



Issue 27

**News Highlights in This Issue:**

Two AGs Write Re Net Gambling Bill	3
Use of Pen Register Not Unconstitutional	7
AG Dann to Keynote Cybercrime Conference	3
New York Bans Domain Name Profiteering	11
Sharp Rise in Spam From China Reported	14
Search of Probationer's Hard Drive OK	8
Nebraska Cyberstalking Law Now Effective	12
Flaws in Forensic Software Outlined	15
Viewing Child Pornography Violates PA Statute	8
Supreme Court Hears Child Pornography Case	11
Florida Sex Offender Law Takes Effect	12
Must Allege Loss to Prevail in Data Breach Case	10
Illinois Restricts Access to Internet Wine Sales	12
Internet Gambling Regulations Open for Comment	16
Site Not Liable for User Age Misrepresentation	10
Internet Tax Ban Extended Seven Years	12
RIAA Sends Letter Threats to 19 Universities	18
Senator Biden Introduces Omnibus Crime Bill	19
Crossing State Lines Required in Possession Case	9
California Bans Teen Driving With Cell Phones	13
IT Security Awareness Brief Available	15

**Table of Contents**

**Features**

Phishing, Vishing and Smishing	2
AG Dann Keynotes at Conference	3
As We Go to Press: Omnibus Bill	19

**AGs Fighting Cyber Crimes**

Florida, Maryland AGs Fault HR 2046	3
AG King: Arrest in Computer Info Misuse	
Connecticut AG sues Tech Services Company	
AG McCollum Opens Expanded Predator Unit	
Hawaii AG: Guilty Verdict in Predator Case	
AG Wasden Announces Video Game Campaign	
Illinois AG: Arrest in Predator Case	
AG Morrison Creates Cyber Crime Unit	
Kentucky AG: Sting Gets Seven Predators	
AG Foti Creates 6 <sup>th</sup> Regional ICAC Force	
Michigan AG Unveils Internet Safety Program	
AG Hood: Child Pornographer Convicted	
New Jersey AG: Pornography Sweep Results	
AG King Gives Internet Safety Presentation	
New York AG Settles With Verizon Wireless	
AG Corbett: Unit Arrested Two Predators	
South Carolina AG: Predator Arrested in Sting	
AG Cooper Takes Part in Net Safety Forum	
Texas AG: Predator Gets Seven Year Sentence	
AG Shurtleff: Award for ICAC Task Force	
Virginia AG Launches Internet Safety Contest	
AG McKenna Settles With Internet Advertiser	

**In the Courts**

4 <sup>th</sup> Amendment Not Violated By Pen Register Use	7
Search of Probationer's Hard Drive Constitutional	
Viewing Child Pornography Violates PA Statute	
Possession Case Needs Interstate Commerce Proof	
Data Breach Case Dismissed: No Financial Loss	
No Liability For User's Age Misrepresentation	

**In the Supreme Court**

**Legislation Update**

New York Bans Domain Name Profiteering	11
Nebraska Cyberstalking Law Takes Effect	
Florida Sex Predator Law Becomes Effective	
Illinois Restricts Access to Wine on Internet	
Internet Tax Moratorium Extended 7 Years	
Senate Committee OKs Parental Control Bill	
Internet Safety Bill Approved by Committee	
House Passes Wireless for Minorities Bill	
California Bans Teen Drivers' Cell Phones	
Committee OKs Online Pharmacy Bill	

**News You Can Use**

Sharp Rise in Spam From China Reported	14
Coalition Launches Cybersquatting Campaign	
Facebook Users Easily Give Personal Data	
IT Awareness Brief Available	
Report Details Flaws in Forensic Software	
Parents Worry But Don't Stop Net Use	
Internet Gambling Regs Open for Comment	
User Wrong About Computer Protection	
Education is Big Teen Networking Topic	
ICANN Tests Domains in Foreign Scripts	
Committee Investigates Domain Snatching	
Online Recipe Copying Rampant	
Coalition Issues Guidelines on Site Videos	
RIAA Sends Letters to 19 Universities	
Study Profiles ID Thieves	

**Tools You Can Use**

The Cyber Crime Newsletter is developed under the Cyber Crime Training Partnership between the National Association of Attorneys General (NAAG) and the National Center for Justice and the Rule of Law (NCJRL) at the University of Mississippi School of Law. It is written and edited by Hedda Litwin, Cyber Crime Counsel ([hlitwin@naag.org](mailto:hlitwin@naag.org), 202-326-6022).

This project was supported by Grant No. 2000-DD-VX-0032 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the authors and do not represent the official position of the United States Department of Justice.

The views and opinions of authors expressed in this newsletter do not necessarily state or reflect those of the National Association of Attorneys General (NAAG). This newsletter does not provide any legal advice and is not a substitute for the procurement of such services from a legal professional. NAAG does not endorse or recommend any commercial products, processes, or services. Any use and/or copies of the publication in whole or part must include the customary bibliographic citation. NAAG retains copyright and all other intellectual property rights in the material presented in the publications.

In the interest of making this newsletter as useful a tool as possible for you, we ask that you keep us informed of your efforts. Additionally, we would like to feature articles written by you. Please contact us with information, proposed articles and comments about this newsletter. Thank you.

---

## **PHISHING, VISHING AND SMISHING**

**By Russell “Rusty” McGuire<sup>1</sup>**

I recently attended NAAG’s conference on spyware and phishing. During one of the sessions, we used our sleuth skills to take a quiz on phishing. The goal was simply to distinguish between legitimate or phishing e-mails. All my training and preparation did not help me as I failed the quiz -- which is not a bad thing. I choose to treat every e-mail, phone call, or letter requesting personal identifying information as a scam, and this is what we recommend to our consumers in our identity theft presentations. No longer are phishing e-mails covered with misspellings or other obvious indicia of fraud. Even a room full of competent attorneys was split during the quiz on what was fraud. If we can’t figure it out, how can a consumer? Then comes the vishing phone call from a person who represents themselves as your bank in an effort to relieve you of your account information. These callers are quick to point out how the Internet is not safe so they send you to a phone number. Little does the caller know that

the phone number is hosted by a computer and just as susceptible to fraud. If these two methods of the scam were not enough, here comes a text message over your handheld device trying to convince you to part with your information, and this is the smishing.

This is why we tell our consumers to simply ignore an unsolicited communication asking for your personal identifying information. It is irrelevant whether the communication comes from an e-mail, text, telephone or any other form of communication. If the consumer is really concerned about the validity of the problem in the communication, simply pick up the telephone and call their bank at a number they have used in the past.

*<sup>1</sup>Russell “Rusty” McGuire is an Assistant Attorney General in the Office of the Attorney General of Virginia.*

## **ATTORNEY GENERAL DANN TO KEYNOTE CYBERCRIME CONFERENCE**

Attorney General Marc Dann of Ohio will deliver the keynote address before prosecutors and civil enforcement attorneys from Attorneys General offices across the country at the Training Conference on Presenting Digital Evidence in the Courtroom. The conference, developed by the National Association of Attorneys General (NAAG) in cooperation with the National Center for Justice and the Rule of Law (NCJRL) at the University of Mississippi, will take place on November 13-15 at the University of Mississippi School of Law. In addition to members of the Office of Attorneys General, law school faculty and students

are expected to attend Attorney General Dann's speech.

The training itself will cover an entire trial involving digital evidence, starting with considerations in pre-trial motions and ending with closing arguments. Presenters from Attorney General Offices include Carlos Diaz, Maine; Lee Lerussi and Scott Longo, Ohio; and Les Lauziere and Rusty McGuire, Virginia. There will also be a session on the pros and cons of trial software packages, including Verdict Systems and TrialDirector. Attendees from Attorneys General Offices will receive CLE credit and will have their transportation costs reimbursed.

# **AGs FIGHTING CYBER CRIMES**

---

## **MULTI-STATE**

**Attorneys General Bill McCollum of Florida and Douglas Gansler of Maryland** sent a letter to U.S. Representatives Barney Frank (D-MA) and Spencer Bacchus (R-AL), chairman and ranking member, respectively, of the House Committee on Financial Services, expressing grave concerns about H.R. 2046, the Internet Gambling Regulation and Enforcement Act of 2007. Essentially H.R. 2046 would replace state regulations on Internet gambling with a federal licensing system that would permit Internet gambling companies to do business with U.S. companies – a result both Attorneys General McCollum and Gansler believe would undermine states' traditional powers to make and enforce their own gambling laws.

## **ALABAMA**

**Attorney General Troy King** announced the arrest of James Dingler, a former state conservation officer, on charges of misusing confidential information, Attorney General King's Office had presented evidence to a grand jury resulting in a 12-count indictment against Dingler. Specifically, the indictment charges Dingler with: four counts of unauthorized use of a computer to obtain criminal records through the Law Enforcement Tactical System (LETS), a class A misdemeanor punishable by up to 12 months imprisonment and a fine of up to \$6,000; seven counts of obtaining criminal record information from LETS under false pretenses and one count of communicating criminal record information from LETS under false pretenses, both class C felonies punishable by up to five years imprisonment and a fine between \$5,000 and \$10,000. The case was

prosecuted by Assistant Attorney General Stephanie Billingslea of Attorney General King's Public Corruption and White Collar Crime Division.

## CONNECTICUT

**Attorney General Richard Blumenthal** sued Accenture, a New York-based technology services and consulting company, over the loss of confidential information for 58 state taxpayers and hundreds of state bank accounts. The suit accuses the firm of converting state property for its own use, violating its contract with the state and being negligent in allowing the data to be placed on a state of Ohio backup computer tape that was later stolen. Accenture had been hired by the state in 2002 to help the state automate resources and financial information. The lawsuit seeks damages and reimbursement for state funds expended on protecting the information. It also calls on Accenture to return some of the money already paid to it by the state.

## FLORIDA

**Attorney General Bill McCollum** hosted the grand opening of the expanded Child Predator CyberCrime Unit in Jacksonville which will serve as the headquarters of statewide operations. Openings in six more geographical areas are planned. The expansion will allow Attorney General McCollum's investigative team and prosecutors to work more closely with local law enforcement agencies. The unit will offer training, support local operations and provide assistance in areas with few resources.

## HAWAII

**Attorney General Mark Bennett** announced that Earnest Roberts was found guilty by a jury of electronic enticement of a child in the first degree. The verdict resulted from an investigation that involved the Hawaii Internet Crimes Against Children Task Force (HICACTF), including Attorney General Bennett's Office and the Honolulu Police Department. The case was prosecuted by Deputy Attorney General Albert

Cook. Roberts faces a maximum sentence of 10 years in prison and, under a new sentencing law, a minimum sentence of five years probation with a one-year prison term as a condition of probation. He must also register as a sex offender.

## IDAHO

**Attorney General Lawrence Wasden** joined Entertainment Software Rating Board (ESRB) President Patricia Vance to unveil a statewide Public Service Announcement (PSA) campaign to explain video game ratings to parents. The PSAs, produced and distributed by ESRB, will air on TV and radio stations throughout the state through Christmas. ESRB also prepared a brochure that provides detailed information to parents. Both the brochure and PSAs can be viewed on Attorney General Wasden's web site.

## ILLINOIS

**Attorney General Lisa Madigan** announced that the Winfield Police Department, working with her Internet Crimes Against Children (ICAC) Task Force, arrested Timothy Davis as he attempted to meet a person he met on the Internet that he believed to be a child. The "child" was an undercover police detective that Davis solicited for sex. Davis was charged with one count of indecent solicitation of a child and one count of attempted aggravated criminal sexual abuse, both class 3 felonies punishable by a maximum of five years in prison. Following the arrest, a search warrant was executed for Davis' computers, and three computers and related media were seized. Attorney General Madigan's High Tech Crimes Bureau will conduct a forensic search of the computers.

## KANSAS

**Attorney General Paul Morrison** announced the creation of a Cyber Crime Unit within his office and outlined plans for an expanded Cyber Crime Initiative to provide tools and resources to fight Internet crime. The new unit will begin with one assistant attorney general and one investigator funded with existing resources,

although Attorney General Morrison urged the legislature to adopt his initiative during the 2008 session. Following successful models used across the nation, the new unit will focus on education and investigation and prosecution of crimes in which a computer was used.

### **KENTUCKY**

**Attorney General Greg Stumbo** announced the arrests of seven sexual predators, including a former Indiana law enforcement employee, who were caught in a child sexual predator sting. Arrested were Michael Patterson of Indiana; John Elliot of Kentucky; and Lorne Armstrong, James Fowler, Richard Watwood and Dustin McPhetridge, all of Tennessee. The predators were met by Kentucky law enforcement, host Chris Hansen of NBC's "To Catch a Predator" and Perverted Justice volunteers as they arrived at the sting location. Each predator was charged with attempted unlawful transaction with a minor under age 16, a class C felony. If convicted, each man faces five to 10 years in prison. Attorney General Stumbo's Kentucky Bureau of Investigation and Office of Consumer Protection coordinated the sting operation.

### **LOUISIANA**

**Attorney General Charles Foti, Jr.** announced the formation of the Capital Area Internet Crimes Against Children (ICAC) Task Force, part of the Louisiana ICAC Task Force led by Attorney General Foti's Office. This is the sixth such regional task force, with others located throughout the state.

### **MICHIGAN**

**Attorney General Mike Cox** unveiled the Michigan Cyber Safety Initiative (CSI), a comprehensive Internet predator education program for school children. The program is being offered to all public and private state schools, as well as the home school community. Attorney General Cox's office is also partnering with the Michigan Cable Telecommunications Association and the Michigan

Association of Broadcasters to promote CSI. Michigan CSI consists of four age-appropriate seminars, including a community seminar. A portion of the program also deals with cyberbullying. Material from the CSI presentations can be found on Attorney General Cox's web site.

### **MISSISSIPPI**

**Attorney General Jim Hood** announced the conviction of Shannon Gilbert on one count of transmission of child pornography via the Internet and four counts of possession of child pornography. Investigation, prosecution and forensic analysis of the case were all done by Attorney General Hood's Cyber Crime Unit based on a cyber tip. Gilbert was sentenced to five years in prison, with three years suspended, and five years probation on each count, to run concurrently. Gilbert will have to register as a sex offender, undergo psychological counseling and his Internet usage will be monitored by either Attorney General Hood's Office or the Department of Corrections.

### **NEW JERSEY**

**Attorney General Anne Milgram** announced the results of her initiative, Operation Silent Shield, a sweeping investigation of child pornography that resulted in 41 arrests. Led by the New Jersey State Police (NJSP) Digital Technology Investigations Unit (DTIU), the investigation encompassed 15 counties and numerous law enforcement agencies, targeting predators who distributed known images and videos of child pornography via the Internet.

### **NEW MEXICO**

**Attorney General Gary King** visited a middle school in Albuquerque to give an Internet safety presentation, "Protect Yourself Online." The presentation was aimed at teaching eighth graders how to protect themselves from online predators.

## NEW YORK

**Attorney General Andrew Cuomo** announced that Verizon Wireless agreed to stop the deceptive marketing of its Internet usage plans and reimburse \$1 million to customers for wrongful account termination worldwide. The settlement follows a nine-month investigation by Attorney General Cuomo into the marketing of *NationalAccess* and *BroadbandAccess* plans for wireless access to the Internet for laptop computers. While the company marketed these plans as “unlimited,” they did not disclose that common usages such as downloading movies and playing games were not allowed. The company also cut off heavy Internet users for exceeding an undisclosed cap of usage per month, resulting in customers being abruptly terminated without Internet access and unable to obtain refunds. The company has agreed to reimburse all terminated customers for the cost of wireless access cards or cell phones purchased in order to use Verizon Wireless’s wireless Internet service, estimated at \$1 million nationwide. It will also pay penalties and costs of \$150,000 to New York state and revise the marketing of its plans. The case was handled by Justin Brookman, chief of Attorney General Cuomo’s Internet Bureau, with assistance from Investigator Vanessa Ip.

## PENNSYLVANIA

**Attorney General Tom Corbett’s** Child Predator Unit agents arrested David Frew and Clifford Hayes, both of New Jersey, who are accused of using Internet chat rooms to send sexually explicit photos and videos to what they believed were young girls. The “girls” were actually undercover Unit investigators who were using online profiles of children. Both men were taken into custody at their homes, and agents also executed a search of each residence, seizing two computers and a webcam from each home that will be analyzed by Attorney General Corbett’s Computer Forensics Unit. Frew is charged with three counts, and Hayes with two counts, of unlawful contact with a minor and both men are also charged with one count of criminal use of a

computer. All of the charges are third degree felonies, each punishable by up to seven years in prison and a \$15,000 fine. Both men will be prosecuted by Deputy Attorney General Michael Sprow of Attorney General Corbett’s Child Predator Unit.

## SOUTH CAROLINA

**Attorney General Henry McMaster** announced that Jeffery Miller was arrested in an undercover Internet sting conducted by the city of Charleston Police Department, a member of Attorney General McMaster’s Internet Crimes Against Children (ICAC) Task Force. According to the arrest warrant, Miller approached an adult woman online and later sought to have sex with her 13-year-old daughter. In reality, he was communicating with an undercover police officer. Miller was arrested on one count of criminal solicitation of a minor, a felony offense punishable by up to 10 years in prison. He will be prosecuted by Attorney General McMaster’s Office.

## TENNESSEE

**Attorney General Bob Cooper** joined several other state and local officials at a Child Internet Safety Forum at the Nashville Public Library. Attorney General Cooper also joined Tennessee Division of Consumer Affairs Director Mary Clement in offering additional information to keep youth safe online. The Forum is the latest in a series of events in which Attorney General Cooper and Director Clement have participated to commemorate the 30<sup>th</sup> anniversary of the state Consumer Protection Act.

## TEXAS

**Attorney General Greg Abbott** announced that Guadalupe DeLaGarza, a sex predator who used MySpace.com to sexually solicit someone he believed to be a 14-year-old girl, received a seven-year prison sentence. Attorney General Abbott’s Cyber Crimes Unit investigated and prosecuted DeLaGarza for using the Internet to prey on children. DeLaGarza was arrested when he arrived

at the proposed meeting place to meet and sexually assault the teen he met online who was actually an undercover Unit investigator. DeLaGarza pled guilty to attempted sexual performance with a child, a third degree felony. Upon release, he will be required to register as a sex offender for 10 years.

## UTAH

### **Attorney General Mark Shurtleff**

announced that the Utah Internet Crimes Against Children (ICAC) Task Force, which is overseen by his Office, received the “Child Defender” Award from the non-profit National Law Center for Children and Families. The award recognizes the Task Force for having the highest rate of Internet predator arrests per capita in the nation. The Task Force had 51 arrests in 2005, 72 arrests in 2006 and 46 arrests by end of July 2007.

## VIRGINIA

### **Attorney General Bob McDonnell**

launched a Youth Internet Safety Contest for students in grades six through 12. Under the contest rules, students will have six months to write, direct and produce their own 30-second television ads on Internet safety. The winning entrant will have his or her ad aired on state television next year, get a private screening of a new Fox movie with 70 of his or her friends and receive an X-Box 360 and a basket of Fox DVDs. Second and third place winners will each receive a basket of Fox DVDs. The submission deadline for the contest is February

1, 2008. Entries will be narrowed down by Attorney General McDonnell’s Office, and the winner will be chosen by an online vote. Posters advertising the contest have been placed in schools throughout the state in conjunction with the state Department of Education, and print ads will appear in publications in the state in the upcoming weeks.

## WASHINGTON

**Attorney General Rob McKenna** entered into a settlement with HoanVinh Nguyenphuoc, one of three California-based Internet affiliate advertisers accused of violating the state’s consumer protection and spyware laws. Nguyenphuoc, owner of FixWinReg, sent anonymous “Net Send” e-mail messages to consumers that simulated security warnings but were actually ads for registry-cleaner software. According to court documents, those messages told users that their computers contained registry errors requiring immediate attention and directed them to a web site where they were asked to download a free trial of the software. Attorney General McKenna’s Consumer Protection Unit sued Nguyenphuoc, with Assistant Attorney General Katherine Tassi leading the investigation. Under the settlement, Nguyenphuoc will pay \$25,000 in attorney’s fees and costs, in addition to \$75,000 in civil penalties if he fails to comply with the settlement. The settlement prohibits him from using “Net Send” messages to promote products or services or make other representations.

# IN THE COURTS

---

## **FOURTH AMENDMENT: PEN REGISTER**

*U.S. v Forrester*, 2007 WL 2120271 (9<sup>th</sup> Cir. July 6, 2007). The Ninth Circuit Court of Appeals determined that the use of a pen register to monitor defendants’ Internet and e-mail activity did not

violate the Fourth Amendment. The Drug Enforcement Agency (DEA), believing that Mark Forrester and Dennis Alba were manufacturing ecstasy, obtained court permission to install a pen register wiretap on Alba’s computer so they could monitor the defendants’ Internet and e-mail activity.

The pen register only recorded IP addresses of visited web sites and the To/From addresses of e-mails. However, since defendants were using encrypted e-mail services, the DEA could not obtain the information they wanted. The DEA then persuaded a judge to allow a DEA agent to enter the defendants' office and install key-logging software, allowing the DEA to monitor all activity on the defendants' computers. Both men were charged with offenses related to the operation of an ecstasy-manufacturing laboratory and were convicted by a jury. Surprisingly, at trial, the defendants did not move to suppress any evidence obtained as a result of the key-logger and instead disputed the validity of the pen register. On appeal, the Ninth Circuit found that the use of the pen register did not violate the Fourth Amendment because defendants had no reasonable expectation that the IP addresses and To/From lines of e-mails would remain private since such activity is transmitted through a third party.

**FOURTH AMENDMENT: SEARCH  
OF PROBATIONER'S HARD  
DRIVE**

*United States v. Herndon*, 2007 WL 2457452 (6<sup>th</sup> Cir. August 31, 2007). The Sixth Circuit Court of Appeals found that a probation officer who was monitoring compliance with a probation condition limiting Internet access acted reasonably under the Fourth Amendment when he searched a hard drive in the probationer's home and found child pornography. Jeffrey Herndon was on probation for sexual exploitation of a minor. One of his probation conditions was a ban on using the Internet without his probation officer's permission. His probation officer subsequently learned that Herndon was using the Internet

without permission, and went to Herndon's home, finding a laptop under Herndon's pillow. A pre-search scan revealed pornographic images, but was inconclusive as to whether the images were children. The probation officer then found an unconnected external hard drive in Herndon's bedroom, connected it to the laptop and found and seized more than 3,000 images and several hundred videos of child pornography. Herndon was charged with knowing receipt and possession of child pornography. He moved to suppress the evidence on the grounds that it was secured in violation of his Fourth Amendment rights. The U.S. District Court for the Middle District of Tennessee denied the motion as to the pornographic images and videos. On appeal, Herndon argued that the probation search condition that allowed the probation officer to search his computer did not extend to unconnected peripheral hardware. The Sixth Circuit disagreed, ruling that Herndon's computer and the external hard drive could not function independently of one another, and thus Herndon had a substantially reduced expectation of privacy in the hard drive.

**VIEWING CHILD  
PORNOGRAPHY: POSSESSION  
STATUTE**

*Commonwealth v. Diadoro*, 2007 WL 2390713 (Pa. Super. August 23, 2007). An en banc nine-member panel of the Pennsylvania Superior Court, by a vote of 7-2, reversed a three-judge panel and found that a person who views child pornography on their computer has violated the state's criminal ban on "possession" or "control" of such material, even if he never downloaded it, printed it out or sent it to another person. Anthony Diadoro surfed on the Internet

and found pictures of child pornography which he only viewed. Acting on a tip regarding an unrelated incident, police subpoenaed Diadoro's computer and, upon expert examination, numerous images of adolescent sexual activity were found in the cache files, which are temporary files that are automatically downloaded when one views an image online. More than 30 of those images were found to violate the state's criminal prohibition on possession and control of child pornography. Diadoro was convicted and appealed, arguing that he had not actually possessed or controlled the images but merely viewed them. He stated he was not aware that his computer was automatically creating cache files, which he never accessed. A three-judge panel of the Superior Court agreed and reversed his conviction by a vote of 2-1. The state petitioned for en banc review that was granted. The majority reversed, finding that regardless of whether Diadoro knew the workings of his computer, the result of his sessions was that copies of the images he viewed were available in temporary storage, if he knew how to access them. Therefore, in a literal sense, he possessed them. The court noted that Diadoro could have downloaded the images, printed them and e-mailed them and thus was capable of exercising control over them.

*Ed. Note: The original decision by the three-judge panel was reported in the November-December 2006 issue of this newsletter.*

### **POSSESSION OF CHILD PORNOGRAPHY: INTERSTATE COMMERCE**

*U.S. v. Schaefer*, No. 06-3080 (10<sup>th</sup> Cir. September 5, 2007). The Tenth Circuit Court of Appeals reversed a conviction for receipt and possession of child pornography because the government failed to satisfy the federal jurisdictional requirement that the pornographic images had traveled across state lines. Acting on a tip that William Schaefer had used his computer and credit cards to subscribe to a web site containing child pornography, federal agents executed a search warrant on his home and seized a laptop, CDs and several documents. Forensic analysis of the computer showed that Schaefer had purchased at least five subscriptions to child pornography web sites and there was pornography in temporary storage as well as on the CDs. Schaefer was charged with one count of receiving child pornography and one count of possession of child pornography. The district court found Schaefer guilty on both counts, although there was no evidence presented as to where Schaefer got the images, where the web sites Schaefer allegedly accessed were located or whether Schaefer had exercised control over the images. Schaefer appealed, seeking a reversal and acquittal, arguing that the government failed to show any evidence that any image he possessed traveled across state lines, as required by 18 U.S.C. §§ 2252(a)(2) and (a)(4)(b). The Tenth Circuit agreed, finding that it is insufficient to assume that an Internet communication, standing alone, necessarily traveled across state lines.

*Ed. Note: This decision causes a split with the Third and Fifth Circuits. As reported in the May-June 2006 issues of*

*this newsletter, in U.S. v. MacEwan, 445 F.3d 237 (2006), the Third Circuit held that given the interstate character of the Internet, a connection to a web site or server must involve data moving in interstate commerce. In U.S. v Runyan, 290 F.3d 223 (2002), the Fifth Circuit assumes that use of the Internet may be equated with a movement in interstate commerce in child pornography cases.*

### **DATA BREACH: CIVIL LIABILITY**

*Pisciotta v. Old National Bancorp., 2007 WL 2389770 (7<sup>th</sup> Cir. August 23, 2007).* The 7<sup>th</sup> Circuit Court of Appeals affirmed a district court's dismissal of a class action suit against a financial services company that suffered a computer hacking data breach because no completed direct financial loss was alleged. Old National Bancorp (ONB), a financial services company based in Indiana, used NCR, an information technology company, to maintain its web site. When NCR reported a malicious security breach, ONB customers, Luciano Pisciotta, Daniel Mills and others, filed a class action complaint in U.S. District Court for the Southern District of Indiana against ONB and NCR alleging state law claims of negligence and breach of implied contract as to their failure to protect personal information from security breaches. They did not allege any direct financial loss as a result of the breach, nor did they claim any class member was a victim of identity theft, but they requested damages for the cost of the credit monitoring they incurred as well as for emotional distress. Jurisdiction was based on the Class Action Fairness Act (CAFA) of 2005. The district court dismissed the complaint for failure to state a claim upon which relief can be

granted. On appeal, the 7<sup>th</sup> Circuit found no compensable injury and affirmed the dismissal.

### **WEB SITE LIABILITY: MISREPRESENTATION OF AGE**

*Doe v. SexSearch.com, 2007 WL 2388913 (N.D. Ohio August 22, 1007).* The U.S. District Court for the Northern District of Ohio broadly construed 47 U.S.C. 230 to absolve a web site of liability for a user's misrepresentation of her age. "Jane Roe" posted a profile on SexSearch.com, a web site that helps people hook up to have sex, saying that she was 18 years old and wanted sex. "John Doe" contacted "Roe" through the profile and they met offline and had sex. In reality, "Roe" was only 14 years old, and "Doe" was charged with felony statutory rape. "Doe" sued SexSearch.com for breach of contract, fraud and breach of warranty. SexSearch filed a 12(b)(6) motion to dismiss, asserting immunity under the Communications Decency Act at 47 U.S.C. § 230, which provides that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." "Doe" argued that SexSearch, not "Roe," was the author of the profile because its site stated that it "reserved the right to modify the content of profiles when they did not meet the profile guidelines" and thus SexSearch was responsible in whole or part for the creation or development of the information. The court rejected this argument because the complaint did not allege that SexSearch had modified the content. It granted the motion to dismiss.

# IN THE SUPREME COURT

---

In this issue, we'll discuss the case of *U.S. v Williams*, as the Supreme Court will once again ponder attempts by Congress to prohibit child pornography. This time, it's a provision of the Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today ("PROTECT") Act, which bans the pandering of "any material or purported material" in a way that "reflects the belief" or "is intended to cause another to believe" that the material is child pornography. The Court will have to decide if the Act is overly broad and thus unconstitutional on its face in violation of the First Amendment. Oral argument in the case is scheduled for October 30.

The facts of the case began with an undercover operation by the Secret Service aimed at combating online child exploitation. As part of that operation, Agent Timothy Devine engaged Michael Williams in a private Internet chat, during which Williams sent Devine a computer hyperlink with "good pics of her and me" referring to Williams' young daughter. Agents subsequently obtained and executed a search warrant at Williams' home, which resulted in a finding of child pornography on Williams' computer hard drives.

Williams was charged and convicted on one count of pandering material causing belief that it is child pornography under the PROTECT Act and one count of possession of child pornography. Williams filed a motion to dismiss the pandering charge on the grounds that the provision in the PROTECT Act was unconstitutionally overbroad and vague. While the motion was pending, a plea agreement was reached whereby Williams would plead guilty to both counts but reserve his right to appeal the pandering charge. He was sentenced to 60 months in prison for each charge to be served concurrently.

On appeal, the 11<sup>th</sup> Circuit found that the pandering provision abridges the freedom to engage in a substantial amount of lawful speech and was thus constitutionally overbroad. It also found that the provision failed to outline its restrictions with sufficient clarity to enable compliance. Williams' sentence on the pandering count was reversed. The court's ruling also rendered that provision of the PROTECT Act unenforceable in the 11<sup>th</sup> Circuit, which covers Florida, Georgia and Alabama.

## LEGISLATION UPDATE

---

### **Domain Name Profiteering**

New York Governor Eliot Spitzer signed S03814B into law, a measure aimed at preventing a person

from registering a domain name that is similar to, or the same as, another living person or business with the specific intent to profit from selling the domain name. Under the new law, a person or

entity will be liable for a violation if they are the domain name registrant or the registrant's authorized licensee. The law provides for a civil penalty of up to \$1,000 for each day the violation occurs. In addition, the New York Attorney General is empowered to apply to the state Supreme Court for an injunction, including forfeiture or cancellation of the domain name. The law, now Chapter 449, will take effect on December 1, 2007.

### **Internet Crimes Against Children**

Nebraska's new cyberstalking law, which was part of Attorney General Jon Bruning's legislative package, went into effect on September 1, 2007. Under the new law, adults over age 18 who knowingly send sexually explicit language and material to victims under the age of 16 can be charged with a class IV felony, punishable by up to five years in prison and a \$10,000 fine. Previously, the charge was only as a class I misdemeanor, punishable by up to one year in jail and a \$1,000 fine.

Florida's new sex predator law, vigorously supported by Attorney General Bill McCollum, became effective on October 1. The new law triples maximum sentences to 15 years for soliciting minors for sex and possessing child pornography. Previously, prosecutors could only seek sentences of up to five years for attempting to meet a child for sex or possessing more than 10 child pornography images. The law also increases penalties for "grooming" and for particularly heinous pornography with victims under five years old, now punishable by up to 30 years in prison. The law also reclassifies possession of child pornography as a second-degree

felony, while promotion and distribution of it becomes a first-degree felony. Additionally, the law requires offenders to register their e-mail and instant message handles with authorities.

### **Internet Wine Sales**

On October 3, Illinois Governor Rod Blagojevich signed into law HB 429, a bill that would restrict access to order wine over the Internet. It allows both in and out of state wineries to ship up to 12 cases of wine per year directly to a consumer. Wineries must obtain a winery shipper's permit from state regulators. The law brings Illinois into compliance with the U.S. Supreme Court ruling in *Granholm v. Heald*.

### **Internet Access Taxes**

The controversy in Congress centering around the effort to extend the moratorium on state Internet access taxes ended one day before the moratorium was set to expire on November 1 as a seven-year extension of the moratorium was signed into law. The House had passed a four-year moratorium, but action in the Senate had stalled in a dispute over whether the ban should be permanent or temporary. S. 1453, a bill sponsored by Senator Thomas Carper (d-DE) would have extended the moratorium for four years until November 1, 2011. S. 2128, a bill sponsored by Senator John Sununu (R-NH) would have made the ban permanent. The Senate finally approve approved a moratorium extension of seven years and the House agreed to the Senate version. The bill includes a "grandfather" clause that will allow states with Internet tax laws enacted prior to the original ban to continue enforcing such laws.

## **Internet Safety**

The Senate Commerce, Science and Transportation Committee approved S. 602 by voice vote, a bill that would require the Federal Communications Commission (FCC) to explore advanced technology to give parents more flexibility in controlling what their children view on the Internet and on television. The bill, introduced by Senator Mark Pryor (D-AR), specifically requires the FCC to explore filtering technology that could be used across media platforms. It requires a report from the FCC within one year of enactment on their findings.

On September 27, the Senate Committee on Commerce, Science and transportation favorably reported S. 1965, a bill that would direct the Federal Trade Commission to carry out a nationwide campaign to increase awareness and provide education on the safe use of the Internet. The bill, introduced by Senator Ted Stevens (R-AK) would also require schools to educate minors about Internet safety, increase fines on Internet service providers who fail to report violations of child pornography laws and require reporting of online child pornography to foreign law enforcement agencies.

## **Wireless Networks**

On September 4, the House passed HR 694, a bill sponsored by Representative Edolphus Towns (D-NY) that would assist minority-serving educational institutions in acquiring and

using digital and wireless technologies. The bill has been sent to the Senate where it has been referred to the Committee on Science, Commerce and Transportation.

## **Ban on Electronic Devices While Driving**

On September 13, California Governor Arnold Schwarzenegger signed SB 33 into law, a bill barring the use of cell phones and other electronic devices by drivers under age 18. Violators will be fined \$20 for the first offense and \$50 for subsequent offenses. The law includes an exception for emergency calls. By this enactment, California joins 15 other states and the District of Columbia in banning the use of wireless communication devices for teenage drivers. The new law will take effect on July 1, 2008.

## **Online Pharmacies**

On September 27, the Senate Committee on the Judiciary favorably reported out S. 980, a bill sponsored by Senator Dianne Feinstein that would prohibit an online pharmacy from selling a controlled substance without a valid prescription. The bill would also impose penalties on the unlawful delivery, distribution or dispensing of controlled substances over the Internet. It would authorize a state Attorney General to apply for injunctions or obtain damages and other civil remedies against an online pharmacy that poses a threat to state residents.

# NEWS YOU CAN USE

---

## **REPORT: RISE IN SPAM FROM CHINA**

A sharp spike in spam messages containing URLs that use “.cn,” the top-level domain (TLD) for China, has been noted in a report from security firm Symantec. According to the firm, one reason for the growing popularity of Chinese domains is the ban on TLDs from other countries on spam blacklists, so spammers have to register new TLDs from countries not yet on the blacklists. Another reason is that spam is becoming increasingly localized for specific target markets. Symantec also noted a decline in spam using Hong Kong (“.hk”) TLDs, which could have resulted from the recent enactment of anti-spam laws there. Also declining is image spam, although it is being replaced by attachments in other forms, such as greeting card spam. According to the report, other forms of spam increasing are PDF spam, Excel and ZIP-file spam, although spam numbers for the latter two remain low.

## **COALITION LAUNCHES ANTI-CYBERSQUATTING CAMPAIGN**

The Coalition Against Domain Name Abuse (CADNA), a new non-profit organization with members including Yahoo!, AIG, Dell, Eli Lilly, Hilton, HSBC, Marriott, Verizon and Wyndom, launched a national campaign against the fraudulent abuse of domain name registration that is at the core of cybersquatting. CADNA notes that the number of cybersquatting disputes filed with the World Intellectual Property

Organization has increased by 25 percent from 2005 to 2006, with cybersquatting itself having increased 248 percent in the past year. According to CADNA, sophisticated cybersquatters are exploiting a supposed flaw in the domain registration process in that domain names can be registered and later dropped risk-free within a five-day grace period. This grace period allows cybersquatters to “taste” and “kite” the domain names so that they can test their profitability. CADNA reports that more than one million kited sites are re-registered daily, which CADNA claims is costing brand owners more than \$1 billion annually as the result of diverted sales, loss of goodwill and expenses incurred in fighting fraud.

## **REPORT: FACEBOOK USERS FREELY GIVE INFORMATION**

According to a report by Sophos, an information technology security and control firm, 41 percent of Facebook users willingly divulge personal information, such as e-mail addresses, birth dates and phone numbers, to strangers. In its study, Sophos created a Facebook profile under the name “Freddi Staur,” an anagram for “ID Fraudster.” They used an image of a shiny, happy frog statue as a profile picture, and then sent out 200 friend requests. Out of that small sample, 72 percent who responded divulged an e-mail address; 84 percent listed their full date of birth; 78 percent listed their current address; 26 percent provided their instant messaging screen name and 23 percent listed their phone numbers. In total, of the 200 Facebook users

contacted, 87 responded to “Freddi,” with 82 divulging personal information.

### **BRIEF ON IT SECURITY AWARENESS RELEASED**

The National Association of State Chief Information Officers (NASCIO) released “IT Security Awareness and Training: Changing the Culture of State Government,” a research brief that highlights how IT security awareness and training activities, if conducted consistently, can instill culture change in state government. It also discusses the role of the chief information officer (CIO) in these activities, including partnering with other state government officials to achieve a change. Finally, the brief discusses a broader role that CIOs can pursue by expanding the scope of awareness efforts to include private state citizens. A copy of the brief may be accessed at: <http://www.nascio.org/publications/>.

### **REPORT DETAILS FLAWS IN FORENSIC SOFTWARE**

Researchers at Isec Partners, Inc., a California-based security company, released a detailed paper that examines vulnerabilities found in forensic software such as EnCase and The Sleuth Kit. Encase, in particular, is used by law enforcement to search a suspect’s hard drive for evidence without damaging or altering files. The Isec researchers focused on ways a hacker could use “crashers,” such as damaged data files, storage volumes or file systems, to cause forensic software to crash before the forensic analyst can interpret the data. The 31-page report details the techniques used to test the forensic software and sets forth recommendations

for the software manufacturers as to how they can address these vulnerabilities. The report can be accessed at: [http://www.isecpartners.com/files/iSEC-Breaking\\_Forensics\\_Software-Paper.v1.\\_1.BH2007.pdf](http://www.isecpartners.com/files/iSEC-Breaking_Forensics_Software-Paper.v1._1.BH2007.pdf).

### **PARENTS WORRY BUT DON’T STOP KIDS’ INTERNET USE**

According to a survey by market researcher Harris Interactive, 71 percent of parents of children aged six through 18 years of age admitted their child had encountered at least one “issue” with the Internet, such as bad language, sex or advertising, within the past year. However, they are not stopping their kids’ Internet use. The survey of 411 parents also reported that four out of five parents said the Internet helped their children in school, and only 31 percent of parents said their children spent too much time online. Rather than banning or restricting Internet access, parents were found to be taking an active role in monitoring their children, with 93 percent engaging in some type of monitoring activity. The survey also found that 74 percent of parents visited web sites with their children; 56 percent used a filter or blocking software; and 55 percent would visit a web site before their child. Additionally, 85 percent of parents have talked to their children about online safety. The survey was commissioned by Common Sense Media, an organization dedicated to improving the media for children and families, and Cable in the Classroom, the national education foundation of the U.S. cable industry.

## **NET GAMBLING REGULATIONS OPEN FOR COMMENT**

The U.S. Treasury Department and the Federal Reserve Board proposed Internet gambling regulations designed to put into effect a law passed by Congress last year to stop most forms of Internet gambling. The regulations would make U.S. banks responsible for blocking credit and debit card payments for online gambling. They also would bar bank customers, such as online casinos, from receiving Internet gambling proceeds. A December 12 deadline has been set for public comments on the proposal. The proposed rule can be accessed at <http://www.treas.gov/press/releases/reports/noticeofproposedrule.pdf>.

## **POLL: USERS WRONG ABOUT HAVING COMPUTER SECURITY**

Most Americans believe their computers are protected against viruses and spyware, but scans found many had outdated or disabled security software, according to a survey by McAfee, a security software maker, and the National Cyber Security Alliance. While 87 percent of those surveyed said they had anti-virus software, only one-half had updated the software in the past month. Although 73 percent said they had a firewall, nine percent had not enabled it, and although 70 percent said they had anti-spyware software, 15 percent had not enabled it. The survey also found that nine percent of the 378 people surveyed reported having had their identity stolen.

## **STUDY: BIG TEEN NETWORKING TOPIC IS EDUCATION**

A study by the National School Boards Association and Grunwald Associates found that 96 percent of U.S. teens and tweens with Internet access use networking technologies, such as chat rooms, text messaging, blogging and visiting social networking sites. The study also found that nearly 60 percent of those online students report discussing education-related topics, such as college planning and careers. Additionally, 50 percent report talking specifically about schoolwork. The report, titled "Creating and Connecting: Research and Guidelines on Online Social and Educational Networking," is based on three surveys: 1) an online survey of nearly 1,300 nine to 17-year-olds, 2) an online survey of more than 1,000 parents, and 3) telephone interviews with more than 300 school district leaders who make decisions on Internet policy. It was carried out with support from Microsoft, News Corporation and Verizon. It can be accessed at: <http://files.nsba.org/creatingandconnecting.pdf>.

## **TESTING SET FOR DOMAINS IN FOREIGN SCRIPTS**

The Internet Corporation for Assigned Names and Numbers (ICANN), the non-profit group contracted to run the Internet by the U.S., is conducting tests to see whether domains written entirely in foreign scripts can work without crashing the Internet. Currently, ICANN allows domains that are half in foreign characters, such as [foreign text].com; however, with this hybrid model,

speakers of Hebrew, Arabic and any other language written from right to left must type half of the URL in one direction and the postscript, such as .com, in the opposite direction. ICANN's experiments use the domain name "example.test" translated into 11 languages.

And more ICANN news...

### **ICANN COMMITTEE PROBES DOMAIN NAME SNATCHING**

The Security and Stability Advisory Committee of ICANN is investigating suspicions that insider information is being used to "snatch" desired domain names before an individual or business can register them. The committee termed the practice "domain name front running," and the committee is looking into suspicions that someone with access to search requests has been using the information to gauge interest in a domain name. By buying the domain first, that person can then try to sell it to the interested party for a profit. The committee cited several ways front running may be occurring, including the installation of viruses and other software programmed to collect such information and the use of unscrupulous third party sites to check domain name availability.

### **STUDY FINDS ONLINE RECIPE COPYING RAMPANT**

Concerns for recipe publishers were raised as a result of a study by Attributor, a content tracking company, of how frequently online recipes are copied and reposted to other sites. Attributor collected all of the original recipes on Epicurious.com, Allrecipes.com and RachaelRay.com,

then checked those recipes against recipes elsewhere on the Internet. Attributor looked for instances of a "match," which they defined as any two recipes in which at least 50 percent of the content was identical. The company found more than 10,000 copies of recipes that originated on the three sites, but in more than 60 percent of the cases, the reposted recipes weren't attributed to their original sources. Attributor also conducted searches for titles of some of the reposted recipes as part of the study. In many cases, the infringing copies of recipes appeared higher in search results than the original versions. As a result, Attributor estimates that Allrecipes.com is losing more than 800,000 site visits each month, and Epicurious.com is losing 400,000 monthly visits.

### **COMPANIES ISSUE GUIDELINES ON COPYRIGHTED VIDEO**

A coalition of media and Internet companies issued a set of guidelines for handling copyright-protected videos on user-generated web sites, such as MySpace.com. The coalition consists of media companies Walt Disney Co., Viacom, Inc., CBS Corp., NBC Universal and News Corp. and Internet companies Microsoft Corp., MySpace, Veoh Networks and Dailymotion. The guidelines, which do not apply to search engines, e-mail or browsers, are designed for web sites that host user-generated clips, such as YouTube. They require those web sites to use filtering technology to block copyrighted clips from being posted without permission. They also require web sites to identify other web sites that repeatedly try to upload unauthorized content and either block those web sites or remove links to them. The new guidelines require Internet companies to have in place by

year end 2007 filtering software that blocks all content media companies flag as being unauthorized. They also require user-generated video sites to keep their filtering technology current, and they call for cooperation between media and web companies to allow “wholly original” user-generated videos to be posted and to accommodate “fair use” of copyrighted material as allowed by law. The guidelines do not, however, specify how liberally “fair use” will be defined. Fair use provisions of U.S. copyright law allow segments of copyrighted works to be used for purposes of parody or satire or in reviews and other limited circumstances.

### **RIAA THREATENS 19 UNIVERSITIES**

Just in time for the fall semester, the Recording Industry of America (RIAA) sent “prelitigation” letters to 19 universities, alleging that campus networks are being used to commit copyright infringement. Each of the 411 letters indicates that a particular student or employee of the university is about to be sued for copyright infringement. The letters offer an opportunity for those targeted to settle out of court at a “discounted rate,” using a special web site that allows them to settle their claims online. The list of universities receiving letters and the number of letters for each is: Drexel University (17 letters), Indiana University (23), Northern Illinois University (25), Occidental College (19), State University of New York at Morrisville (18), Texas Christian University (20), Tufts University (15), University of Alabama (14), University of California at Berkeley (19), University of Delaware (18), University of Georgia (13), University of Iowa (18), University of

Michigan at Ann Arbor (20), University of Nebraska at Lincoln (13), University of New Hampshire (30), University of New Mexico (17), University of South Florida (43), University of Southern California (37) and Vanderbilt University (32).

### **STUDY PROFILES ID THIEVES**

According to a new study of Secret Service cases, 42.5 percent of identify thieves are between the ages of 25 and 34, with another 18 percent between the ages of 18 and 24. The study also found that two-thirds of the identity thieves were male, and nearly one-quarter of the offenders were born outside of the U.S. Researchers from the Center for Identity Management and Information Protection at Utica College reviewed 517 cases closed by the Secret Service between 2000 and 2006 for the study, which was funded by the U.S. Department of Justice. They found that two-thirds of the cases were concentrated in the Northeast and South, and that 80 percent of the cases involved an offender working alone or with a single partner. There were 933 defendants in the 517 cases, and 609 of them said they initiated their crime by stealing fragments of personal identifying information, as opposed to stealing entire documents. The study also found that most of the offenses were committed by non-employees who victimized strangers. Employee offenders were the offenders in only one-third of the cases, and of that one-third, 40 percent were employed in a retail business and 20 percent worked in the financial services industry. The full study can be accessed at <http://www.utica.edu/academic/institutes/cimp/publications/index.cfm>.

## **AS WE GO TO PRESS...OMNIBUS CRIME BILL INTRODUCED**

On October 25, Senator Joseph Biden introduced S. 2237, an omnibus anti-crime bill which contains several provisions to address computer crimes. Those provisions include the following:

- 1) Establishing an Internet Crimes Against Children (ICAC) task force program that will ensure each state has a specialized unit to prevent, investigate and prosecute online child exploitation cases. The bill provides \$635 over eight years for this purpose.
- 2) Establishing a special counsel within the Department of Justice to oversee online child exploitation prevention and prosecution efforts, including working with other federal, state and local agencies and the private sector.
- 3) Additional federal resources to combat online child exploitation, including additional agents at the FBI, Bureau of Immigration and Customs Enforcement and the U.S. Postal Service and increased resources for the FBI's regional computer forensic labs. The bill provides \$400 million for this purpose.
- 4) Making it a federal crime to intentionally injure or attempt to injure a person under 18 years of age by force or threat

of force if the crime involves interstate commerce or travel, took place in a territory of the U.S. or if the defendant used an instrument of interstate commerce, such as a phone or the Internet, in the commission of the crime. The bill directs the U.S. Sentencing Commission to provide enhanced penalties for crime involving a victim under the age of 18 years.

- 5) Regulating rogue, online Internet pharmacies by requiring that before selling a controlled substance, patients receive at least one in-person consultation with a physician.
- 6) Re-authorizing the Paul Coverdale forensic grant program that provides grants to state and local crime labs to process forensic and DNA evidence. It directs the U.S. Attorney General to take steps to reduce the backlog at state and local labs. The bill provides \$150 million per year for five years.
- 7) Amending the Computer Fraud and Abuse Act to penalize conduct that causes limited damage to a large number of victims, to criminalize the use of botnets to perpetrate online crimes or attacks and to make computer equipment used to commit crimes forfeitable. The bill authorizes \$30 million per year for five years for this purpose.

- |  |  |
|--|--|
| 8) Amending the Computer Fraud and Abuse Act to criminalize accessing without authorization a computer used by a registered candidate or political party or used to administer a federal, state or local election. | Providing the Department of Justice with new investigative tools, criminal penalties and forfeiture and restitution provisions to combat copyright infringement. |
|--|--|

## TOOLS YOU CAN USE

---

### Findings From Identity Theft Research

“Identity Theft: A Research Review,” a study sponsored by the National Institute of Justice, discusses the information currently available on identity theft and pinpoints areas that need further research. Researchers’ findings concluded that additional information is needed in areas relating to prevention, including reduction of harm to individual victims, financial institutions and society. The study may be accessed at <http://www.ojp.usdoj.gov/nij/publications/id-theft/welcome.htm>.