National Association of Attorneys General

SEPTEMBER - OCTOBER 2008 CYBERCRIME NEWSLETTER

National Center for Justice and the Rule of Law
The University of Mississippi School of Law

Issue 33

News Highlights in This Issue:

Table of Contents

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, 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.

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.

ACQUIRING COMPUTER COMMUNICATIONS: Often a Treacherous Task

By Stephen Treglia
Chief, Technology Crime Unit
Office of the Nassau County District Attorney

You the prosecutor are provided with a printout of a communication in a child abuse case that was transmitted digitally over a computer network or the Internet. Can you use it as evidence?

That single question inevitably presents an additional line of inquiry: Was the communication lawfully acquired? Is the communication subject to suppression? The answers to these questions are among the toughest for any lawyer to divine today. Due to a jumbled confluence of federal and state constitutional, statutory and case law, the answers become invariably complex because they depend on many different factors. More to the point, the slightest variation in the fact pattern can immediately flip the answer, like a light switch, in the opposite direction. Even still, the correct answers today risk obsolescence tomorrow due to changes in either the law or technology.

Part of the difficulty is that the law is still evolving. Many of the questions have not yet been answered directly by the courts, and as a consequence, law enforcement must speculate as to the proper course of action. Existing statutes governing this area, drafted when many of today's technologies were not within man's realm of imagination, do not begin to provide the necessary guidance. Digital technology progresses and mutates rapidly, while democratic policy making, with its need for general awareness of impending consequences and consensus of the appropriate response, moves more ponderously. Not surprisingly, the issues the courts have addressed often result in conflicting or confusing decisions. In short, these factors serve to plague our system of laws unlike any other scientific advance in history.

The Starting Point

Of course, law enforcement must respond when crimes are committed, even without the benefit of legal

precedent on occasion. But where to begin? The answer may be derived from four simple questions, all of which relate directly to the nature of the communication at issue:

- What kind of communication is it?
- How was it secured so as to deliver its contents to law enforcement?
- Who secured it?
- From what point in the transmission process was it secured?

The analysis begins with what shall be described as "static communication," in other words, communication seized while it is stored stagnantly in some form of computer storage media (e.g., a hard drive, a CD, a floppy disk, etc.).

Private searches

The easiest analysis in the realm of static communications involves searches not conducted by law enforcement, often referred to as "private searches." As long as the searcher is not acting as an agent of law enforcement, the fruits of the search may be used by law enforcement because the Fourth Amendment is "wholly inapplicable to a search and seizure, even an unreasonable one, effected by a public citizen," *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

One of the more dramatic examples of how far this principle extends can be found in *United States v. Runyan*, 275 F.3d 449 (5th Cir. 2001). Mrs. Runyan left the family abode (a Texas ranch) to live with another man. Following her departure, her husband changed the locks on the doors of the structures on the ranch, installed a fence surrounding the ranch secured by lock and chain and had surveillance cameras placed on the premises. Despite these measures, the wife, accompanied by her boyfriend and/or several friends, repeatedly gained access to her former residence. On the first two occasions, they climbed over the newly-installed fence, and on the third they cut the fence open with bolt cutters. On the last of these visits, Mrs. Runyan and six friends spent two days on the ranch rummaging through personal items. As they left, they took with them a computer and several removable discs. Upon returning to Mrs. Runyan's new home, they discovered that some of the discs contained child pornography and promptly turned the material over to the authorities.

The Fifth Circuit upheld the portion of the lower court's denial of the defendant's motion to suppress the information from the disc and computer that Runyan and her friends seized. Regardless of the felonious entry and apparent theft of property, the suppression court held that the appropriation of the items by the wife and her friends was not the product of law enforcement activities, even though clearly illegal.

Of course, the story did not end there. The sheriff's department that received the stolen property in *Runyan* inspected the contents of each and every disc that Mrs. Runyan and her cohorts seized. As a consequence, the lower court granted the motion to suppress with respect to the evidence not viewed first by civilian eyes because the deputies did not secure a search warrant for them. As for the discs previously viewed by the civilian criminals, the

court upheld the warrantless search of those discs, even though the deputies viewed additional depictions on those same discs the civilians had not viewed before they provided them to law enforcement.

Computer repair issues

Expanding the scope of the original private search in the digital world most frequently occurs when computers are delivered to others for repair. So far, the case law in this area has been somewhat erratic. In *Runyan,* the court seemed to apply a "once you're there" rule, permitting law enforcement to expand the scope of the original search beyond the depictions of child pornography found by civilians on the discs to additional depictions as long as they were part of the same discs. At least two decisions reject this theory.

In *United States v. Barth*, 26 F.Supp.2d 929 (W.D. Texas 1998), the district court granted the motion to suppress depictions of child porn law enforcement viewed without a warrant that exceeded the limited number originally observed by the technician repairing defendant's computer. Although there was no suppression in *People v. Emerson*, 196 Misc.2d 716, 724 (Sup. Ct. Monroe Cty. 2003), this New York court speculated in *dicta* that it would have granted the suppression motion had the police search gone beyond the initial private search of those items.

Even where the courts have found the technician to be an agent of law enforcement, the holdings have been less than uniform. In *Barth,* the technician was, coincidentally, already an active FBI informant when he discovered a single depiction of child pornography on the defendant's computer. The court denied suppression of the initial depiction because the technician discovered it while working outside the scope of his duties as an active informant. Once the technician called the FBI following his discovery of the first depiction, however, his continued search, conducted at the direction of the FBI, transformed him into an agent for the remaining depictions he viewed after that contact.

In contrast, where the FBI repeatedly used the services of an anonymous hacker that ultimately resulted in child pornography charges being filed in *United States v. Jarrett*, 338 F.3d 339 (4th Cir. 2003), the court did not find an agency relationship existed to mandate suppression of the depictions at issue. The Fourth Circuit determined the FBI did not "demonstrate the requisite level of knowledge and acquiescence" of the informant's involvement in accessing this specific defendant's computer before the hacker advised the FBI of the child porn he discovered on defendant's computer. The government's use of the hacker's assistance in prior child porn distribution cases, or the open invitation the FBI left to the hacker to provide information on future similar cases, did not alter the court's determination.

Consent

Federal and New York law require the consent of only one party to a communication in order for it to be secured by law enforcement without a warrant. Does the result change when one party to the communication is from a jurisdiction that requires both parties to consent to the release of a

communication? Certainly, this scenario presents a realistic possibility when dealing with online communications.

One answer might be found in the theory of implied consent. Online communications, by their very nature, are recorded. In order to be transmitted they are preserved in digital format and made visible on a computer screen. Can anyone engaged in online communications realistically expect that a typed communication disappears as easily as the spoken word?

Consent of the Fellow User

Generally, the ability to gain joint access to shared property grants one user the authority to consent to law enforcement's search of a particular item, such as a computer, without a showing that the consenting party ever used the item. *United States v. Duran*, 957 F.2d 499 (7th Cir. 1992); *United States v. Smith*, 27 F.Supp.2d 1111 (CD Ill. 1998). At least two state courts have agreed with this theory. *See Walsh v. State*, 236 Ga. App. 558 (1999); *State v. Guthrie*, 2001 S.D. 61 (2001).

Mere joint access to computer-related items alone, when the ability to use those items has been absent, has not always been held to grant the accessible party authority to consent. One court has recognized the inability of a housemate to consent to the seizure of her fellow housemate's password-protected computer files, even when the two jointly shared the use of the computer, *Trulock v. Freeh*, 275 F.3d 391 (4th Cir. 2001). In *United States v. James*, 353 F.3d 606 (8th Cir. 2003), the defendant's mere delivery of "backup computer discs" to another person for safekeeping, followed by an instruction to destroy them once the defendant was incarcerated, did not give the possessor of the discs the authority to consensually turn them over to law enforcement.

When Joint Possessors' Conflict on Consent

What if one possessor gives consent to law enforcement but the other opposes consent? A recent decision warns the opposing party that he or she had better be on the premises when the opposition is conveyed. In *Georgia v. Randolph*, 547 U.S. 103 (2006), the Supreme Court held that a wife could not grant permission to search the marital residence for drugs when her husband, present at the residence when she gave her consent, opposed the search – even though the husband and wife were estranged at the time.

In a case decided shortly after *Randolph,* a circuit court considered the suppression of evidence obtained from a home computer jointly owned by a husband and wife. The wife gave consent while present in the marital home, but only after her husband, arrested at his office, had refused his consent. In *United States v. Hudspeth*, 459 F.3d 922 (8th Cir. 2006), the Eighth Circuit ruled that *Randolph* mandated suppression of the seized evidence, because the wife's consent occurred after her absent husband's refusal to consent to the search. About four months later, however, the Eighth Circuit vacated that ruling, and subsequently ruled *en banc* that the wife's consent was valid, since the husband was not at home at the time of his refusal, even though his wife had not been informed of her husband's earlier opposition. *Hudspeth*, 518 F.3d 954 (2008).

Workplace searches

How do consent issues morph when the computer being searched is located in an office? Depends on the nature of the office. In a private company, any co-worker can usually authorize the search of any co-worker's office property. *See United States v. Gargiso*, 456 F.2d 584 (2nd Cir. 1972); *United States v. Bilanzich*, 771 F.2d 292 (7th Cir. 1985); *JL Foti Constr. Co. v. Donovan*, 786 F.2d 714 (6th Cir. 1986). Even if the consenting party is lower in the chain-of-command, the lower level employee can authorize the search of a superior's computer. *United States v. Murphy*, 506 F.2d 529 (9th Cir. 1974); *United States v. Buettner-Janusch*, 646 F.2d 759 (2nd Cir. 1981); *United States v. Jenkins*, 46 F.3d 447 (5th Cir. 1995). A noteworthy limitation to a broad rule-of-thumb of co-worker consent occurred in *United States v. Buitrago Pelaez*, 961 F.Supp. 64 (S.D.N.Y. 1997). There, the court ruled that while a receptionist could consent to a general office search, that consent was invalid for a locked safe where the receptionist did not know the combination.

Thus, *Buitrago Pelaez* begs the question in the computer realm where the worker has decided to password-protect or encrypt the files stored on the office computer. Unless the password or encryption key is known by co-workers or there is an unequivocal computer use policy authorizing the disclosure of all computer data stored on office computers, *Buitrago Pelaez* supports suppression of seized data that is protected. As mentioned earlier, a housemate's ability to jointly use a computer did not give her authority to grant law enforcement to search her co-housemate's password-protected files stored in the same computer. *See, Trulock*, *supra*.

Government employees

The ability of a co-worker to authorize the search of an office computer in a government agency is not as broad as in a private company. The Fourth Amendment protection against government searches applies to searches of a public employee's office computer under certain circumstances. *United States v. Slanina* 283 F.3d 670 (5th Cir. 2002). The more accessible the computer is for use by fellow co-workers, the less likely any single employee can claim a reasonable expectation of privacy. If, however, the computer is in an office assigned solely to the employee and that employee is the sole user of the computer in that office, there is a stronger likelihood that employee possesses a reasonable expectation of privacy in the use of that office computer, and a search warrant is required to conduct a lawful search of its contents.

A government employee's expectation of privacy, however, is not completely unfettered. Courts have recognized the right of government personnel to search a co-worker's computer without a warrant for "work-related purposes" (i.e., searching for a missing office memo) or "workplace misconduct," *United States v. Slanina*, *supra*.

One might wonder how any investigation of "workplace misconduct" would not also be an investigation of criminal activity. In *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000), the Fourth Circuit did away with attempting to divine the real intentions behind the

warrantless search. In *Simons,* the court ruled that even where the "dominant purpose" of the computer search was "law enforcement-related" the warrantless search of a CIA employee's office computer by the Inspector General's branch was justifiably a search for "workplace misconduct."

Personal property

Obviously, no employer or employee can consent to the search of a co-worker's private property, right? Again, there are no all-inclusive answers when the property in question is a computer.

At least two courts have upheld a warrantless search where a government employee utilized his personal computer in his place of work and allowed co-workers to have access to that computer. The courts reasoned that allowing access caused the employee to forfeit any reasonable expectation of privacy. *United States v. Barrows*, 481 F.3d 1246 (10th Cir. 2007); *United States v. Rosario*, 558 F.Supp.2d 723 (E.D. Ky. 2008).

Certainly, the securing of a search warrant to inspect the data stored on a computer resolves most suppression issues, but not all. Here is just one more example how slavish adherence to the concept that any one answer solves all problems when it comes to computers can get someone in a ton of trouble!

Voice communications

Today, communications containing the human voice are transmitted more and more frequently over the Internet. How federal and state law treat such communications may be a treacherous road for prosecutors to travel.

Under the original version of the Electronic Communications Privacy Act of 1986 (ECPA), voice communications kept in storage with a public electronic communication service awaiting transmission to the intended recipient could only be accessed by law enforcement via an eavesdropping warrant. The USA PATRIOT Act of 2001 amended that provision to allow for such communications to be acquired by search warrant, at first only until January 1, 2006, but now permanently.

The question becomes: what if a state's law still requires an eavesdropping warrant to access such voice communications? For example, New York's Penal Law Section 250.00, subdivision 3, defines voice communications (which are only obtainable under New York law by an eavesdropping warrant) to include "any electronic storage of such communications."

In other words, does the ECPA preempt state law in this area? One case had stood for that position, *Quon v. Arch Wireless*, 445 F.Supp.2d 1116 (C.D. Cal. 2006). The district court decision in *Quon*, however, was recently reversed in part by the Ninth Circuit in a decision which did not adopt the preemption position advanced by the trial court, *Quon*, 529 F.3d 892 (9th Cir. 2008).

Another argument exists that lends strong support to the absence of federal preemption of state law on the acquisition of computer-generated voice communications. The provision of the ECPA that governs law enforcement's acquisition of computer communications

is contained wholly within Title II, entitled the "Stored Wire and Electronic Communications Act" (SCA).

Title III of ECPA, on the other hand, initiated the need of law enforcement to acquire pen registers for the real-time dialed numbers from a telephone. Prior to ECPA, law enforcement simply obtained subpoenas for the location of the "pairs and appearances" of the connecting telephone wires from the telephone company, and attached the pen register to those wires. Title III also requires all states to adopt their own version of pen register statutes mirroring at least the minimum requirements of ECPA within two years or Title III would automatically become the law of any non-enacting state. Hence, if ECPA's Title III unequivocally contains preempting language but Title II (SCA) completely lacks similar language, the argument exists Congress evinced its intent not to make SCA the mandatory law in every state.

The significance of all this? If law enforcement, relying solely on SCA's requirements, is lulled into the belief that a search warrant is sufficient to acquire an electronic communication from a public communication service provider containing the human voice, those involved in that acquisition could discover that their state's wiretap laws might dictate such communication could only properly be acquired via an eavesdropping warrant. Such consequences could be extremely dire. Acquiring an electronic communication without a proper search warrant usually results in suppression of the evidence at a criminal trial and could lead to a civil suit against those involved in the illegal search. The illegal acquisition of a voice communication not only leads to the suppression of the evidence, but it is a crime.

Acquisition of real-time communications

Federal and state law are currently in synch to require an eavesdropping warrant for what was earlier described in this article as a "dynamic communication," that is, a communication actively "in transit." This rule applies to both electronic and voice communications. In other words, any communication intercepted while actively in transit between its starting and ending points without an eavesdropping warrant is illegal.[1] (Remember, however, that ECPA permits the legal acquisition of online communications by law enforcement via search warrant while in temporary storage at a public communication service provider.)

That having been said, the courts have issued less than crystal clear rulings in this area. In *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005), the defendant was charged with eavesdropping email communications entering his company's computer system. The email was intended to be ultimately delivered to the company's customers. Despite the fact that the email was already received and stored on the company's computers, the court created the previously non-existent

[1] Scenarios under which a communication service provider may legally access communications over its own service without an eavesdropping or search warrant are beyond the scope of this article.

concept of "transitory storage" to hold the defendant liable for eavesdropping on electronic communications still "in transit" in that the emails had not yet been forwarded to the "inboxes" of each customer's respective email account.

Two other federal court decisions have been less willing to hold the interceptors of computer-generated communications liable. Both cases, however, may be so fact-specific that they ultimately lack precedental value. In *United States v. Scarfo*, 180 F.Supp.2d 572 (D.N.J., 2001), the FBI obtained a search warrant in an ongoing gambling investigation, and installed a keystroke logging software program onto the defendant's computer. In seeking suppression, defendant contended that the government was intercepting communications "in transit" without an eavesdropping warrant.[2] The court ruled that since the keystroke logging program ceased operation whenever the modem accessing the Internet was activated, it was impossible for the FBI to have captured any communication "in transit."

In *United States v. Ropp*, 347 F.Supp.2d 831 (C.D. Calif., 2004), the district court was faced with a keystroke logging method different from that in *Scarfo*. Here, the keystroke logger was a piece of hardware. An employee at an insurance company installed the keystroke logger on his co-worker's computer by attaching it to the cable connecting the keyboard to the central processing unit (CPU). As a result, the defendant was able to read all the words and symbols keyed into the computer by his co-worker including those keystrokes involving computer-generated communications. Prosecuted by the federal government for eavesdropping, the court dismissed the charges. Although it found that the communications were intercepted "in transit," the point of interception forced the court to dismiss the eavesdropping count.

A necessary element of the federal offense of eavesdropping is that the intercepted communication is transmitting over a device which "affects interstate or foreign commerce." A communication captured before it even reaches the computer's CPU was, in the court's opinion, not far enough along the "information superhighway" to affect interstate or foreign commerce. One wonders, however, if a state court might have found illegal eavesdropping because, usually, state wiretapping laws lack the "affecting interstate or foreign commerce" requirement.

Interestingly, the district court in *Ropp*, in determining that existing precedent offered "little guidance," rested its holding on *Scarfo* and *Councilman*. The irony here is that *Councilman,* as relied upon in *Ropp*, was an decision issued earlier than the one cited in this article -- specifically withdrawn and voided by the First Circuit just two days before *Ropp* was decided. As demonstrated by *Ropp*, even courts can fall prey to the fluid nature of this constantly evolving area of the law!

[2] For some unknown reason, the defense did not argue that the search warrant secured by the FBI in this case was really designed to be executed like an eavesdropping warrant.

Familial consent

One of the more common practices advocated by some matrimonial attorneys and some advocates for the prevention of child abuse is the installing of keystroke logging devices to spy on the online activities of spouses or children. It is likely that this category of online communications will most frequently be presented by attorneys and civilians for use in a criminal proceeding. As a consequence, law enforcement must be very careful when accepting communications intercepted by civilians using such devices.

First, potential defendants may argue that certain "real-time" online communications intercepted by such devices could be the recording of communications "in transit." While the law allows evidence obtained by civilians without a search warrant to be utilized by law enforcement, such is not the case with evidence that can only be obtained via an eavesdropping warrant unless there is consent by at least one of the communicating parties.

New York does not have a familial exception written into its eavesdropping statutes. Nor does there appear to be any court decisions in New York on when a computer-generated communication is considered to be "in transit." Hence, recourse must found, if anywhere, in the case law regarding telephonic communications.

In *I.K. v. M.K.*, 194 Misc.2d 608 (Sup.Ct. N.Y. Cty. 2003), a father who intercepted telephone conversations between his child and estranged wife sought to have these conversations admitted into evidence in a custody proceeding. The court ruled that this evidence was inadmissible because it violated New York's eavesdropping statute. In a criminal prosecution for child abuse, the court refused to accept in evidence telephone calls surreptitiously recorded by the victim's parents between the minor victim and the defendant, again because such recordings were illegally acquired in violation of New York's eavesdropping law. *People v. Heffner*, 187 Misc.2d 617 (Rensselaer Co. Ct. 2001).

One recent case, however, has attempted to divine a way to shield parents from an eavesdropping prosecution when done to prevent suspected abuse of a child. The court in *People v. Clark*, 19 Misc.3d 6 (Sup. Ct. App. Term, 2008), adopted a common law concept of derivative consent, where a parent may consent on behalf of a minor child who is incompetent to consent due to his or her young age. The court recognized that other states specifically accept a rule of parental "vicarious consent" of a minor's telephone conversations. The court further noted that federal case law has construed its wiretap statutes, upon which New York's are based, to permit the parent to consent to the recording of a child's telephone calls where there is a "good faith, objectively reasonable basis to believe that it was necessary for the welfare of the child."

Conclusion

How such holdings will translate from the acquisition of telephonic communications in child abuse investigations to the world of seizing online communications presents one of the myriad ways that law enforcement will find itself up the creek of the

"information superhighway" with a very unstable paddle. The tolerance for risk, the degree of the needs of the investigation in preventing harm, the limited legal precedent in place and, finally, the privacy interests at stake will all have to be carefully counterbalanced in each and every case when making these very difficult decisions.

AGs FIGHTING CYBER CRIMES

ARIZONA

Attorney General Terry Goddard discussed Internet safety with 700 middle school students as part of his statewide Internet Safety School Tour. His presentation emphasized precautions young people should take with social networking web sites. He also talked about teens who have been victims of Internet exploitation and cyberbullying.

DISTRICT OF COLUMBIA

Acting Attorney General Peter Nickles' Office joined forces with the U.S. Attorney's Office for the District of Columbia (USAO) to provide Internet safety awareness presentations for District of Columbia school children and their parents. The USAO trains all volunteers, who include representatives from the Attorney General's Office, District of Columbia Public Schools and the Metropolitan Police Department's Internet Crimes Against Children Unit. Each presentation is geared to an age level, with the one for younger children featuring 3-D animation and interactive games to teach them about Internet safety. Children sign an Internet safety pledge card which they can take home. Presentations for pre-teens and teens include accounts from children who have encountered online dangers, as well as success stories from teens who avoided them.

FLORIDA

Attorney General Bill McCollum's Cybercrime Unit, together with the Longwood Police Department. arrested Dewey Cruse, Jr. on one count of possession of child pornography, a third-degree felony carrying a maximum prison sentence of five years. Investigators discovered the pornography during an undercover Internet investigation that identified a known image of child pornography and traced the files back to Cruse's computer. A search warrant was executed at Cruse's home, and his computer and other computer equipment were seized. The equipment will undergo additional forensic analysis to determine whether additional images of child pornography are present. Additional charges could be added.

HAWAII

Attorney General Mark Bennett's agents participated in the arrest of Francisco Amsic and Matthew Lewis on separate charges of Electronic Enticement of a Child. Under a new law, both men face a mandatory sentence of 10 years in prison. Both Amsic and Lewis are accused of using the Internet to solicit a law enforcement officer whom they believed to be a 14-year-old girl. Each was arrested separately when he arrived at the pre-arranged meeting place and later indicted. The Honolulu Police Department, U.S. Immigration and Customs Enforcement and Naval Criminal Investigation Service participated in one or more of the arrests.

IDAHO

Attorney General Lawrence Wasden announced that Marcus Young, who pled guilty to one count of possession of sexually exploitive materials and one count of destruction of evidence, was sentenced to serve up to six years in prison.

Young will also be required to register as a sex offender once he is released from custody. According to the indictment, Young, a former county IT manager, was accused of possessing more than 100,000 pornographic images on four county computers. It further alleged that Young used a "wiping program" to remove the images from the hard drives and, as a result, it took investigators more than one year to analyze and conduct forensic analysis. Deputy Attorney General Justin Whatcoff of Attorney General Wasden's Special Prosecution Unit prosecuted the case.

ILLINOIS

Attorney General Lisa Madigan announced that Kristopher McNew was indicted on one count of Receipt of Child Pornography and one count of Possession of Child Pornography. Receipt of Child Pornography carries a potential penalty of five to 20 years in prison, while Possession carries a potential penalty of up to 10 years imprisonment, but both charges also carry a potential fine of $250,000 and from five years to lifetime supervised release after incarceration. The investigation was conducted by Attorney General Madigan's Crimes Against Children Task Force, the FBI Southern Illinois Task Force and other state and local law enforcement agencies. McNew was arrested following execution of a search warrant at his house by the FBI. He will be prosecuted by the U.S. Attorney's Office for the Southern District of Illinois as part of Project Safe Childhood.

KANSAS

Attorney General Steve Six created the Kansas Identity Theft Repair Kit to assist state citizens faced with identity theft. The Kit offers a step-by-step guide to repairing credit, as well as reviews a consumer's rights and liability under state and federal laws. It also provides tips for protecting personal information.

MICHIGAN

Attorney General Mike Cox's agents joined Kent County Sheriff's deputies in a joint Internet Child Predator sting that resulted in the arrest of 21 individuals who are charged with using the Internet to commit child sexual activity and Child Sexually Abusive Activity. The predators were arrested at or near a decoy home after engaging in explicit Internet chats with undercover agents posing as children. All defendants face at least two 20-year felonies. The defendant range in age from 20 to 65, with 17 from Michigan, three from Indiana and one from Illinois.

MISSISSIPPI

Attorney General Jim Hood's Internet Crimes Against Children (ICAC) investigators arrested Donald Lowery after he attempted to meet a child under 18 years of age for the purpose of having sex. Lowery, who had communicated online with an undercover ICAC officer, is charged with exploitation of a child. The Flowood Police Department participated in the arrest. Lowery is the first arrest by the ICAC Task Force since the state was awarded an ICAC grant by the Department of Justice.

MISSOURI

Attorney General Jay Nixon announced that social networking site MySpace removed an additional 212 online profiles that appear to match those of registered sex offenders in Missouri. To date, 1,449 profiles from the state have been turned over to the State Highway Patrol. Attorney General Nixon has asked the Patrol to examine the data for parole violations by offenders who may be barred from using a computer or contacting minors.

NEBRASKA

Attorney General Jon Bruning charged Kevin Fullerton with four counts of enticement by electronic communication device. Fullerton contacted one of Attorney General Bruning's investigators posing as an underage girl on an instant messaging site, identified himself as a 45-year-old male and encouraged the investigator to view a live sexually explicit video stream from his webcam. Enticement by Electronic Communication

Device is a Class IV felony carrying a penalty of up to five years in prison and/or a $10,000 fine.

NEW JERSEY

Attorney General Anne Milgram announced that Mario Esposito pled guilty to accessing a woman's e-mail account and retrieving nude photos of her without her authorization. Esposito was charged with third-degree computer criminal activity following an investigation by the State Police Cyber-Crimes Unit. Under a plea agreement, the State will recommend a sentence of probation conditioned on Esposito serving a county jail term not to exceed 364 days. In addition, Esposito must undergo a psychological examination and participate in a recommended course of treatment at his own expense. He will be prohibited from using the Internet during his probation except for employment or school purposes. Deputy Attorney General Mark Murtha took the guilty plea for the Division of Criminal Justice Computer Analysis and Technology Unit. Detective Sergeant John Gorman and Detective Brian Kearns handled the investigation.

NEW MEXICO

Attorney General Gary King's Internet Crimes Against Children (ICAC) unit led a cross-country online investigation resulting in the arrest of Albert Godwin III of North Carolina, charging him with 100 counts of sexual exploitation of a minor. Special Agent Lois Kinch, working undercover, received information indicating that Godwin was distributing child pornography. She contacted the North Carolina Internet Crimes Against Children (ICAC) Task Force, which executed a search warrant on Godwin's home and found thousands of child pornography images.

NEW YORK

Attorney General Andrew Cuomo's office filed a settlement agreement with MagsforLess.com over the online seller's failure to fulfill subscriptions or provide timely refunds to consumers. MagsforLess.com, aka HalfPriceMags.com, SnappyMags.com, AlmostFreeMags.com and MyIMag.com, must provide full refunds to consumers who never received magazines. The company has already paid more than $350,000 in refunds. Attorney General Cuomo's Internet Bureau conducted an extensive investigation after receiving more than 500 complaints. Under the settlement, MagsforLess must (1) process all magazine orders within seven days; (2) Clearly disclose when the consumer will receive the magazines; (3) provide a simple means for consumers to contact the company; (4) pay all refund requests within seven days of receipt; (5) inform all customers about the settlement and the opportunity for refunds; and (6) pay $100,000 in penalties to the State. The investigation was handled by Assistant Attorney General Carolyn Fast with assistance from Investigator Vanessa Ip and Confidential Mediators Penelope Lerner, Rachel Mills and Steven Spitzer under the direction of Justin Brookman, Chief of the Internet Bureau.

OKLAHOMA

Attorney General Drew Edmondson announced that Stephen Lewis, who had been on the run from Attorney General Edmondson's investigators for five months, was arrested in Nebraska on an outstanding warrant. Attorney General Edmondson's Office had charged Lewis with 14 counts of unfair or deceptive trade practices, alleging he had accepted payment for and failed to deliver several items he placed for sale through online auctions or advertisements. Lewis operates several companies, including Cowboy and Company, USA Cowboy, Arieyl Trailer and Pioneer Builders Supply and Services.

SOUTH CAROLINA

Attorney General Henry McMaster announced that Stephen Krum was arrested in an undercover Internet sting conducted by the Myrtle Beach Police Department, a member of Attorney General McMaster's Internet Crimes Against Children (ICAC) Task Force, Krum is charged with one count of Criminal Solicitation of a Minor, a felony offense punishable by up to 10 years in

prison. According to the arrest warrant, Krum solicited sex over the Internet with a boy he knew to be 16 years old. The boy reported the incident to police, and Krum later turned himself in. A search warrant was executed on Krum's hotel room, resulting in the seizure of a laptop, a digital camera and other computer-related items.

TEXAS

Attorney General Greg Abbott announced that Christopher Ferrell, the 100th online sex predator arrested by his Cyber Crimes Unit, was ordered to serve 30 days in jail each year for the next six years for using the Internet to prey upon children. Ferrell also received eight years deferred adjudication for sexually propositioning an undercover Unit investigator who had assumed the identity of a 13-year-old girl. He must also register as a sex offender for 18 years, attend sex offender counseling and is barred from using the Internet and having contact with children. Law enforcement officers from the Sugar Land Police Department and the Harris County Sheriff's Office also participated in the arrest.

UTAH

Attorney General Mark Shurtleff's Internet Crimes Against Children (ICAC) Task Force received $250,000 from Operation Kids, a non-profit organization dedicated to raising funds for children's issues. The donation was presented at an awards ceremony honoring John Walsh, America's Most Wanted host, with a Lifetime Achievement Award.

VIRGINIA

Attorney General Bob McDonnell's office joined with Microsoft and the Southwest Virginia Criminal Justice Training Academy in a one-day program to train more than 75 law enforcement officials from 35 different law enforcement agencies in effective online investigation practices, as well as how to work with Microsoft in the investigation of online crimes. The program consisted of such sessions as "Trends in Internet and Computer Crimes" and "Microsoft Online Services for Law Enforcement." Attorney General McDonnell delivered closing remarks.

WEST VIRGINIA

Attorney General Darrell McGraw filed suit against Blue Hippo Funding, LLC, Blue Hippo Capital, LLC and Joseph Rensin, the primary owner and operator of the two businesses, on charges of operating as an unlicensed telemarketer. Blue Hippo operates an extensive media campaign that advertises the sale of computers on the Internet, radio, television and print media, with all advertisements stating that "all you need is a checking account" to purchase a computer. However, the company failed to disclose that customers would need to sign a written contract, make weekly or bi-weekly payments for almost one year and pay approximately $2,000 for a computer they could have purchased elsewhere for a fraction of that cost. Consumers who complained to Attorney General McGraw's Consumer Protection Division claimed they never received the computers, and those who stopped paying on the account forfeited all the payments they had made. Under state law, telemarketers are required to be registered with the State Tax Department and to post a bond. They must also have a refund policy that allows consumers to obtain refunds, which Blue Hippo did not.

IN THE COURTS

ONLINE CHILD SOLICITATION LAW: 1ST AMENDMENT CHALLENGE

Podracky v. Commonwealth, 2008 Va. App. LEXIS 284 (Va. June 10, 2008). The Virginia Court of Appeals upheld a state statute that prohibits using a "communications system" to solicit a minor for sex against a First Amendment challenge. Dean Podracky was convicted of violating the state law, Va. Code §18.2-374.3(B). The instant messages he sent to the minors soliciting sex formed the basis of his conviction. On appeal, Podracky challenged the constitutionality of the statute, arguing that it violated his First Amendment free speech rights. He relied on *Reno v. American Civil Liberties Union,* 521 U.S. 844 (1997) in which the U.S. Supreme Court struck down two provisions of the Communications Decency Act. The appeals court, however, found that the *Reno* decision was not controlling in the instant case. The court also pointed to both state and federal decisions upholding similar statutes involving solicitation of minors for sex over the Internet. The court affirmed the trial court decision.

Ed. Note: Robert Anderson III, Senior Deputy Attorney General in the Office of the Attorney General of Virginia, argued the case for the Commonwealth.

SEX OFFENDER COMPUTER SEARCH LAW: FOURTH AMENDMENT

Doe v. Prosecutor, Marion County, 2008 U.S. Dist. LEXIS 48515 (S.D. Ind. June 24, 2008). The U.S. District Court for the Southern District of Indiana ruled that a provision in a new Indiana law permitting searches of a convicted sex offender's computer without cause violates the Fourth Amendment. Under Indiana's new statute, which was to take effect on July 1, 2008, all those who must register as sex offenders with the state must also consent to a search of their computers and other devices with Internet access and must consent to installation of hardware and software on those devices, at their own expense, to monitor their Internet use. A class action was brought by convicted sex offenders who had served their sentences and were not on probation, parole or court supervision alleging that the new provision, Ind. Code § 11-8-8-8(b) (effective July 1, 2008), violated their rights under the Fourth Amendment prohibiting unreasonable searches and requiring probable cause for a warrant. They sought a declaration that the new provision was unconstitutional and an injunction against its enforcement. After addressing a defense pre-enforcement challenge and finding the case ripe for decision, the court found that the statute forces the plaintiffs to risk another criminal prosecution for refusing to comply or immediate impairment of their constitutional right of privacy under the Fourth Amendment. It therefore found the statute unconstitutional as to this class of people.

ONLINE CHILD SOLICITATION: TESTIMONY ON MENTAL STATE

U.S. v. Gladish, 2008 WL 2927127 (7th Cir. July 31, 2008). The 7th Circuit Court of Appeals found that an Internet chat of a sexual nature, without more,

does not render a defendant guilty of attempted sex with a minor. Brian Gladish, 35, was caught in a sting operation in which a government agent impersonated a 14-year-old girl in an Internet chat room. Gladish had solicited "Abigail" for sex and discussed the possibility of traveling to meet her, but no arrangements were made. He did send "Abigail" a sexually explicit video of himself. Gladish was convicted of violating 18 U.S.C. Section 1470, which prohibits knowingly transferring obscene material to a person under 16 years of age, and 18 U.S.C. Section 2422(b), which forbids knowingly attempting to induce a person under 18 years of age to engage in any sexual activity for which one could be charged with a criminal offense. Gladish admitted guilt in the first charge, but not the second, arguing that he did not take a "substantial step" toward inducing "Abigail" to engage in criminal sexual activity. The psychologist who examined Gladish prepared a report that concluded Gladish got his sexual gratification solely from Internet chat. Gladish wanted the psychologist to testify to prove he would not have engaged in sex with "Abigail," but the trial court found that the proposed testimony was inadmissible under F.R. Evid. 704(b), which states that no expert witness may state an opinion as to whether the defendant did or did not have the mental state constituting an element of the crime because such issues are matters for the trier of fact. The 7th Circuit rejected this conclusion, holding that while Rule 704(b) precluded the psychologist from testifying that Gladish did not intend to have sex with "Abigail," he could have testified that it was unlikely that he would act on his intent.

EVIDENCE FROM FILE-SHARING PROGRAM: 4TH AMENDMENT

U.S. v. Ganoe, 2008 U.S. App. LEXIS 17424 (9th Cir. August 15, 2008). Tyrone Ganoe was charged with three counts of knowingly receiving child pornography and one count of knowingly possessing child pornography after an ICE agent found child pornography on Ganoe's computer while using LimeWire. LimeWire is a free file-sharing program that can be downloaded from the Internet, and users can input search terms and receive a list of responsive files from other computers attached to the network. Ganoe had used LimeWire to download music. At trial, Ganoe argued that the agent's use of LimeWire to access his files constituted a warrantless search under the Fourth Amendment, and moved to suppress the evidence obtained from the search. The U.S. District Court for the Central District of California denied the motion, finding that Ganoe knew or should have known that the software might allow others to access his computer, and he therefore lacked a reasonable expectation of privacy. On appeal, the Ninth Circuit affirmed, finding that since Ganoe had failed to demonstrate he had a reasonable expectation of privacy, he could not invoke the protections of the Fourth Amendment.

E-DISCOVERY

F.R.C.P 34'S TRANSLATION REQUIREMENT

Mon River Towing, Inc. v. Industry Terminal and Salvage Co., 2008 WL 2412946 (W.D. Pa. June 10, 2008). In this negligence action, Industry Terminal and Salvage Co. filed a motion to compel response to their discovery request for computer printouts and

records. Mon River Towing objected, arguing that they did not keep computer printouts in the ordinary course of business and that the Rules of Civil Procedure do not require the creation of documents for production. After analyzing FR.C.P. 34 (a) (1), the U.S. District Court for the Western District of Pennsylvania found that the rule's translation requirement does not obligate the responding party to create responsive documents, but it does require them to produce computer printouts. The court therefore granted the motion to compel, but also advised both parties to confer and reach an agreement in accordance with the court's finding.

LEGISLATION UPDATE

TEXTING WHILE DRIVING

CALIFORNIA. Governor Arnold Schwarzenegger signed SB 28 into law, a bill banning motorists from sending, reading or writing messages on electronic devices while driving, effective January 1, 2009. A first time offender will receive a fine of $20, followed by a fine of $50 for each subsequent offense.

ELECTRONIC DISCOVERY

CALIFORNIA. On September 27, Governor Schwarzenegger vetoed AB 926, a bill passed by the Legislature which proposed amendments to the state's Code of Civil Procedure Regarding Electronic Discovery. The bill would have implemented procedures for obtaining electronically stored information in civil actions, in addition to providing parameters for when the imposition of sanctions is appropriate. The bill can be accessed at http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_0901-0950/ab_926_bill_20080808_enrolled.html.

INTELLECTUAL PROPERTY ENFORCEMENT

ENACTED. On October 13, S. 3325, a bill enhancing remedies for violations of intellectual property laws, was signed into law as Public Law 110-403. The bill, sponsored by Senator Patrick Leahy (D-VT), authorizes a civil enforcement, in addition to criminal, action, as well as the establishment of a task force to investigate and prosecute copyright crimes. It prohibits the importation and exportation of copyrighted goods without the approval of the copyright owner. The bill also authorizes grants for training, prosecution and enforcement of copyright infringement actions.

PASSED SENATE. On September 26, the U.S. Senate passed S. 2913, a bill sponsored by Senator Patrick Leahy (D-VT), that limits the remedies and compensation in a civil action brought for copyright infringement in an orphan work. It also prohibits compensation if the infringer is a nonprofit educational institution,

museum, archive or public broadcasting entity.

ONLINE PHARMACY REGULATION

ENACTED. On October 15, H.R. 6353, the Ryan Haight Online Pharmacy Consumer Protection Act, was signed into law as Public Law 110-425. The bill, sponsored by Representative Bart Stupak (D-MI), prohibits the delivery, distribution or dispensing of controlled substances over the Internet without a valid prescription. It requires an online pharmacy to display on its web page a statement that the pharmacy complies with this legislation and that it complies with state licensing laws, as well as contact information and a statement that it has a licensed pharmacist. It authorizes states to apply for injunctions or obtain damages and other civil remedies for pharmacies deemed a threat to state agencies.

ONLINE CHILD EXPLOITATION

ENACTED. On October 13, S. 1738, a bill designed to develop a national strategy to combat online child exploitation and enhance existing programs, was signed into law, becoming Public Law 110-401. The bill, sponsored by Senator Joseph Biden (D-DE), establishes a national Internet Crimes Against Children Task Force with defined purposes. It authorizes grants for state and local task forces and provides for additional computer forensics capability to address the backlog.

ENACTED. On October 8, H.R. 4120, a bill sponsored by Representative Nancy Boyd (D-KS), became Public Law 110-358. The bill focuses on child pornography and expands the jurisdictional basis for online sexual exploitation of children to include foreign or interstate commerce.

PASSED BOTH HOUSES. On October 3, S. 602, a bill sponsored by Senator Mark Pryor (D-AR), passed the House after having passed the Senate two days prior. The bill requires the Federal Communications Commission to explore the use of advanced blocking technologies to improve or enhance the ability of parents to protect their children from indecent or objectionable videos and programming.

SEX OFFENDER REGISTRATION

ENACTED. On October 13, S. 431, sponsored by Senator Charles Schumer (D-NY), became Public Law 110-400. The bill requires sex offenders to register and keep current on the National Registry all Internet identifiers, and mandates the development of procedures to notify offenders of a change in requirements.

BROADBAND SERVICES

ENACTED. On October 10, S. 1492, a bill sponsored by Senator Daniel Inouye(D-HI) became Public Law 110-385. Among other initiatives, the bill provides for grants to develop and implement state initiatives to identify and track the availability and adoption of broadband services in every state. It requires the Federal Communications Commission to provide nonprofit organizations selected by the states as a partner with access to data collected from broadband service providers.

MOBILE COMMUNICATIONS ON FLIGHTS

PASSED HOUSE COMMITTEE. On September 28, the U.S. House Committee on Transportation and Infrastructure approved H.R. 5788. a bill sponsored by Representative Peter DeFazio (D-OR) that would prohibit engaging in voice communications using a mobile device during a flight.

IDENTITY THEFT ENFORCEMENT AND RESTITUTION

ENACTED. On September 26, H.R. 5938, a bill sponsored by Representative John Conyers (D-MI), became Public Law 110-326. The bill authorizes criminal restitution orders to compensate victims in identity theft cases for the time spent to remedy the harm. It also eliminates the requirement that damage to a victim's computer amount to $5,000 or more before a prosecution can be brought and makes it a felony to damage 10 or more computers within a one-year period. The bill also imposes criminal and civil forfeitures of property used to commit computer fraud offenses.

WEB REPRODUCTION OF MUSIC

ENACTED. On October 16, H.R. 7084, sponsored by Representative Jay Inslee (D-WA), became Public Law 110-435. The bill provides for a receiving agent, designated by the Library of Congress, to collect royalties to be disbursed to sound recording copyright owners who enter into agreements with webcasters for the performance of sound recordings over the Internet.

NEWS YOU CAN USE

STUDY: PARENTS OFTEN UNAWARE OF CYBERBULLYING

As many as 75 percent of teens have been bullied online, but only 10 percent have reported the problem to parents or other adults, according to a new study published in the September issue of The Journal of School Health. The U.C.L.A. study surveyed 1,454 teens between the ages of 12 and 17, who were recruited through an unidentified teen web site from August through October 2005. Of those surveyed, 41 percent reported between one and three online bullying incidents over the course of a year; 13 percent reported four to six incidents; and 19 percent reported seven or more incidents. Despite this prevalence, most teenagers don't realize how common cyber-bullying is and often believe it is only happening to them. One-half of the teens said they felt they "just had to learn to deal with it." Almost one-third said they didn't tell their parents for fear parents might restrict Internet access

– a fear more commonly expressed by girls than boys. Another one-third of teens aged 12-14 said they didn't tell an adult out of fear they could get in trouble with their parents. Although most people view cyber-bullying as anonymous, almost 75 percent of the bullied teens said they knew or were "pretty sure" they knew who was doing the bullying.

Fighting back on bullying…

WEB SITE ALLOWS ANONYMOUS REPORTING OF BULLIES

Six Utah schools, including elementary, middle and high schools, are using a web site that allows students to anonymously report bullies. Justin Bergener, a Brigham Young University student, created the site, which allows students to post tip information about drugs, thefts and harassment. The site makes school administrators aware of any tips by e-mail or text message. If a tip goes unread for a day or more, the site reminds schools a tip is waiting. The site, SchoolTipline.com, has almost 50 participating schools in Arizona, California, Texas and Washington.

U,S. LAGS WORLD IN INTERNET SPEED

The U.S. lags behind other countries in Internet connection and download speeds, according to the Speed Matters Speed Test, a project of the Communications Workers of America. The survey also determined that at the present rate, it will take the U.S. more than 100 years to catch up with Internet speeds in Japan. It is based on aggregated data from almost 230,000 Internet users and shows that the median real-time download speed in the U.S. is only 2.3 megabytes. By contrast, the average download speeds in Japan are 63 mbps; South Korea, 49 mbps; and France, 17 mbps. What that means is that a multimedia file that takes four minutes to download in South Korea would take almost one and one-half hours to download in the U.S. The report also ranks individual states on download speeds, with the five fastest states being Rhode Island (6.8 mbps), Delaware (6.7 mbps) New Jersey (5.8 mbps), Virginia (5.0 mbps) and Massachusetts (4.6 mbps). The report and a full list of state rankings can be accessed at http://www.speedmatters.org/pages/state.html.

MANAGERS USE SOCIAL NETWORKS FOR JOB SEEKERS

One in five hiring managers say they use social networking sites to research job candidates, with one-third of them dismissing the candidate after what they find, according to a survey by online job site CareerBuilder.com. The survey of 3,169 hiring managers found that the top area of concern for those that screened potential staff on the Internet were candidates posting information about drinking or using drugs, followed closely by those who posted provocative or inappropriate photographs or information. Other areas of concern were poor communication skills, lying about qualifications, using discriminatory

remarks and using an unprofessional screen name. However, 24 percent of these managers found content that solidified their decision to hire the candidate. An additional nine percent of those managers who did not use social networking sites said they plan to start that practice.

MUSIC INDUSTRY RESOLVES 2 ROYALTY ISSUES

Groups representing songwriters, music publishers, record labels and digital music web sites ended a seven-year dispute over two types of music royalties, but not the highly controversial performance royalty for Internet radio. However, the Digital Media Association, the National Music Publishers' Association, the Recording Industry Association of America, the Nashville Songwriters Association International and the Songwriters Guild of America agreed on mechanical royalties for interactive streaming music and limited music downloads. Mechanical royalties are those paid to songwriters, composers and publishers – not the artists who perform the music or the record companies who produce it. Limited music downloads are those with significant restrictions, such as songs disappearing from a device if the user does not pay a monthly fee. Under the new agreement, the royalty rate will be 10.5 percent of revenue as of January 1, 2008, with a rate of 8.5 percent of revenue applied retroactively from December 31, 2001 until the end of 2007.

REPORT LISTS STATE MODELS FOR ENCOURAGING BROADBAND

The Alliance for Public Technology and the Communications Workers of America jointly released a report with a searchable database of state government initiatives for access to advanced communications. The report, "State Broadband Initiatives: A Summary of State Programs Designed to Stimulate Broadband Deployment and Adoption," surveys state initiatives in seven areas: broadband commissions, task forces and authorities; public-private partnerships; direct funding programs; state networks; telehealth initiatives; tax policies; and demand-side programs. As a whole, they provide a checklist for policymakers wanting to encourage investment in and adoption of high-speed broadband networks. The document and the database can be accessed at http://www.speedmatters.org.

RECORD NUMBER OF DATA BREACHES IN '08 TO DATE

U.S. corporations, government agencies and universities reported a record 516 consumer data breaches, mostly caused by hackers and employee theft, in the first nine months of 2008, according to a report by the Identity Theft Resource Center. Approximately 80 percent of the breaches involved digital records, with the remainder from loss, theft or exposure of paper-based records. More than 36 percent of the breaches this year have been at businesses, while educational institutions accounted for 21 percent. Breaches

attributed to the military or state and federal government entities declined for the third straight year, down to 16 percent. Organizations reported that hacking (13.4 percent) and insider theft (16.5 percent) caused almost one-third of all breaches. Lost or stolen laptops and other digital storage media accounted for 20 percent of breaches, with another 14 percent blamed on accidental exposure, such as posting of Social Security numbers and other data on a public web site.

RESEARCHERS FIND KEYBOARD "SNIFFING" METHOD

Swiss security researchers have reproduced what a target typed by analyzing the signals produced by keystrokes, leading them to declare that keyboards are "not safe to transmit sensitive information." The keyboard attacks were developed by Martin Vuagnoux and Sylvain Pasini, doctoral students at the Security and Cryptography Laboratory at the Swiss Ecole Polytechnique Federale de Lausanne (EPFL). The students tested 11 different keyboard models that connected to a computer via either a USB or a PS/2 socket. The attacks they developed also worked with keyboards embedded in laptops. Every keyboard tested was vulnerable to at least one of the four attacks the researchers used. One attack was shown to work over a distance of 20 meters. Their work is expected to be reported in a peer-reviewed journal soon.

GUIDELINES FOR ".COM" ALTERNATIVES ISSUED

The Internet Corporation for Assigned Names and Numbers (ICANN), the Internet's key oversight agency, issued preliminary guidelines for the introduction of alternatives to ".com" as the beginning of many changes to the Internet's 25-year-old address system. The application fee, however, is expected to be about $200,000, partially refundable only in limited circumstances, in order to cover the potential $20 million cost of developing guidelines and reviewing applications. By contrast, the cost of a personal domain name using an existing suffix like ".com" is less than $10. The new suffixes might be for locations, such as ".nyc," industries, such as ".bank" or companies such as ".disney." The draft rules would allow non-English addresses for the first time and bar numerals-only suffixes in order to avoid technical problems. The rules also address potential conflicts, such as multiple requests for the same name or a request for another's trademark or geographic location. ICANN will start accepting applications early in 2009.

TOOLS YOU CAN USE

Protecting State Electronic Data

An issue brief, "Protecting the Realm: Confronting the Realities of State Data at Risk," was developed by the Security and Privacy Committee of the National Association of State Chief Information Officers (NASCIO). It underscores the critical nature of managing states' digital assets and identifies key elements for establishing better data security programs. The brief covers data ownership and governance, recommends grounding data protection in states' architecture frameworks and outlines nine primary elements that a comprehensive data protection program must incorporate. It also describes data classification frameworks and includes summaries of those in Arkansas, Iowa and Ohio. It can be accessed at http://www.nascio.org.

Internet Safety

The National Criminal Justice Reference Service (NCJRS) issued the "Internet Safety Special Feature," an online resource which includes a compilation of publications and related documents on Internet safety for children, Internet privacy, cyberbullying, cyberstalking and identity theft. It can be accessed at http://www.ncjrs.org/internetsafety.

Inaccessible Electronic Discovery Information

Working Group One of the Sedona Conference, which focuses on Electronic Document Retention and Production, released a commentary offering guidance on the preservation, management and identification of sources of information that are not readily accessible. The paper sets forth guidelines to assist litigants and courts in determining which sources of information will contain discoverable information. It can be accessed at http://www.thesedonaconference.org/dltForm?did=NRA.pdf.

Cross-Border Electronic Discovery Conflicts

Working Group Six of the Sedona Conference, which focuses on International Electronic Information Management, Discovery and Disclosure, released a paper for public comment on navigating the competing currents of international data privacy and e-discovery. The framework is composed of four parts: jurisdiction, applicability of provisions limiting cross-border data transfers, blocking statutes and considerations surrounding treaties, legislation or other party agreement that may provide a solution, It can be accessed at http://www.thesedonaconference.org/dltForm?did=WG6_Cross_Border.

Teens and Technology

The Office of National Drug Control Policy (ONDCP) developed a package of information for both parents and teens to help combat potentially dangerous online behaviors and misinformation. The "teens and technology" package includes a fact sheet, accessible at http//www.theantidrug.com/resources/pdfs/Teens-Tech-Factsheet.pdf; an open letter to parents, accessible at http://www.theantidrug.com/openletter_e-Monitoring_editable.pdf; and a technology guide for teens and parents, accessible at http://www.theantidrug.com/teens-technology/index.asp.