pf

cybercrime LAW REPORT

Vol. 3, No. 8 April 21, 2003

Highlights

Child Abuse Prevention Bill Bans Misleading Domain Names

House and Senate conferees have included new restrictions on the use of "misleading" Internet domain names in legislation aimed at providing tougher penalties for child abuse and child pornography. **Page 3**

FTC Hampered by Lack of Funds, Power

The Federal Trade Commission lacks both the authority and resources to fully aid victims of identity theft, an agency official said at an April 3 congressional hearing. **Page 3**

State Legislative Priorities Set for Prevention of Identity Theft

Despite the enactment of many privacy and identity theft protections in recent years, law enforcement officials said April 9 that California still has far to go in protecting its citizens from identity theft. **Page 4**

Three Charged Over E-Mails Purporting to Sell 'Inside' Information

A Baltimore man and two affiliated financial publishing companies were charged April 10 in the U.S. District Court for the District of Maryland with disseminating e-mails that offered to sell purported inside information concerning the award of a government contract. **Page 5**

Policy Leadership on Cybersecurity Questioned

President Bush's former cybersecurity adviser criticized the administration April 8 for failing to provide the leadership necessary to ensure the federal government's own computer systems are not vulnerable to a major cyberattack. **Page 5**

Two Circuits Address Limitation on Computer Use as Condition of Release

The U.S. Courts of Appeal for the Seventh and Eighth Circuits released opinions within a day of one another that address restricting convicted felons' use of computers and the Internet as a condition of their release. While the two decisions address convictions for the possession and/or sale of child pornography, the principles they articulate apply to any sentence imposed for using a computer as a criminal instrumentality. **Page 7**

Spreader of Multinational Virus Face Fines, Prison

A Swedish citizen who admitted he created and spread a computer virus detected in at least 40 countries faces fines and a two-year prison sentence for violating Swedish law, Swedish police officials said April 3. **Page 10**

Table of Contents

Organizations in this Issue

cybercrime LAW REPORT

Published by Pike & Fischer, Inc., a subsidiary of BNA, Inc.

Carol Eoannou, Managing Editor ..... 301-562-1530 ext. 269 ..... ceoannou@pf.com
Adam Rickel, Marketing Manager ..... 301-562-1530 ext. 225 ..... arickel@pf.com
Zachary Wheat, Publisher ..... 301-562-1530 ext. 229 ..... zwheat@pf.com

cybercrime LAW REPORT (ISSN 1535-5853) is published biweekly (except for the last biweekly publishing date in December) for $315 per year by Pike & Fischer, Inc., 1010 Wayne Avenue, Suite 1400, Silver Spring, MD 20910-5600. Editorial questions, comments, and materials relating to this publication should be directed to the Publisher.

POSTMASTER: Send address changes to *cybercrime LAW REPORT*, Pike & Fischer, Inc., 1010 Wayne Avenue, Suite 1400, Silver Spring, MD 20910-5600.

Policy & Legislation

Minors

Child Abuse Prevention Bill Bans Misleading Domain Names

House and Senate conferees have included new restrictions on the use of "misleading" Internet domain names in legislation aimed at providing tougher penalties for child abuse and child pornography.

House and Senate negotiators agreed to a final version of the legislation (S. 151) April 8 that includes the domain name amendment adopted by the House.

The provision, added to the House version of the bill by Rep. Mike Pence (R-Ind.), would make it illegal and punishable by a fine and up to two years in prison to knowingly use a misleading domain name with the intent of deceiving a person into viewing obscene materials on the Internet. Under the legislation, those who knowingly use a misleading domain name with the intent of deceiving a minor into viewing Internet material that is "harmful to minors" could face a fine and up to four years in prison.

In the manager's statement accompanying the bill's conference report, supporters say the provision is "constitutional and necessary. There is a growing trend for those attempting to sell pornography to use aggressive and misleading tactics to deceive unsuspecting and unwilling individuals, both adults and minors, into viewing the pornography—often obscene or harmful to minors."

Critics have raised concerns about the provision's potential impact on free speech, however. In addition, some have noted that federal courts have raised questions about the "harmful to minors" standard used in the legislation.

In addition, the bill would create a national Internet site containing information about registered sex offenders and includes a ban on computer-generated child pornography aimed at addressing concerns raised by the Supreme Court when it struck down a similar law last year.

Identity Theft

FTC Hampered by Lack of Funds, Power

The Federal Trade Commission lacks both the authority and resources to fully aid victims of identity theft, an agency official said at an April 3 congressional hearing.

Howard Beales, director of FTC's Bureau of Consumer Protection, told lawmakers that financial institutions currently are not required to notify consumers when a security breach has taken place.

"We don't have the regulating authority to do that," Beales said. "I'm not sure there's any agency that does."

Beales also said that FTC currently does not have a program in place for helping victims of identity theft to clean up their credit rating.

"That's not something we have the resources to do," he said, noting that the agency received 380,000 identity fraud complaints in 2002.

The hearing was jointly held by the House Financial Services subcommittees on Financial Institutions and Consumer Credit, and Oversight and Investigations to review current industry practices and to ensure that proper security procedures and protocols are being implemented.

"Congress must remain vigilant to ensure that existing requirements are implemented appropriately and examine whether new safeguards are necessary," said Rep. Spencer Bachus (R-Ala.), who chairs the Financial Institutions Subcommittee.

Beales told the congressional panel that FTC's primary role in combatting identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act, which directed the agency to establish the federal government's central repository for identity theft complaints and to provide victim assistance and consumer education.

FTC develops 'theft response kit'

Beales said that FTC has developed a business record theft response kit that will be posted on the agency's identity theft web site. The kit includes steps that should be taken in response to an information compromise and a form letter for notifying individuals whose information was stolen. Organizations will be encouraged to print and include copies of the FTC guide, *Identity Theft: When Bad Things Happen to Your Good Name*, with the form letters.

Notification could be costly to industry

Stuart Pratt, president of the Consumer Data Industry Association, said that notifying consumers whenever there is a security breach could be a financial burden to the industry.

"We obviously need to work with Congress so that we're not handling the cost on our own," Pratt said.

John Brady, vice president of merchant fraud control at MasterCard International, added that it may not be appropriate to release information about a security breach in every circumstance. "The message I want to get out is: let's not create a panic here," he said.

David McIntyre, president of TriWest Healthcare Alliance, said his company voluntarily spent about $1 million to correct a major security breach last December.

Confidential files containing the names and personal data of military personnel and their families were stolen from the Phoenix office of TriWest, the central region contractor for the Department of Defense's TRICARE health system.

"For the past three months, this issue has been a critical focus for our company," said McIntyre. "First and fore-

most, we believed it was necessary to alert DOD, as well as the affected individuals, so that they could take action to protect themselves, should the thieves choose to misuse the personal information they illegally obtained."

McIntyre said consumers should be notified about breaches in every "reasonable" circumstance. A new California law serves as a good model for requiring disclosures, he said.

California Senate Bill 1386, signed into law on Sept. 25, 2002, and effective on July 1, amends the California Civil Code to require notice of security breaches involving unencrypted personal information.

California

Legislative Priorities Set for Prevention of Identity Theft

Despite the enactment of many privacy and identity theft protections in recent years, law enforcement officials said April 9 that the state still has far to go in protecting Californians from identity theft.

Authorities United to Defeat Identity Theft (AUDIT) unveiled 10 legislative proposals it is working to enact during the 2003 state legislative session, many of them building on measures that have already been enacted. Not all of the ideas have been introduced as bills so far this year.

One of the top priorities for AUDIT, which includes members of the California Union of Safety Employees, is to strengthen the state's ability to compel out-of-state companies to provide information requested by law enforcement organizations. The union's vice president, Jim Miller, said some companies, including Citibank and Verizon, have not been cooperating with information requests from California officials.

Other proposals

Other proposals include:

- requiring credit reporting agencies and credit grantors to verify data discrepancies in their systems such as misspellings or incorrect numbers (A.B. 1610);
- requiring a biometrics system for the Department of Motor Vehicles that uses fingerprints already collected in DMV's database to confirm the identity of those seeking licenses (A.B. 1305);
- clarifying a measure passed last year (A.B. 1773) that requires identity theft crimes to be prosecuted in the jurisdiction of the victim's residency, not where the information was stolen or used to break the law;
- making possession of birth certificates, Social Security numbers, and other personal information unlawful unless there is a demonstrated need to possess the information;
- expanding a prohibition on the use of Social Security numbers in mailings to the public sector (S.B. 25);
- requiring fingerprinting of people cited for a misdemeanor vehicle code violation when they do not have identification (S.B. 752);
- setting national standards through the American Association of Motor Vehicle Administrators for drivers licenses;
- requiring redaction of personal information such as Social Security numbers in court documents that are reproduced for people, such as the news media, when no lawful need for the information exists; and
- clarifying a bill enacted last year (S.B. 1614) that prohibits schools from using identifiers such as Social Security numbers on school documents. Miller characterized the measures as necessary to build on California's efforts to prevent identity theft.

The first year of the legislature's two-year session ends in September.

Texas

Bill Would Authorize Attorney General to Prosecute ID Thieves

The Texas Senate April 2 passed a comprehensive bill that would protect consumers against identity theft and give the attorney general authority to prosecute ID thieves.

S.B. 405, introduced by Sen. Juan "Chuy" Hinojosa (D), will now be considered by the House. The legislation has been titled the Identify Theft Enforcement and Protection Act.

Under the measure, the state attorney general would have authority to assess hefty civil penalties for individuals convicted of identify theft, Hinojosa said in a statement. The bill also would allow a victim of ID theft to recover attorney's fees from the identity thief and allow cases to be prosecuted in the county where the victim resides or in any county in which the offense was committed.

The measure additionally would require businesses to maintain procedures to protect and safeguard personal identifying information collected or maintained in the regular course of business. Under the bill, a business that accepts a debit or credit card would not be able to use a cash register or other machine to print a receipt that prints more than the last four digits of the cardholder's debit or credit card account number.

"Identity theft is the fastest growing crime in the nation," Hinojosa said. The bill would provide remedy and relief to those Texans who are trying to regain their credit ratings and lives after ID theft, he said.

Other bill provisions would:

- prohibit a consumer credit reporting agency from furnishing a consumer report unless the person to whom the report is furnished provides at least four separate items of identification;
- require a consumer credit reporting agency to follow reasonable procedures in preparing or disseminating information to assure maximum possible accuracy of the information about the consumer to whom the information related;
- prohibit a credit reporting agency from recording a requested change of the consumer's address in a consumer's file until the change is verified with the consumer;
- require a credit card issuer to verify a change of address when it receives within 11 days a request for an additional credit card be sent to the new address; and
- prohibit the state from including electronically readable personal identification information on drivers licenses.

S.B. 405 would require the attorney general to establish guidelines for state and local governmental entities to follow when considering privacy and security issues that arise in connection with requests for public information.

Victim assistance

The Texas Senate additionally approved April 3 S.B. 566, authored by Sen. Royce West (D), that would assist victims of identity fraud. Under current law, a person has no way of knowing if someone who was caught committing a crime used a false identity at the time of the arrest.

S.B. 566 would require local law enforcement agencies to contact a person whose identity has been misused once the true identity of the person has been determined. The bill also would require local law enforcement agencies to notify the identity theft victim that he or she is entitled to an expunction of that criminal record.

News

Securities and Exchange Commission

Three Charged Over E-Mails Purporting to Sell 'Inside' Information

A Baltimore man and two affiliated financial publishing companies were charged April 10 in the U.S. District Court for the District of Maryland with disseminating e-mails that offered to sell purported inside information concerning the award of a government contract (*SEC v. Agora Inc.,* D. Md., Docket No. MJG 03 1042, 4/10/03).

In a release, the Securities and Exchange Commission said it is asking the court to bar the defendants—Frank Porter Stansberry, Agora Inc., and Pirate Investor LLC—from future securities law violations. It also is seeking disgorgement plus prejudgment interest and civil penalties.

"The SEC is overreaching," Agora General Counsel Matthew Turner said in response to the allegations. He pointed out that 1934 Securities Exchange Act Rule 10b-5 proscribes " 'fraud in connection with the purchase and sale of securities.' Not one of the defendants named ever purchased or sold securities," Turner emphasized, adding: "Agora and affiliates are publishers not securities traders."

Unsolicited e-mails

Allegedly, beginning May 14, 2002, Agora, Pirate, and Stansberry disseminated unsolicited e-mails to subscribers of more than 15 Internet newsletters published by Agora. The e-mails, which were authored by Stansberry, offered to sell inside information concerning government approval—to be announced May 22—of a contract that purportedly would yield billions of dollars in revenues for an unnamed New York Stock Exchange-listed company.

According to the SEC, the e-mails stated that the information was obtained from a senior executive of the company and offered to sell a report that named the company, for a payment of $1,000. "Approximately 1,000 subscribers purchased copies of the report yielding revenues of approximately $1,000,000 for Agora," the SEC said.

It contended that the so-called inside information was false "in that even the company did not know when government approval of the contract would be received and that such approval was ultimately not received on May 22 as promised in the unsolicited e-mails and the report."

The SEC was represented by Karen L. Martinez, Thomas M. Melton, and Brent R. Baker, Salt Lake City.

Preventing Cyberattacks

Policy Leadership on Cybersecurity Questioned

President Bush's former cybersecurity adviser criticized the administration April 8 for failing to provide the leadership necessary to ensure the federal government's own com-

puter systems are not vulnerable to a major cyberattack.

In his first congressional appearance since leaving his job earlier this year as the administration's top cybersecurity policy maker, Richard Clarke also was critical of the Bush administration for not appointing a senior official responsible for handling cybersecurity policy.

Clarke's concerns were echoed by Michael Vatis, the former director of the National Infrastructure Protection Center (NIPC), which had been part of the FBI. He said he believed the government's ability to deal with a major cyberattack has "regressed in recent months" following the White House's move to dismantle the President's Critical Infrastructure Protection Board, which Clarke headed, and an apparent unwillingness to appoint someone to formally replace Clarke.

"There's a serious void in Executive Branch leadership on cybersecurity," Vatis said. "That will impede the government's ability to move forward on the issue."

Concerns at DHS

Vatis noted that many of the cybersecurity functions handled by various agencies, including NIPC, have been moved to the new Department of Homeland Security. But both he and Clarke expressed concern that the department has yet to appoint top officials to oversee cybersecurity.

"Unfortunately, the department is not organized to take on the responsibility," Clarke said.

In addition, Vatis said he was concerned that cybersecurity would not get the attention it needs if it is grouped under the new department's critical infrastructure protection division as planned.

Clarke was particularly critical of the Office of Management and Budget for failing to provide the necessary leadership, saying it has attempted to oversee the efforts of federal agencies to secure their computer systems without adequate staff or authority.

Despite the enactment of legislation last year requiring federal agencies to develop plans for securing their computer systems, Clarke advocated the appointment of a chief information security officer to oversee such efforts.

"Until we get a high-quality nationally recognized person with authority and clout, we'll continue to have agencies get Fs" on their efforts to fix vulnerable computer systems, Clarke told reporters after testifying at the hearing.

Mark Forman, the OMB's associate director for information technology and electronic government, said that while agencies still have a lot of work to do, they have made some progress. For example, he noted that for fiscal year 2001 only 40 percent of federal agencies had updated computer security plans. But by 2002, that number had increased to 61 percent, he said.

Pushing private sector

Meanwhile, noting that much of the nation's critical infrastructure is in the hands of the private sector, Vatis suggested that Congress consider legislation to put more pressure on the private sector to secure their critical computer systems. This could include providing tax incentives, requiring companies to obtain cybersecurity insurance or imposing penalties on companies that are negligent in protecting critical systems.

Vatis noted that past efforts to encourage industry action have not done enough, saying, "what we have seen is many companies sweep it under the rug."

Clarke said while he does not favor government regulators telling private companies how to secure their computer systems, he did express support for directing the Securities and Exchange Commission to require companies to report on their cybersecurity efforts or requiring big companies to obtain insurance to cover cyberattacks.

He said insurers would likely require companies to do as much as possible to protect their systems from attack in order to obtain coverage.

Hospital Hacked

Computer Data Stolen from Rural Nevada Facility

Hackers broke into the computer system at the William Bee Ririe Hospital in Ely, Nev., gaining access to an undetermined amount of data, a hospital official said April 9.

Two computer hard drives from the hospital were turned over to the White Pine County, Nev., Sheriff's Office for investigation, and are to be forwarded to the Federal Bureau of Investigation, according to a sheriff's department spokesman.

The data accessed may include employees' Social Security numbers and bank information, the hospital's information technology manager and director, Jim Crosley, said. As many as 190 employees may be affected, although to date, there have been no reported incidents of fraudulent use of that data.

The source has not been traced, Crosley said. He added that the hacker or hackers used a masked IP address.

The incident was discovered early on the morning of March 20, when Crosley witnessed an active computer connection coming from outside the facility, routed through the emergency room and into the payroll department's computer.

Crosley became suspicious because at that hour, 6 a.m., no personnel were in the payroll office. He then removed the network cable from the computer.

Analysis of the computer data indicates the hackers may have been able to access the system as early as March 3, but that cannot be confirmed, Crosley said.

Downloaded computer game

Crosley theorizes that a computer game which was downloaded by hospital employees from the Internet contained a Trojan horse, or code. That code, he said, may have served as a cyberspace beacon, leading the hacker or

hackers to the system and enabling them to gain entry.

Crosley said the hospital's recent log files indicate that between 80 and 200 electronic attacks occur daily.

The incident has resulted in upgraded security measures for the hospital computer system, including installation of new software.

Cases

Restricting Parolees' Computer Access

Two Circuits Address Limitation on Computer Use as Condition of Release

Cite as: *United States v. Holm*, 2003 WL 1844823 (7th Cir., decided 4/9/03) and *United States v. Fields*, 2003 WL 1798976 (8th Cir., decided 4/8/03)

The U.S. Courts of Appeal for the Seventh and Eighth Circuits released opinions within a day of one another that address restricting convicted felons' use of computers and the Internet as a condition of their release. Both circuits agree that such restrictions are appropriate as long as they are reasonably related to the statutory purposes underlying conditions of release, involve no greater deprivation of liberty than is reasonably necessary, and are not overly broad. While the two decisions address convictions for the possession and/or sale of child pornography, the principles they articulate apply to any sentence imposed for using a computer as a criminal instrumentality.

The *Holm* decision

The special condition of supervised release imposed on Holm, who pled guilty to possessing child pornography, was as follows:

> You shall not possess or use a computer that is equipped with a modem, that allows access to any part of the Internet, e-mail service, or other "on-line" [*sic*] service. You shall not possess software expressly used for connecting to online service, including e-mail, or installation disks for online services or e-mail.

Judge Diane P. Wood, writing for a three-member Seventh Circuit panel, finds this restriction is too broad and imposes a greater deprivation on Holm's liberty than is necessary. Notably, Holm had been employed for almost 30 years as an information systems technologist and put forth a convincing argument that prohibiting him from use of computers with network connectivity would seriously impede his ability to find gainful employment upon his release. He also presented undisputed evidence at his sentencing hearing that he had not used any of the computer systems at his place of work in committing his crimes. However, Judge Wood writes that for *anyone*, a total ban on all Internet use would render life "exceptionally difficult," given that today, "the government strongly encourages taxpayers to file their returns electronically, … more and more commerce is conducted online [*sic*], and … vast amounts of government information are communicated via website."

Judge Wood suggests that "various forms of monitored Internet use might provide a middle ground between the need to ensure that Holm never again uses the worldwide web for illegal purposes and the need to allow him to function in the modern world." Two possibilities are subjecting Holm to random searches of his computer and residence and requiring that filtering software be installed on any computer he uses. Accordingly, Holm's sentence is vacated and remanded to the district court for revision.

The *Fields* decision

Unlike Holms, Fields was convicted of selling child pornography, which activity netted him over $22,000 in approximately eight months. His conditions of special release prohibited him from "owning or operating any photographic equipment including … computers, scanners, and printers" and from having Internet service in his residence. Furthermore, he may only possess a computer if he is granted permission by his probation officer and agrees to periodic inspections and other restrictions.

Judge Diana E. Murphy, writing for the three-member panel, finds these conditions to be reasonably related to the statutory factors for supervised release. She explains, "Limits on Fields' use of computers and the Internet are obviously related to the circumstances of his offense—running a child pornography website for profit. The conditions are calculated to deter Fields from repeating his illegal activity and to protect the public from similar conduct."

Citing the gravity of his offense—exploiting young girls for profit by making materials available to child predators—and the less-than-total ban on computer ownership the condition imposes, the court concludes that the conditions do not involve a greater deprivation of liberty than is reasonably necessary. Accordingly, the judgment of the district court is affirmed.

Grand Juries

Attorney Must Produce Client's Billing Computer to Grand Jury

Cite as: *In re Original Grand Jury Investigation re Subpoena Duces Tecum Served upon Mark A. Kaiser*, 2003 WL 1721058 (Ohio App. 3 Dist., decided April 2, 2003)

An attorney is required to comply with a subpoena duces tecum by producing for a grand jury the billing computer of his client, a physician, who was the subject of an ongoing criminal and administrative investigation for Worker's Compensation fraud, drug trafficking, and prescription offenses. The attorney, who was never the target of the grand jury investigation himself, obtained the computer from an office manager in the employ of the client's brother, who was also a doctor. The Ohio Court of Appeals was asked to review an order denying the attorney's motion to quash the subpoena and holding him in contempt for not complying with it.

The court first finds that the attorney failed to carry his burden of showing the unreasonableness or oppressiveness of the subpoena. The attorney claimed that while he had no knowledge of the specific content of the computer records at issue, they had no relevance to the grand jury investigation. However, he also acknowledged that the records "may" contain billing information. The court interprets that acknowledgement to mean that the information contained on the computer could conceivably be relevant to the investigation, particularly in light of the broad scope of a grand jury's investigatory powers. The subpoena therefore was neither unreasonable nor oppressive.

The court also rejected the attorney's assertion that compliance would be tantamount to violating the disciplinary rule prohibiting a lawyer from knowingly revealing a client confidence or secret. The court acknowledged that the computer records constitute a client secret by virtue of their having come into the attorney's possession through his professional relationship with the doctor and because their disclosure could be potentially embarrassing or detrimental to him. The court explains, however, that the ban against disclosing client secrets is subject to four exceptions. The relevant exception requires disclosure "in the context of mandating that attorneys relinquish evidence and instrumentalities of crime to law enforcement agencies." The court concluded that since the computer records and other physical evidence sought in the case may contain evidence of a possible crime, they must be turned over to the grand jury.

The attorney argued unsuccessfully that his compliance with the subpoena would violate the work product doctrine, which protects from discovery documents and tangible things prepared in anticipation of litigation. The court finds that privilege inapplicable because the attorney "put forth no effort to produce the information contained on the computer."

The attorney's Fifth Amendment assertion was also unsuccessful. The computer not only didn't belong to the attorney, he had denied that it contained evidence that would incriminate him. The court therefore finds that the attorney's request for Fifth Amendment protection is without merit, in light of his not having been called to testify against himself in a criminal matter or to offer up his own personal papers and effects.

Sentencing

Increased Time for Using Computer to Send Child Porn OK

Cite as: *United States v. Dotson,* 4th Cir., No. 02-4208, 3/28/03

An undercover law enforcement officer's use of a computer to send an advertisement for child pornography to a defendant served as a sufficient basis for the enhancement provided by Section 2G2.2(b)(5) of the U.S. Sentencing Guidelines ("[i]f a computer was used for the transmission of the material or a notice or advertisement of the material,") the U.S. Court of Appeals for the Fourth Circuit held March 28.

A postal inspector posted an advertisement for videotapes featuring child pornography on an Internet newsgroup. The defendant ordered some of the tapes. When the tapes arrived by mail, the defendant was arrested and convicted of possession of child pornography.

In an opinion by Judge William B. Traxler Jr., the court decided that, if the U.S. Sentencing Commission had intended to require that the defendant be the person who used the computer to transmit an advertisement for child pornography, it could have used language like that in Section 2G2.2(b)(4), which specifically requires that the defendant engage in a pattern of abuse or exploitation of minors. The court agreed with the Seventh Circuit in *United States v. Richardson,* 238 F.3d 837 (2001), that the enhancement is based on the added dangerousness arising from the anonymity provided by the Internet and that this anonymity blankets receivers of ads as well as senders. The court also rejected the defendant's argument that, because there are statutes that directly address usage of a computer in other connections with child pornography, Section 2G2.2(b)(5) exceeded the commission's statutory authority to promulgate sentencing guidelines.

Insufficient Evidence

No Proof of Unauthorized Access

Cite as: *Idaho v. Hargrove,* Idaho Ct. App., Docket No. 28212, 3/27/03

There was insufficient evidence to sustain a conviction under a state unauthorized access law when there was no evidence that the defendant accessed her ex-employer's computer after she left employment, the Idaho Court of Appeals ruled March 27.

The court, in overturning a lower court's finding and its jail sentence, said that as a matter of law, the defendant could not be convicted of the misdemeanor of unauthorized access without evidence that she had accessed the computer at a time when she did not have authorization.

The defendant, Jennifer Hargrove of Idaho, had been employed by an insurance agency affiliated with Farmers

Insurance Group from 1990 to 1999 as a secretary and as a licensed agent. In 1999, Hargrove left her employment and became an agent for Allstate Insurance Agency and took with her a copy of a client list, apparently under the mistaken impression that she was permitted to do so.

After it was discovered that Hargrove used information from her ex-employer's files in order to obtain and serve customers, she was charged with unauthorized access of her employer's computers under Idaho Code §18-2202(3). That section states that a "person who knowingly and without authorization uses, accesses, or attempts to access any computer, computer system, or computer network ... or any computer software, program, documentation or data contained in such computer, computer system, or computer network, commits computer crime."

A magistrate judge of an Idaho district court found that Hargrove "actually went into the computer-data base itself and retrieved information about [her former employer's] clients." The finding was upheld by the district court.

Evidence must show computer was accessed

However, Chief Judge Darrel R. Perry concluded that the evidence presented to the district court was insufficient to sustain a conviction under the unauthorized access law. First of all, there was evidence that the information in question was available in paper form, to which Hargrove had access when she was employed at the Farmers agency. Therefore, the state had failed to prove that the information could only have been obtained from the ex-employer's computer.

More significantly, the court said, even if the information had not been available otherwise, there was no evidence presented by the state to prove that Hargrove had actually accessed or attempted to access the Farmers computer system after she left her employment there.

The ex-employer testified that it was unlikely that anyone could access the computer system from a remote location and he testified that as far as he knew, Hargrove had not visited the office since her separation from service.

Without such evidence, a conviction could not stand, the court said, because in order to make a case under the code provision, it must be shown that the defendant accessed the computer "at a time when she lacked authorization to do so."

Hargrove was represented by Dennis R. Peterson of Petersen & Parkinson, Idaho Falls, Idaho. The state was represented by Attorney General Lawrence G. Wasden (R) and Lori A. Fleming of the Idaho Attorney General's office, Boise, Idaho.

Murder Conviction Upheld

Admission of Computer Animation Was Harmless Error

Cite as: *Cox v. Mississippi*, 2003 WL 1091065 (Miss. Sup., decided 3/13/03)

The Mississippi Supreme Court used the appeal of a convicted murderer as an opportunity to announce the law pertaining to computer animations and demonstrative evidence, making clear that the principles articulated in its decision will be applied prospectively in both criminal and civil cases.

The case below

Robert Cox was convicted of the murder of his wife's long-time lover, whose body was found beside his car, along with a 12-gauge pump shotgun. The top of the victim's head had been blown off.

At trial, Cox advanced the theory that the victim's death was not the result of murder, but suicide. A computer-generated animation created by Cox's expert witness was used to assist the expert in explaining how the victim's alleged suicide could have occurred. Although Cox argued that the animation was used only as demonstrative evidence, i.e., to help the expert explain his testimony, it was admitted as an exhibit and included in the evidence that was given to the jury to consider during its deliberations.

The state's assignment of error

The state in its cross appeal claimed the trial court erred both in admitting the animation into evidence and allowing the jury to take it into the jury room. The Mississippi Supreme Court agrees, but finds that both errors were harmless.

At trial, the expert had testified that since no measurements were made at the death scene, the animation was based on his study of the case, including pictures, investigative reports, the weapon, the crime scene, the vehicles, etc. In response to the state's suppression motion, the court ordered Cox to "provide full and complete disclosure of any and all underlying data and scientific principles relating to 'utilized computer analysis, enhancements and animation' of the proposed suicide video. The disclosure by the defendant must include but is not limited to the mathematics, physics, programming, hardware or software and any supporting documentation or studies used to create or support the animation."

The only additional information Cox supplied in response to the order was the name of a person who purportedly assisted the expert in the generation of the animation. The state argued that the response was deficient because it failed to outline the specific, scientific data including measurements which were used to create the animation; it listed various software programs without accompanying explanation of their application; and it failed to describe the hardware utilized. The state also cited as objectionable the absence of any testimony at trial as to the software or hardware actually used to make the animation or the specific mathematical data used to manufacture the video animation prior to it being shown to the jury. The state relied on the testimony of an FBI Visual Information Specialist Examiner who testified that because of current technologies in computer animation, it was possible to create an anima-

tion showing literally anything as "real," when it was not based on any facts. The examiner concluded, "[A]ny computer animation which was not based on actual, physical measurements from the crime scene was mere speculation." The Mississippi Supreme Court agrees.

The holding

The court adopts the following holdings of several other jurisdictions to support the ruling that to be admissible, an animation must be based on scientific, identifiable, and objective facts:

- The foundation for admission of a computer-generated animation must include specific physical measurements from the scene and testimony as to what software, process and date were used.
- A computer-generated animation is admissible as demonstrative evidence when the proponent shows that the animation is authentic, relevant, a fair and accurate representation of the evidence to which it relates; and its probative value substantially outweighs the danger of unfair prejudice, confusing the issues, or misleading the jury.
- To be admissible, a computer-generated animation must be relevant and fair and accurate, and its probative value must outweigh its prejudicial effect.

The court concludes that while demonstrative evidence is admissible if it is necessary and relevant to a fact at issue, evidence which is admitted for demonstrative purposes only (as opposed to substantive evidence which is evidence offered for the truth of the matter asserted) *should not* be given to the jury for its consideration during deliberations. Accordingly, it agrees with the state's assignments of error. The court finds those errors to be harmless, in light of the jury returning a verdict of guilty.

International

Sweden

Spreader of Multinational Virus Faces Fines, Prison

A Swedish citizen who admitted he created and spread a computer virus detected in at least 40 countries faces fines and a two-year prison sentence for violating Swedish law, Swedish police officials said April 3.

The virus, known as a worm because it bores into a computer's hard drive when activated, is contained in an e-mail attachment. When launched, the worm is mailed to other e-mail accounts, disables virus software, and generates a letter and sends it to selected journalists, explained District IT Crime Specialist Torbjörn Ull. Ull is headquartered in Sundsvall, Sweden, a town about 400 miles north of Stockholm. The suspect, who lives in the town of Härnösand, about 30 miles north of Sundsvall, admitted to police he created and spread the virus, Ull said.

The e-mail attachments, bearing subject lines such as "Spy pics" and "USA always No. 1," capitalize on curiosity related to current military actions in Iraq. Other subject lines promise to deliver illegal screensavers or provide timely news to cat lovers.

Virus attacks, propagates

If launched, the attachment performs a number of actions. First, it re-sends itself to every e-mail address the virus locates on the infected computer's hard drive, not just those located in address books of e-mail programs.

Second, the worm disables anti-virus software installed on the infected computer. The virus author targeted specific anti-virus software products, including those marketed by F-Secure Corp., Sophos Plc., and Symantec Corp.

Third, the virus generates a statement complaining about what the virus author claims to be discriminatory behavior he experienced during eight years in the Swedish school system. The suspect claims he has difficulty speaking in front of groups and unsuccessfully asked school officials to be able to communicate mostly in writing, Ull said. The attachment has e-mailed that statement to national school authorities and selected Swedish journalists and media outlets thousands of times due to another virus command, Ull said.

E-mail bearing the worm is delivered in both the Swedish and English languages, which Ull theorizes has been a key reason for the virus' rapid spread in Sweden. Virtually no major viruses have been written in Swedish, so Swedes were "less cautious" about opening attachments received in the Swedish language from people they know, Ull said.

Law violation

The suspect is accused of violating the country's Dataintrång law (Swedish Criminal Code/BrB 4:9c), which prohibits an individual from distributing worms that cause changes in other people's software without their permission, according to Sundsvall District Prosecutor Christina Brohlin.

The law provides punishment by fine or a maximum of two years' imprisonment. The law does not set fine parameters, but fines awarded by Swedish courts are subject to national rules that in part set award ceilings, Brohlin said. The suspect's age has not been released, but Brohlin said he would be tried as an adult if charged with a crime.

By combining technical skills and traditional police techniques, Ull said he traced the virus to its source and obtained a warrant to search the suspect's dwelling. Computer equipment and storage media were seized.

The suspect has been questioned twice by police but has not been arrested, Brohlin said. Her office has not been contacted by foreign police agencies seeking damages or criminal actions against the suspect, she added.

Cyberstalking

Australian State Responds to Stalkers' Use of Technology

The state government of Victoria has introduced a bill to parliament that would for the first time introduce a specific offense of cyberstalking into Australian law.

"Although all states in Australia have stalking legislation, Victoria is the first state to respond specifically to the developments in technology which are being used by stalkers," Victoria's Attorney-General Rob Hulls told Parliament March 27.

The provisions of the Crimes (Stalking and Family Violence) Bill would apply to a person overseas or interstate who stalks a victim in Victoria and a person in Victoria who stalks a victim overseas or interstate.

Cyberstalking conduct is defined in the bill to include assuming the identity of a person on the Internet, uploading doctored images of a person, tracing a person's use of the Internet and sending obscene, threatening or harassing e-mails.

The victim need not show that the cyberstalking activity caused them harm or made them afraid.

"Certain types of cyberstalking activity can take place without the knowledge of the victim," Hulls told Parliament. "A number of threatening or offensive e-mails may be sent to a person but that person may not log on to their computer for a number of days. A victim may also not be aware that someone has uploaded images or information about them onto the Internet."

The Crimes (Stalking and Family Violence) Bill can be found on the Victorian parliamentary web site at http://www.dms.dpc.vic.gov.au/ under the parliamentary documents link.

In Brief

Internet Fraud

Dramatic Increase in Complaints Reported

The Internet Fraud Complaint Center (IFCC) referred 48,252 cases to federal, state, and local law enforcement authorities last year, almost three times the number of referrals for 2001, according to a report released April 9.

The 2002 report offers a recap of Internet crime "hot spots" by state, statistical information, and victim demographic data gleaned through complaints the IFCC has received and referred through its online web portal.

Total dollar loss from all referred fraud cases was $54 million, up from $17 million in 2001, the report says.

IFCC, which is co-managed by the National White Collar Crime Center and the FBI, found that California, New York, Florida, Texas, and Illinois were the top five states for victims of Internet crime. In cases where the perpetrator had been identified, nearly four in five were male and over half resided in California, New York, Florida, Texas, Illinois, and Pennsylvania.

For the third straight year, Internet auction fraud was the most reported offense, making up 46 percent of referred complaints. Nondelivery of merchandise and nonpayment accounted for 31 percent of complaints, and credit/debit card fraud comprised nearly 12 percent of complaints.

IFCC has developed partnerships with such agencies as the National Infrastructure Protection Center, the Federal Trade Commission, and the U.S. Secret Service.

The report is available at http://www1.ifccfbi.gov/strategy/2002_IFCCReport.pdf.

Charter Subscriber Certificate

❑ **Yes!** I need current and comprehensive cybercrime news and legal information. Begin my one-year print subscription to Pike & Fischer's cybercrime LAW REPORT at the charter rate of $285 — a $50 savings off the normal rate of $335. Plus, send me cybercrime LAW REPORT via e-mail* absolutely free!

Payment Options

❑ Payment Enclosed
❑ Bill me ($20 service charge added)
❑ Charge my:

❑ Visa ❑ MasterCard ❑ American Express

Card number **Exp. Date**

Signature

cybercrime LAW REPORT

Subscribe today and save $50!

- There's no risk in subscribing.
- If you decide within 45 days that cybercrime LAW REPORT is not an invaluable investment, you may cancel for a full refund (the issues you've received are yours to keep). Any time thereafter you may cancel and receive a prompt refund on the remainder of your subscription.

Please provide us with the additional information we need to fulfill your subscription.

Name _____

Title _____ **Firm Name** _____

Address _____

City _____ **State** _____ **Zip** _____

Telephone _____ **E-mail Address** _____

Residents of Maryland please add appropriate sales tax. Canadian residents please add appropiate GST. Make checks payable to Pike & Fischer, Inc. If paying by credit card, your statement will show a charge from Pike & Fischer, Inc.

*Issue will be sent as a pdf attachment.

Published by Pike & Fischer, Inc.
A subsidiary of The Bureau of National Affairs, Inc.
1010 Wayne Ave, Suite 1400
Silver Spring, MD 20910
Telephone: 800-255-8131 ext. 237
Fax: 301-562-1521
E-mail: pike@pf.com