registration number(s)</th>
<th>State _____ Number _______</th>
</tr>
</thead>
<tbody>
<tr>
<td>(For CLE credit)</td>
<td></td>
</tr>
<tr>
<td>State Bar registration number(s)</td>
<td>State _____ Number _______</td>
</tr>
<tr>
<td>(For CLE credit)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dietary Restrictions? If so describe:</th>
<th>Full Mailing Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Special Requests</th>
<th>Full Mailing Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you require</td>
<td></td>
</tr>
<tr>
<td>special services</td>
<td></td>
</tr>
<tr>
<td>or auxiliary</td>
<td></td>
</tr>
<tr>
<td>aids to assist</td>
<td></td>
</tr>
<tr>
<td>you while</td>
<td></td>
</tr>
<tr>
<td>attending the</td>
<td></td>
</tr>
<tr>
<td>meeting and</td>
<td></td>
</tr>
<tr>
<td>events during</td>
<td></td>
</tr>
<tr>
<td>the Cyber Crime</td>
<td></td>
</tr>
<tr>
<td>Training, such</td>
<td></td>
</tr>
<tr>
<td>as sign-language</td>
<td></td>
</tr>
<tr>
<td>interpreters,</td>
<td></td>
</tr>
<tr>
<td>note-takers,</td>
<td></td>
</tr>
<tr>
<td>large print</td>
<td></td>
</tr>
<tr>
<td>materials or</td>
<td></td>
</tr>
<tr>
<td>Braille materials,please contact Marland Holloway, Cyber Crime Project Assistant, at 202-326-6262 or by email at <a href="mailto:mholloway@naag.org">mholloway@naag.org</a>. NAAG will make suitable arrangements.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(NAAG Use Only):</th>
<th>Full Mailing Address:</th>
</tr>
</thead>
<tbody>
<tr>
<td>This Nominee Has</td>
<td></td>
</tr>
<tr>
<td>Been Approved</td>
<td></td>
</tr>
<tr>
<td>To Attend This</td>
<td></td>
</tr>
<tr>
<td>Training: Yes (__) No (____)</td>
<td></td>
</tr>
</tbody>
</table>