Network Law Update: March 1995

William J. Cook
Willian Brinks Hofer Gilson & Lione
Chicago
Internet Publication Address:
ftp://coast.cs.purdue.edu/pub/doc/law+ethics/
Cook_William_Network_Law_M95.ps.z

Table of Contents

Network Law Update: March 1995

by William J. Cook[1]

The headline in the New York Times was clear, "Pirated Copies of the Latest Software From IBM, Others Posted on the Internet." The ramifications were simple; the market for a new computer program can be quickly destroyed if it is posted on the Internet. Most new programs will enjoy at least a six month marketing "shelf life." But a million dollar computer program created on Monday, stolen and uploaded to the Internet on Tuesday, can be worthless by Friday. The victim-author-programmer may not even know his new, "heater" program now resides on a publicly accessible, anonymous file server in France. Nevertheless, his (and your) projected six month marketing window has now shrunk to four days.[2]

Understand the scope of the Internet. It currently has 15 million users, 7.5 million of which are in the U.S. It is thought of as one network, but in fact it is at least 59,916 combined networks entering 92 countries. Its growth rate is 160% per year. *(DOD Assist Project).* Much of the traffic on the Internet is E-mail. Just one of the common on-line service providers, America On-Line, handles 1.8 million pieces of E-mail a day. *(AOL SysOp letter 2/15).*

This update focuses on recent underground technology cases, the changing nature of illegal network traffic, and recent developments in liability law that impact on downstream service providers. An update on network investigations is also provided.

On-Line Traffic Problems

Unlicensed Copyrighted Program Traffic

The expansion of BBS's on the Internet has dramatically increased the potential damages resulting from the traffic in pirated computer programs. At a minimum, it has made it very difficult to establish the damage done by uploading a new program into the uncontrolled Internet environment.

The illegal, international traffic in computer programs is extensive. 94% of the computer software in China is pirated software (CT 1/1/95). Pirated software currently accounts for 92% of software sales in Japan, representing a loss of $3 billion (US) to the software industry. In November, 1993, the United States Government wrote a protest letter to a Japanese proposal that Japanese copyright law legalize "reverse engineering" (decompilation) of computer software (NYT 11/22/93). The SPA estimates that computer software piracy cost European industry and government at least $2.9 billion last year, including $431 million in lost tax receipts (WSJ 6/10/93). In Canada it is estimated that nearly half of the software in use is pirated (Globe and Mail 7/24/93).[3]

However, recent cases reflect a willingness of companies to respond to copyright infringement in a network environment.

Sega v. MAPHIA BBS. In 1994, Sega Enterprises sued Chad Scherman and his computer bulletin board system for copyright infringement, trademark infringement, unfair competition (under federal and state law). On March 26, 1994, a federal court in San Francisco issued a temporary restraining order, approved the seizure of copyrighted information and issued an order to "show cause" for a preliminary injunction against Chad Scherman and the MAPHIA BBS for illegally trafficking Sega computer video games, including "pre-release" place. The court dismissed this with the observation:

> Even if defendants do not know exactly when games will be uploaded to or downloaded from the MAPHIA bulletin board, their role in the copying, including provision of facilities, direction, knowledge and encouragement, amounts to contributory copyright infringement. *(Citing Playboy v. Frena, 839 F. Supp. 1552 (M.D. Fl. 1993)).*

The court also rejected Scherman's "fair use" defense, noting that he did not have an authorized copy of the Sega games and that the downloaded Sega games had a direct adverse impact on Sega's sales. Scherman's argument that there were 45,000 bulletin boards like MAPHIA in the U.S. was not well received by the court. Instead, the court used Scherman's statement to support its conclusion that unauthorized copying of Sega's video games by bulletin boards would have a widespread and substantial adverse effect on Sega's market for its copyrighted video games.

Scherman claimed that he did not profit from the illegal traffic. But, the court noted that Scherman profited from direct fees received from BBS users and from a barter arrangement for downloading privileges. The court also noted that Scherman profited indirectly from the increased prestige of the MAPHIA BBS, which in turn increased the number of BBS users.

The Court affirmed the seizure of Scherman's computer and memory devices, among other things. The BBS memory was copied and returned to Scherman, but the Sega games were deleted. *Sega Enterprises Ltd. v. MAPHIA BBS, 30 U.S.P.Q. 2d 1921 (N.D. Cal. 1994). (See also Cyberlex @aol.com).*

Playboy v. Frena. On July 26, 1993, Playboy Enterprises sued George Frena and his computer bulletin board system for copyright infringement and trademark infringement. On December 9, 1993, a federal district court in Jacksonville, Florida held George Frena d/b/a Techs Warehouse BBS had infringed Playboy's display and distribution rights in its copyrighted photographs, infringed Playboy's trademark by identifying certain files as PLAYBOY and PLAYMATE, and engaged in unfair competition by removing Playboy's text from the photographs and by not identifying Playboy as the source of the photographs.

The court found liability even though Frena maintained that he never uploaded any of the Playboy photographs onto the BBS and that he had removed the photographs and kept additional photographs from being uploaded once he was put on notice of the problem by Playboy. The court observed:

> It does not matter that Defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement. Intent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement; rather, innocence is significant to a trial court when it fixes statutory damages, which is a remedy equitable in nature.

839 F. Supp. at 1559. The court added that the display right is broad and precludes unauthorized transmission of the display from one place to another by a computer system. *Playboy v. Frena, 839 F. Supp. 1552 (M.D. Fl. 1993).*

Playboy Enterprises v. Maxey d/b/a Event Horizons. A civil settlement in a similar case was reached the year before. There, Playboy sued Event Horizons BBS when the BBS uploaded GIF (Graphic Image Format) copyrighted photographs from Playboy magazine and distributed the graphics on the BBS. On that copyrighted musical compositions, including "Unchained Melody," were being uploaded to and downloaded from Compuserve's MIDI Forum BBS. Frank Music alleged that Compuserve's control over the nature and content of the BBS and their knowledge of the activities on the BBS makes them liable for $100,000 in damages for each infringement. *Frank Music v. Compuserve (MIDI Forum) (E.D.N.Y. 11/93)*.

California Dreamin' BBS et al. On October 5, 1993, WordPerfect announced that it had reached a civil settlement with a Texas company that did its beta testing and with a Toronto BBS known as "California Dreamin'." WordPerfect stated that they had observed new WordPerfect products on the Toronto BBS and had conducted an investigation to determine which of their beta test companies were releasing the information. *(WordPerfect Information Release, 10/5/93)*.

Riggs II. The electronic distribution of information was also involved in the Riggs II case in Chicago. There, in pre-trial motions, the EFF claimed that prosecution of Craig Neidorf, editor of an electronic publication known as PHRACK, for publishing a text file of information belonging to BellSouth, violated his First Amendment rights. In rejecting this motion, the court ruled that no First Amendment protection existed for the publisher of a computer newsletter who knowingly published stolen proprietary information about a telephone network. In denying Neidorf's First Amendment claim, the court stated:

> Neidorf's violation of criminal law is not excused simply because he provided the public with interesting information.
>
> In short, the court finds no support for Neidorf's argument that the criminal activity with which he is charged in this case is protected by the First Amendment. Interpreting the First Amendment as shielding Neidorf from criminal liability would open a gaping hole in criminal law; individuals could violate criminal laws with impunity simply by engaging in criminal activities which involve speech-related activity. The First Amendment does not countenance that kind of end run around criminal law.

U.S. v. Riggs and Neidorf II, 743 F. Supp. 556, 561 (N.D. IL. 1990).

Criminal Prosecutions of Copyrighted Software Traffic

As in the case of criminal prosecutions under the National Stolen Property Act (discussed above), prosecution of illegal copyright traffic under the federal wire fraud statute has recently received rough handling.

Kenadek. In August, 1994, Richard D. Kenadek, the system administrator of the Davy Jones Locker BBS in Millbury, Mass., was indicted by a federal grand jury on federal wire fraud and criminal copyright infringement charges. The indictment alleges that Kenadek's BBS carried copyrighted Lotus and Symantec computer programs which were made available free of charge to BBS subscribers that paid their $99 per year membership dues to Kenadek. *U.S. v. Kenadek, (E.D. Mass. 8/94) (WSJ 9/27/94)*.

This indictment is still pending at the time of this update, but he is reportedly attempting to negotiate a plea agreement with the government. However, these negotiations may be adversely affected by the result in the **LaMacchia** case.

LaMacchia. In 1993, a 20-year old MIT science major, David LaMacchia, indictment. The court held that prosecutions should be evaluated under the new copyright statute that requires evidence that the defendant acted "for purposes of commercial advantage." The court also cited the Supreme Court's decision in Dowling v. U.S. in support of its decision limiting the scope of criminal prosecution under the wire fraud statute. *U.S. v. LaMacchia (E.D. Mass. 1994) (Indictment dismissed 12/28/94)*.

On January 27. 1995, the U.S. Attorney in Boston announced that the government would not appeal the court's ruling, but would instead cooperate with the Justice Department's legislative effort to criminalize willful, multiple copyright infringements even in the absence of commercial motive on the part of the defendant.

Theft of Proprietary Information and Privacy

Computer networks are increasingly being used to steal information and privacy and the burglar tools have very strange names: sniffers, sweepers, trojan horses, back doors, snoopers, and spoofers. *(DOD Assist Project).* Real-time interception of data on the network violates wiretapping laws. It creates criminal[4] and civil liability.[5] Even the *possession* of electronic wiretapping technology carries criminal penalties.[6]

Russian Hackers. On February 6, 1995, it was reported that Russian computer hackers had successfully broken into computers of U.S. banks, securities firms and corporations on behalf of transnational criminal organizations. The Russian hackers, made up of former members of the Soviet military-industrial complex, used "sniffers" and "Trojan horses" to overcome computer security "firewalls" built by U.S. companies to gain access to corporations from the Internet. About $300 million in untraceable computer transfers vanished between December, 1994 and February, 1995, from banks and securities firms based on the East and West coasts of the United States. *(WT 2/6/95).*

U.C.S.D. Christmas Intrusions & Mitnick. On December 25, 1994, computer hackers, using Internet access, broke into the University of California Supercomputer Center in San Diego for 28 hours. During this period they allegedly copied 20,000 files containing unpublished software, computer security related correspondence and research into cellular telephone security. *(SJM 1/28/95, Newsweek 2/6/95).*

Kevin Mitnick, 31, a fugitive after a guilty plea to computer charges in Los Angeles in 1989, was arrested on February 15, 1995 after security experts tracked him down in connection with the U.C.S.D. Christmas intrusions. *(CT 2/16/95).*

MOD. The "look and feel" of hacker reform is not always clear. On January 12, 1995, Mark Abene was released after 10 months incarceration. He attended a welcome home party thrown by New York's "radical chic" in his honor. One news article reported on the party "Unrepentant computer thief gains hero status." The article detailed his reception attended by Manhattan artists, professionals, advertising agency designers and a flutist from the underground band Foamola. *(CT 1/15/95).*

Earlier, in July, 1993, Abene and four other members of the MOD (Masters of Deception) computer hacker group had admitted violating the Computer Fraud and Abuse Act.[7] In pleading guilty they acknowledged entering and disrupting telephone switching computers of four Regional Bell Operating Companies, IT&T, and Martin Marietta; stealing and altering credit information on individuals charge. According to prosecutors, only 2 members of MOD (John Lee and Julio Fernandez) made any money from their misdeeds - $800 from another hacker for phony information on how to break into the TRW system. *U.S. v. Fernandez, 1993 WL 88197 (S.D.N.Y., 5/6/93).*

LOD. The actions of the MOD hackers tracked the actions of the Legion of Doom hackers between 1987 and 1989.

Evidence in the LOD case disclosed that from September 1987 to July 21, 1989, members of their group laid siege to the BellSouth data network, breaking into the proprietary BellSouth network and stealing proprietary information, long distance services and data network services. They also compromised BellSouth's login and password files, as well as connect addresses (i.e., access information).

BellSouth responded to the LOD activities by forming a 42 man 24-hour a day investigative task force that engaged in real time monitoring of their data network in order to protect their network and to isolate and identify the intrusions which threatened their network. BellSouth's use of dialled number recorders (DNR's) on telephones used by the LOD quickly established the interaction of the members and formed critical evidence for the conspiracy allegations brought by the government. To support the government investigation BellSouth released parts of its internal investigation (not including the data monitoring) to law enforcement. BellSouth estimated its revenue losses to be approximately $233,880. The company also spent approximately $1.5 million to identify the intruders into their systems and roughly $3 million more to resecure their network.

As a result of the BellSouth investigation and the assistance of the Secret Service, five members of the Legion of Doom hacker organization were convicted and received criminal sentences. Robert Riggs, 22, was sentenced to 21 months in prison, ordered to pay restitution in the amount of $233,880, and placed on supervised release for two years. A condition of Riggs' sentence was that he not "own personally or directly have control over a computer of any type for [his] own personal use during the period of supervised release." Adam Grant, 23, and Frank Darden, 24, were sentenced to 14 months in prison, including 7 months in a half-way house. They were also ordered to pay $233,880 in restitution. Salzman was sentenced to 6 months incarceration in a half-way house in San Francisco. "Fry Guy," 15, was sentenced as a juvenile in Indianapolis. *U.S. v. Grant, Darden and Riggs, 1:90-CR-31 (N.D. Ga. 1990) aff'd U.S. v. Riggs, 967 F.2d 561 (11th Cir. 1992). U.S. v. Riggs and Neidorf I, 739 F. Supp. 414 (N.D. Ill. 1990). U.S. v. Riggs and Neidorf II, 743 F. Supp. 556 (N.D. Ill. 1990). U.S. v. Salzman, (N.D. Fl. 1990), U.S. v. John Doe a/k/a Fry Guy, (S.D. Ind. 1990).*

Poulsen I. In 1989, Kevin Poulsen was indicted on computer espionage and wiretapping charges in San Francisco. The evidence allegedly establishes that Poulsen was able to enter the Pacific Bell data network and use the telephone company's own equipment to eavesdrop on private conversations and unclassified military computers. When substantial evidence resulting from the search of a locker was excluded by a federal judge in San Francisco, an interim appeal was taken by the government. On December 8, 1994, charges were reinstated after the Ninth Circuit ruled that evidence seized from a locker that had been used by Poulsen could be admitted in evidence. *U.S. v. Poulsen I, CR 89-21133 (N.D. Ca. 1989) reversed 41 F.3d 1330 (9th Cir. 1994).*

Poulsen II. On April 21, 1993, Poulsen was again indicted. This time a federal grand jury in Los Angeles charged him with computer fraud, interception of wire communications, mail fraud, money laundering and

Hawaii.

In June, 1994, Poulsen pleaded guilty to seven counts of the indictment. Sentencing is currently being delayed due to continued activity on the San Francisco case, discussed above. _U.S. v. Poulsen II_, *(C.D.Ca. 4/21/93 and 6/14/94). (See also Cyberlex @aol.com).*

Wang and Eubanks (Borland/Symantec Case). E-mail can be used to steal and transfer stolen information. Eugene Wang allegedly used his MCI E-mail account at Borland to transfer Borland trade secrets to his future employer, Gordon Eubanks at Symantec. This material included Borland's product design specifications, product development strategies, sales data, and information regarding a prospective contract for which both companies were competing.

Borland's internal investigation rapidly focused on Wang's E-mail traffic to Symantec in the days before he resigned. They were able to recover copies of the Wang E-mail from their own computers and from Wang's MCI E-mail account. This material was then given to law enforcement and was later used to obtain search warrants for Wang's premises. Additional incriminating evidence was allegedly found at this location in September, 1992.

After the warrants were executed, Borland obtained a temporary restraining order. The order barred Symantec from using any of Borland's trade secrets or confidential information and required Symantec to return any proprietary information taken from Borland.

On March 4, 1993, Wang and Eubanks were charged under California law with conspiring to steal trade secrets, conspiring to unlawfully access Borland computer data, and conspiring to receive stolen trade secrets, in addition to various substantive acts of unlawful access and receiving stolen property.

It is anticipated that Wang's and Eubanks' defenses will include a challenge to the trade secret nature of the information involved and the assertion that Borland improperly recovered Wang's E-mail in violation of California's privacy act.[8] An interim appeal has delayed resolution of this matter. _People v. Wang and Eubanks_, *(Indicted 1993, Santa Cruz County, CA)*.[9]

Lopez-VW Investigation. The international computer network of General Motors was allegedly used by Jose Lopez and his associates to steal and transport information from the United States to Germany. Since March 1993, GM and its German subsidiary, Adam Opel A.G., have been battling Volkswagen over the circumstances surrounding the defection of Jose Lopez, GM's former head of worldwide purchasing.

GM has accused Lopez and a group of seven former GM employees of taking proprietary information with them. They maintain that in the months preceding their departure from GM in March 1993, Lopez and his allies allegedly used GM's internal, international computer network to collect confidential GM strategy data and proprietary information on computers in Germany. The information included, for example, 90,000 computer print-out pages of component price data, some 10,000 GM proprietary documents including secret construction plans, internal cost calculations, and purchasing lists.

Search warrants executed by German authorities against the homes and residences of Lopez's allies surfaced incriminating evidence. An additional raid at the VW Wolfsburg headquarters resulted in seizure of large volumes of documents and computer disks, along with close to 30 personal computers. *(Computer Fraud and Security Bulletin).*

In 1985, S.O.S. sold computerized accounting hardware and software products to companies. Payday was licensed to use S.O.S.'s software (object code) to provide computerized payroll and financial services to the entertainment industry. S.O.S. would not release the source code to Payday.

During 1985, two S.O.S. programmers, Bacchus Chu and Eiichi Koyama, left S.O.S. but continued as outside consultants. As outside consultants, they were authorized limited access to S.O.S.'s computer systems and source code. As Chu's and Koyama's consulting business expanded, Payday hired them with the understanding that they would obtain the S.O.S. source code for Payday.

When S.O.S. refused to release the source code, Chu and Koyama resorted to self-help. S.O.S. discovered that Koyama had entered their offices without authorization and made an unauthorized copy of some of the S.O.S.'s source code. Anticipating further problems, S.O.S.'s system administrator changed the passwords on company computers and began monitoring for outside intrusions. A few days later, Chu and Koyama successfully hacked into the S.O.S. computers by circumventing the password program. S.O.S.'s system administrator responded by again modifying the computer system to eliminate further intrusions.

At trial, Payday convinced the court that their license from S.O.S. authorized access to the source code. However, the appellate court reversed the trial court, noting the "self-help" methods used by Chu and Koyama to obtain the source code. The appellate court observed that Chu and Koyama had obtained information without S.O.S.'s approval through the use of "software piracy" and ruled that the trial court had erroneously concluded that a licensee of a trade secret could not be an infringer under these circumstances. <u>*S.O.S. Inc. v. Payday, Inc*</u>*, 886 F.2d 1081 (9th Cir. 1989)*.[10]

Shadowhawk. In February, 1989, a Chicago youth with the hacker handle "Shadowhawk" was tried, convicted and sentenced to prison for violating the federal Computer Fraud and Abuse Act, 18 U.S.C. §1030. Shadowhawk was able to penetrate poor security on one of AT&T's dial-in ports in Illinois and gain access to the company's internal data network. Once on the network, he disguised his computer as an AT&T "gateway" computer and thereafter attacked company computers from the inside to steal source code from Bell Labs in Illinois and New Jersey, from a NATO missile support site supported by AT&T, and from an AT&T computer located at Robbins Air Force Base in Georgia. In total, he stole copies of AT&T trade secret source code worth $1.2 million and caused $174,000 worth of damage between July and September, 1987.

The initial investigation was conducted by AT&T corporate auditors and members of technical staff at AT&T Bell Laboratories. They were able to recover stored audit trials of several of Shadowhawk's intrusions and thereafter identify the hacker's location through the use of "trap and trace" technology and DNR's. The subsequent involvement of law enforcement resulted in a search warrant at the hacker's home and the recovery of the stolen source code. Shadowhawk was sentenced as a juvenile to nine months detention and ordered to make partial restitution. <u>*U.S. v. Shadowhawk*</u>*, 88 CR 673 (N.D. Ill. 1988)*.

Is On-Line Information Property? Two Views of the N.S.P.A.

Civil courts have had little difficulty finding that computer software is tangible property for various purposes, <u>*South Central Bell v. Barthelemy*</u>*, 94 C 0499 (La. 1994)* (BellSouth telephone switching software is taxable addressed by Judge Nicholas Bua of the U.S. District Court in Chicago in *U.S. v. Riggs*. *Riggs* involved the transfer of alleged trade secret information via computer networks from Georgia to Illinois and on to Missouri. The trade secret involved was a computerized E911 text file describing Southern Bell's E911 network.

BellSouth's internal investigation, conducted for the protection of their own network, disclosed that Riggs had "hacked" into a BellSouth administrative computer and then gained access to the broader BellSouth data network. Riggs located and downloaded BellSouth's proprietary E911 file that described the operation of their E911 system. Riggs thereafter electronically transferred the stolen file from Georgia to a BBS. It was subsequently downloaded electronically from the Illinois BBS by Craig Neidorf at the University of Missouri.

Before trial, Judge Bua rejected arguments by the Electronic Frontier Foundation that computer data is not "property" as defined in the N.S.P.A. However, the case was later dismissed when it was learned that Ohio Bell had publicly disseminated the E911 text file as part of a marketing venture in the Ohio region. As a result, even though the file was stolen by Riggs, the case against Neidorf was dismissed because the information was not, in fact, a trade secret. *U.S. v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990)*.

Brown. A contrary opinion about the N.S.P.A. was expressed several months later by the Tenth Circuit in *U.S. v. Brown*. There the computer source code was stored on paper and/or on magnetic media, but there was no evidence of how the source code moved from Georgia to New Mexico. In deciding the case, the court observed that the computer code was not pure intangible property not covered by the "goods, wares, [or] merchandise" language of 18 U.S.C. § 2314. Their decision is contrary to the holding in *Riggs* and other circuits, as described in *Riggs*. *U.S. v. Brown, 925 F.2d 1301 (10th Cir. 1991)*.

Encryption - Unlicensed Export of Patented and Controlled Programs

The instantaneous, international nature of Internet traffic has raised special problems with respect to export controls. While the end of the Cold War has dramatically reduced export controls, a number of sensitive technologies still are controlled. These include types of missile technology, nuclear technology, chemical and biological technology, plus various types of telecommunications technology.[11] Of these "tech data" groups, the continuing control on encryption technology is clearly the most controversial.[12] And the international border is where the telephone line plugs into the modem on the PC.

EFF Action Against Encryption Controls. On February 21, 1995, the EFF filed a lawsuit on behalf of a San Francisco area programmer and against the State Department challenging the validity of U.S. export restrictions against encryption systems. The case filed in federal court in San Francisco alleges that the U.S. export control laws are unconstitutional because they violate the first amendment rights of computer programmers; the export scheme is not subject to prior court approval; and are too vague to be enforceable. The EFF information release argues that the Internet should be used for the open exchange of information in this area and cites the example of the PGP code. *Bernstein v. U.S. State Department, C95-0582-MHP (N.D.Cal.)*.

Cryptography." Included on the disk is source code, including instructions for the Data Encryption Standard (DES) and Pretty Good Privacy (PGP) (see below). Karn argued the restrictions were meaningless because the same information can be obtained in standard cryptographic textbooks that can freely be exported and the same software is already freely available around the world. *(NYT 10/17/94 & Cyberlex @aol.com 10/94)*.[13]

Zimmerman Investigation (PGP Code). In September, 1993, a federal grand jury in San Jose, California began an investigation to determine Philip Zimmerman's role in placing the PGP program on the Internet and thereby exporting this encryption program overseas. The problem began in 1991 when Zimmerman wrote a "military grade" encryption program called Pretty Good Privacy, or PGP. His proclaimed goal in writing the program was to "inoculate the body politic from the danger of government prying." It is alleged that, after PGP was created, it was placed on the Internet by a friend of Zimmerman's and exported from the United States without an export control license from the State Department. Zimmerman has not disclosed the name of the friend that placed the PGP program on the Internet.

Zimmerman's actions have also generated patent infringement questions. Zimmerman may have dramatically exceeded the scope of his limited license from RSA when he incorporated one of their patented RSA Data Security cryptographic algorithm patents into PGP. Zimmerman claims that he has not infringed the RSA patents because he has not profited from the PGP program and because the on-line documentation for the PGP suggests that users contact RSA about a license on the patent. Nevertheless, the PGP text file discussing the potential patent infringement consequences makes it clear that Zimmerman deliberately used the RSA patents without a license as a type of political statement. *(WSJ 4/28/94)*.[14]

Hoffman. While not a network transfer case, <u>U.S. v. Hoffman</u> is another example of the export of computerized high technology. In <u>Hoffman</u>, between September, 1986 and October, 1989, Ronald Hoffman, a former employee of a Los Angeles software company, illegally exported military application software from the United States without the required State Department export license.

The trial evidence established that Hoffman received $636,000 for transferring military application CONTAM 3 computer software technology from the United States to Nissan, Toshiba and Mitsubishi in Tokyo without the required export license. CONTAM 3 can identify intercontinental ballistic missiles by their exhaust plumes and distinguish "ours" from "theirs." The computer program additionally has applications in the design, engineering and development of spacecraft, launch vehicles, guided missiles and rockets - all uses controlled by the State Department and the Defense Department. Earlier versions of the CONTAM technology also allegedly had commercial satellite development uses that would make it "dual use technology" licensed by the Commerce Department. The portion of the information passed by Hoffman allegedly dealt solely with the weapon system program.

During trial, Hoffman argued that CONTAM 3 was in the public domain. However, the Court held that CONTAM 3's unique combination of computer programs to achieve unique capabilities was a trade secret and not in the public domain as defined in the Arms Export Control Act. <u>U.S. v. Hoffman</u>, *10 F.3d 808 (9th Cir. 1993)*

Hanover Hacker Case. The best known Internet intrusion was documented in Cliff Stoll's book, *The Cuckoo's Egg*. In March, 1989, West German authorities arrested hackers and charged them with a series of intrusions into

Cuckoo's Egg by Cliff Stoll, Doubleday 1989.

Defamatory Network Traffic

Stratton. A recent network defamation case was filed in N.Y. on November 7, 1994 by Stratton Oakmont brokerage firm against Prodigy for a message contained on Prodigy's Money Talk BBS. The message alleged that Stratton had issued a fraudulent public offering. In December, 1994, the complaint was modified to eliminate one of the defendants when it was determined that the message involved had been written by a computer hacker who had been using a Prodigy account without authorization. This case is still pending. *Stratton v. Prodigy, (N.Y. 11/94)*.

Santa Rosa Junior College. On September 22, 1994, the New York Times reported that Santa Rosa Junior College in California had admitted liability to two female students and a male student as a result of offensive traffic on a male-only computer BBS conference established by the college. The settlement of $15,000 to each student followed the college's June 23, 1994 receipt of the investigative report of the Department of Education's Civil Rights. Their report indicated that the men-only conference on the BBS probably constituted a violation of federal laws insuring equal access and prohibiting sexual discrimination in schools.

According to the article, two of the female students had alleged that they had been the subject of sexually derogatory comments on the male-only conference. A third student, a male who had disclosed the offensive traffic to the females, had alleged that he had been the subject of retaliation from the school when he broke his confidentiality agreement on the BBS and disclosed the information to the female students. *Branham, et al. v. Santa Rosa Jr. College (NYT 9/22/94)*.[15]

Rindos. In 1994, an Australian court awarded an Australian professor a default judgment of $40,000 as a result of an allegation posted on the Internet that his career had been based not on research, but upon his own bullying and self-promotion. *Rindos v. Hardwick, (Australia, 3/31/94) (Computer Lawyer 7/94)*.

P&G E-mail. An employee won a $15 million defamation suit against Proctor & Gamble for defamatory messages posted on the company's internal BBS. *Hagler v. Proctor & Gamble*.

K.C. Stockbroker. Epitope Inc., based in Oregon, has filed suit alleging that a Kansas City stockbroker short-selling its stock (hoping the price would fall) damaged the company by posting derogatory information about Epitope on the Prodigy computer network under a pseudonym. *Epitope v. K.C.*

Pornography on the Networks

Netupski. On March 22, 1995, Raymond Netupski, a resident of Des Plaines, Illinois, was placed on two years probation and ordered to perform 200 hours of community service after pleading guilty to transmitting pornographic audiovisual images via the Internet to a 12-year old boy. The prosecutor said Netupski plea to the misdemeanor charges was based upon his supplying sexual explicit computer graphics through a computer bulletin board. An additional charge of felonious distribution of copyrighted materials in violation of Illinois state laws was dismissed. *People v. Netupski, (CT 3/22/95 & 8/13/93)*

Thomas. Robert and Carleen Thomas were convicted in Memphis, Tennessee in July, 1994, on charges that they transmitted obscenity interstate on their Amateur Action BBS. Jurisdiction in Tennessee resulted when a Postal Inspector in Tennessee logged into the San Francisco BBS in an undercover capacity and accessed the pornography on-line. In December 1994, the federal judge sentenced the Thomases to 2 1/2 and 3 years respectively. *U.S. v. Thomas d/b/a Amateur Action BBS*. *(CT 7/21/94 & Cyberlex @aol.com).*

U.S. Customs "Operation Long Arm." The import of child pornography is controlled by 18 U.S.C. 2252. This statute was recently, successfully brought into play by the U.S. Customs Service's Operation Long Arm. On August 31, 1993, this Task Force, operating mainly out of Miami, Florida, was responsible for the return of six indictments against six U.S. citizens for downloading child pornography and "hard" pornography from computer bulletin boards in Denmark. Search warrants were executed against at least 17 bulletin board systems as part of the investigation. *(U.S. Customs Release 8/31/93).*

Computer Stalking

Archambeau. In May, 1994, Andrew Archambeau was charged with violating Michigan's misdemeanor anti-stalking laws in connection with 20 e-mail messages he sent to a woman he once dated. If convicted of the misdemeanor offense, he could be jailed for one year or fined $1,000. *State of Michigan v. Archambeau, (NLJ 6/20/94)(SJM 5/27/94). (See also Cyberlex @aol.com).*

Threatening Communications

Cyberspace Threat? In February, 1995, Jake Baker was arrested in Ann Arbor on federal charges of sending threats over state lines. Now Baker is facing expulsion and a possible sentence of five years on the federal charges for posting Internet traffic detailing his plan to rape a Michigan women. The case involves three sexually explicit rape fantasies Baker composed and posted on a news group on the Usenet computer network that is distributed via the Internet. One of the stories contained the name of a women student in one of Baker's classes.*(Time 2/10/95).*

Many public policy factors weigh into the evaluation of this case. However, the First Amendment does not protect threatening activity.[16] See also *United States v. Lincoln, 589 F.2d 379 (8th Cir. 1979) (prosecution under 18 U.S.C. §876).*

Password & Access Code Traffic

Mitnick. As noted above, on May 10, 1989, Kevin Mitnick pleaded guilty in Los Angeles to charges that he used a telephone and computer to steal a $160,000 computer security program from Digital Equipment Corporation and that he unlawfully possessed 16 telephone access codes. At the time of his arrest on February 15, 1995, authorities indicated he was allegedly involved with the theft of an additional 20,000 credit card numbers. *U.S. v. Mitnick, (C.D. Calif.).*

MCI Employee. Ivy James Lay, an MCI employee, was convicted and sentenced to 3 years in prison for stealing 50,000 calling card numbers from MCI and other long-distance companies, which were used to make $28 million worth of long-distance calls. Lay, and his co-defendant Frank R. Stanton (who was sentenced to one year in prison), used software developed to trap callingthousands of telephone calling card numbers used to make $140 million in unauthorized long-distance calls. Louran, a member of an international hacker group, pled guilty to conspiracy and wire fraud charges. *(SJM 10/28/94 & Cyberlex @aol.com 10/94)*

Doucette. On August 17, 1990, Leslie Lynne Doucette, also known as "Kyrie," age 36, was sentenced to 27 months in prison by Judge Milton I. Shadur of the United States District Court in Chicago. Her sentence was based upon her role as the head of a nationwide voice mail computer fraud scheme and her unauthorized possession of 481 access codes as part of that scheme. Doucette's unauthorized "access codes" included credit card numbers from Visa, Mastercard, American Express and Discover Card; telephone calling card numbers from AT&T, MCI, Sprint and ITT; PBX long distance access codes; and computer passwords. In pleading guilty, she admitted that she had trafficked these and other access codes on compromised voice mail computers to approximately 152 computer hackers around the United States, resulting in fraud losses totalling $595,941.00. *<u>U.S. v. Doucette</u>, 89 CR 471 (N.D. Ill. 1989)*.

Fraud Schemes for Money on the Internet

Legends Fraud. On December 16, 1994, the U.S. Attorney's Office in Arizona announced that two individuals had been indicted for using Internet advertising to falsely promise victims copies of a limited edition of a card game known as "Legends." Each of the 22 counts of the indictment carries a potential 5 year prison term and a $250,000 fine. *(CCH Computer Law, 12/27/94, No. 135).*

Trademarks on the Internet

knowledgenet.com. KnowledgeNet, Inc. has brought a trademark infringement action in Chicago against D.L.Boone & Co. in Virginia for Boone's use of the name "knowledgenet" as his Internet address for his consultant group. *(Info. Law Alert 2/24/95).*

kaplan.com. An arbitration panel in New York ruled that the Princeton Review has no right to establish an Internet address (kaplan.com) using the name of its chief rival, Stanley H. Kaplan Educational Centers Ltd. The parties agreed to arbitration after suit was filed in U.S. District Court in Manhattan. *(NYT 10/6/94 & Cyberlex @aol.com 10/94).*

mtv.com. MTV brought a trademark infringement action against its former employee, Adam Curry, in an attempt to recover the "mtv.com" Internet address. Curry had used the address as part of his "cybersleaze report" on the rock industry while he was a VJ at MTV. Since leaving MTV, Curry has continued to use the "mtv.com" address as part of new Internet consulting business. Curry maintains that since he registered "mtv.com" with the Internet, it belongs to him and is his address. *(CT 5/16/94).* The court has already ruled in a pre-trial opinion that an Internet address is a valuable commodity. *<u>MTV v. Curry</u>, 867 F. Supp. 202 (S.D.N.Y. 1994)*.

Threats to the Networks Themselves

In addition to the **LOD** and **MOD** activities discussed above, underground technology presented itself in other forms.

DOD Intrusions. On February 3, 1994, significant portions of the Internet were attacked by a hacker who potentially compromised Defense law for computer tampering. After a client became engaged in a payment dispute with MJL, the men allegedly infected the client's computer with a virus that would automatically shut down the business's access to information. *State v. Lafaro, (NYT 11/23/93).*

Morris Worm. On November 2, 1988, Cornell student Robert T. Morris, Jr. introduced a computer "worm"[17] program into the Internet. Once the program was launched, Morris had no control over the worm as it exploited a weakness in the UNIX file transfer program that rapidly spread the worm to 2,600 computers on the Internet. While the worm program did not damage programs or data, it did effectively "freeze" computers connected to the Internet computer network. As a result, the Internet computers experienced substantially delayed operating times and delayed service for 12 hours. The cost of repair at each individual site was between $200 and $53,000, depending upon the amount of time needed to clean and restore the system. *U.S. v. Morris, 928 F.2d 504 (2nd Cir. 1991).*

Versaggi. Robert Versaggi was found guilty of computer tampering in the second degree. His defense that he did not "alter the computer's program" as required by the statute was rejected. The court held that evidence established that Versaggi accessed his employer's computer systems and used commands on the computer system to cause the system to shut itself down. This action was sufficient, in the Court's view, to establish a violation under the state statute. *People v. Versaggi, 608 N.Y.S. 2d 155, 629 N.W. 2d 1034 (N.Y. App. 2/14/94).*

Vicarious Liability

Who is responsible? In the past victims have been forced to chase "shallow pockets" - underage hackers or fugitive industrial spies -in an attempt to recover damages. This can be expensive and frustrating. However, recently courts have been taking a broader view of liability for network traffic. The focus has shifted to the responsibility of telecommunications service providers and other companies involved with network traffic.

Vicarious liability may result when an on-line service provider has the right to review and control network traffic, and is on notice of specific, damaging traffic. In such situations, the on-line service can be held liable for resulting damages.

Sega v. MAPHIA BBS. In the Sega case, discussed above, Chad Scherman was found liable for traffic on his MAPHIA BBS even though he maintained that he was unaware of each specific illegal upload. The court was satisfied that his general knowledge of the traffic was sufficient since he encouraged the uploading and downloading practices. *Sega Enterprises Ltd., et al. v. MAPHIA BBS, et al., 30 U.S.P.Q. 2d 1921 (N.D. Cal. 1994).*

Playboy Cases. As noted above, bulletin board operators were also found liable for copyright infringement when it was established that they were on notice of copyrighted Playboy photographs on their BBS systems. *Playboy v. Frena, 839 F. Supp. 1552 (M.D. Fl. 1993)* and *Playboy Enterprises v. Maxey d/b/a Event Horizons, 92-311PA (D.Ct. Oregon) (Filed 4/20/92).*

Cubby v. Compuserve. While the *Sega* case and the *Playboy* cases represent an expansion of liability to the providers of illegal network traffic, the landmark case of *Cubby v. Compuserve* still is the leading decision in the area.

numerous newspapers and magazines. As such it was not responsible for defamatory information carried on individual bulletin boards unless it was shown that Compuserve was actually aware of the presence of the defamatory message on the bulletin board. *Cubby v. Compuserve, 776 F. Supp. 135 (S.D.N.Y. 1991)*.[18]

In so holding, the Court noted that Compuserve had no contractual relationship with the bulletin boards on its service and that an intermediate entity known as CIS had accepted the contractual responsibility to edit the bulletin board that had carried the defamatory messages involved. Judge Leisure also noted that Compuserve received no compensation from the bulletin board and had no opportunity to review the contents of the bulletin board before the defamatory comments were published.

While the tenor of the decision in *Compuserve* suggests that the Court might have ruled against the bulletin board and CIS, their liability was not before the Court and was not decided.

A Victim is Not a Racketeer. A federal court in New York held that AT&T was not a racketeering activity under federal laws in view of the fact that it too was a victim of a fraud scheme perpetrated by one of its employees. *CA Westel de Venezuaela v. AT&T, (S.D.N.Y. 10/94).*

Investigations

Use of Undercover Agents

The use of undercover agents to obtain evidence in a networked environment has recently been approved by courts in the *Sega v. MAPHIA BBS* case and the *Playboy v. Frena* case.

In the *Sega* case, the defendant Scherman also raised a defense under the Electronic Communications and Transactional Records Act (ECTRA), 18 U.S.C. 2701(a), which prohibits a person from "intentionally access[ing] without authorization a facility through which an electronic communication service is provided." Scherman alleged that Sega's use of an informant using a pseudonym to collect evidence of the activities on the MAPHIA BBS was unlawful and therefore could not be used to establish the copyright violation. The Court ruled that because MAPHIA BBS was a public board normally accessed by members using an alias or pseudonym, Sega's access in the same manner did not violate the ECTRA. The Court also noted that the ECTRA itself permits a user of an electronic service to access the system to retrieve communications meant for that user.

A variation of the "unclean hands" defense raised in *Sega* and *Playboy* was raised in *Olan Mills Inc. v. Linn Photo Co.*. There Olan Mills' undercover investigator had to sign "hold harmless" agreements at Linn Photo Co. which allegedly absolved Linn of all copyright infringement claims. The court rejected this claim, noting that the defendant's infringing activities could not be protected by such a self-serving warning. *Olan Mills Inc. v. Linn Photo Co., 30 U.S.P.Q. 2d 1798 (8th Cir. 5/5/94).*

Monitoring

Real time data monitoring has sometimes been used by investigators and law enforcement officials to obtain significant trial evidence. In the

the **Legion of Doom** investigations, see above.

Versaggi. Versaggi's activities, described above, were discovered when his employer in New York used keystroke monitoring equipment to identify and document his actions. The appellate court held that this type of monitoring was the same as a surveillance camera and completely permissible.

Seidlitz. Real time data monitoring has long been conducted by system administrators attempting to protect their networks. An early example occurred in *U.S. v. Seidlitz*. There a former employee, Bertram E. Seidlitz, conducted a remote access theft of a specifically modified WYLBUR source code computer program from the computers of OSI corporation. Seidlitz accomplished the theft by masquerading as an authorized user of the OSI computer. OSI detected the intrusion and used a Milten Spy Function program that automatically recorded Seidlitz's keystrokes (audit history file), to capture critical evidence of his intrusions. When Seidlitz challenged the company's use of the Milten Spy as "an electronic eavesdropping device," the court rejected his claim, noting that the activity was conducted on the company's own computer system, and not on the public switched network. *U.S. v. Seidlitz, 589 F.2d 152 (4th Cir. 1978).*

Employer real time monitoring of employee e-mail is very sensitive since, under some conditions, it may be a violation of the federal wiretap statute, 18 U.S.C. 2511(1)(a), unless the interception is done pursuant to a recognized exemption. *Williams v. Poulas, 11 F.3d 271 (1st Cir. 1993) and Manufacturas Intern. v. Mfrs. Hanover Trust Co., 792 F. Supp. 180, 190.* Exceptions exist when the employees clearly consent to the monitoring in advance or under circumstances where the business extension exception applies. *Williams at 281-82.*[19]

Accessing Stored Communications

Stored audit trails have provided critical evidence in the *Shadowhawk* and **Cuckoo's Egg** cases, referred to above.

E-mail is an especially sensitive issue in this area. Employer review of stored e-mail communications does not violate the Electronic Communications Privacy Act, 18 U.S.C. 2711, even if it has not yet been received by the intended recipient. *Steve Jackson Games v. Secret Service, 816 F. Supp. 436, affirmed 1994 WL 561233 (5th Cir. 1994).*

Forensic Software Examination

Misappropriated computer code is sometimes altered to disguise its origins. When that takes place, it is essential that an expert forensic examination of the source code is conducted. Just such an examination was conducted by Gene Spafford of Purdue, in *Palmer v. Fox Software*. The result was a $22 million jury verdict on May 4, 1994, for an investor in Fox Research, a software development company purchased by Microsoft in July, 1992.

Before trial, defendants David Fulton and Richard LaValley argued that Fox Software computer programs developed after 1986 were completely new and created independently of earlier programs. They maintained that supported their position that Palmer's investment was completely independent of the later programs. This contention was rebutted by Spafford's testimony. Spafford testified that he compared the FoxBASE computer source code (funded by Palmer) with later Fox Software programs and determined that a significant subsequent computer programs and that the earlier version was essentially the starting point - or outline - for the later versions. *Palmer v. Fox Software, 3:92 CV 7339 (N.D. Ohio 1994).*

The fact that the "new" or "revised" program is generated in a different computer language does not alter the results of the forensic examination. Thus, in *GNU Business Information v. Social Secretary, Ltd.*, the substantial similarity between the computer programs resulted in a finding of copyright infringement even though the source codes that were compared were in two different computer program languages. *GNU Business Information v. Social Secretary, Ltd., 91 C 8215 (N.D. Ill., 11/9/93)*

Admissibility of DNR's

Dialed Number Recorders (also known as "pen registers") are an invaluable source of evidence in a computer intrusion or telecommunication investigation. When installed correctly, they record all numbers entered into the telephone system by someone using the public switched network. These devices are specifically authorized by the ECPA. 18 U.S.C. 3121(b) and *U.S. v. Fernandez, 1993 WL 88197 (S.D.N.Y., 5/6/93)*.

While they are clearly admissible evidence, DNR's are not business records and an adequate foundation must be laid before they can be admitted. Thus, in *U.S. v. Beverly*, the Seventh Circuit held that DNR's could be properly admitted into evidence based upon the testimony of a supervising DEA agent who was highly familiar and experienced with DNR's generally, but had not been involved in the installation of the DNR involved in the case. *U.S. v. Beverly, 972 F.2d 351 (7th Cir. 1990) (Unpublished)*.

In contrast, in *Illinois v. Casey* an Illinois appellate court noted that DNR's are part of the investigative process and therefore must be authenticated to be admitted into evidence. The court found that the prosecutor had improperly admitted the DNR's as business records and that an adequate foundation under one of the other rules of evidence was required. *Illinois v. Casey, 225 Ill. App.3rd 82, 587 N.E.2nd 511 (1/23/92)*.

Obtaining Passwords

In *U.S. v. David*, the defendant was cooperating with government agents by giving them drug-dealing information from encrypted files in his computer memo book. During one interview, the agent learned the defendant's password by standing over his shoulder and watching as he typed it. Later, when the defendant stopped cooperating and started destroying information in the notebook, the agent seized it and used the defendant's password to access the remaining information. When this use of the password was challenged as an illegal search, the court rejected the argument and reasoned that the agent's learning the password was like his picking up the key to the container. When the defendant withdrew his consent to give more information from the memo book, the act which required a warrant was looking inside the container - whether locked or unlocked - not the acquisition or even the use of the key. If the agent did not have authority to search the data, then knowing the password would not confer it. Id. at 1391. Conversely, if the agent does have a warrant for the data, she may break the "lock" to search it. Although the agent did nothing wrong by leaning over defendant's shoulder to watch him enter the password, the government clearly exceeded the implicit limits of David's consent when agents used the password to read the whole computer book without David's permission.

Admissibility of "Deleted" Files

In <u>*Prism v. Hospital Medical Records*</u>, the Supreme Court of British Columbia held that a computer expert could testify as to the existence and content of "deleted" computer files. <u>*Prism Hospital Software, Inc. v. Hospital Medical Records*</u>, *S.Ct. British Columbia (1991).*

Scope of Grand Jury Subpoena

In <u>*In re Grand Jury Subpoena Duces Tecum*</u>, *(S.D.N.Y., 2/24/94) (47,027 CCH)*, a federal grand jury subpoena for production of a computer, all computer producible data and hard disk drives, was held to be unreasonably broad in connection with a securities trading investigation. Because the government failed to specify the information needed or the directory files to be searched and refused to modify the subpoena, the court quashed the subpoena.

Scope of Civil Seizure

In <u>*Century Home Entertainment v. Laser Beat Inc.*</u>, *30 U.S.P.Q. 2d 1811 (E.D.N.Y. 3/22/94)*, a federal court in New York held that the seizure, pursuant to 17 U.S.C. 503, of allegedly infringing videotapes and recording equipment was warranted, since plaintiff clearly identified videotapes which it owned, since plaintiff established a *prima facie* case of copyright infringement, and since plaintiff demonstrated good cause to believe that tapes might be destroyed or moved. The defendants claimed that the equipment seized should be released because it could be used for "legal" tape copying. This was rejected by the Court in view of the fact that the equipment had been used for illegal purposes and that defendants should not be immunized simply by citing its potential legitimate use.

A seizure under the Copyright Act was also involved in <u>*First Technology Safety Systems v. Depinet*</u>, *(6th Cir., 12/15/93)*. There the Sixth Circuit held that neither the Copyright Act nor the Copyright Rules allowed seizure of anything other than the infringing copies. As a result, business records also seized from the infringing defendant had to be returned absent a showing that the records were likely to be destroyed.

Civil Actions Against Law Enforcement

The Fifth Court of Appeals held that seizure of a computer, used to operate an electronic bulletin board system, and containing private electronic mail which had been sent to a bulletin board, but not read by intended recipients, was not unlawful intercept under the Federal Wiretap Act. <u>*Steve Jackson Games v. U.S.*</u>, *816 F. Supp. 432, aff'd. 1994 WL 561233 (5th Cir. (Tex.) 10/31/94)*.

On March 12, 1993, District Judge Sam Sparks in Austin decided that: (1) The agents <u>did not violate</u> the provisions of the Electronic Communications Privacy Act (ECPA) by "intercepting" e-mail that was allegedly "in transit" because the e-mail was, in the Court's view, actually a stored communication under the provisions of the ECPA (p. 22); (2) The agents <u>did not violate</u> the Fourth Amendment and they did in fact have probable cause to search the Steve Jackson Games premises and seize the computers (pp. 8-9); (3) The agents <u>did not violate</u> the Privacy Protection Act (PPA) (relating to publishers) at the time the search started since they had no information that the company was involved with publishing at or before the time of the search (p. 18); (4) The agents <u>did violate</u> the PPA, when after the search took place, they learned that the company was allegedly involved with publishing and did not immediately arrange to return copies of the seized materials to the company (p. 19); (5) The agents <u>did</u> violate the provisions of the ECTRA by obtaining a search warrant instead of obtaining a subpoena for "disclosure" of the information on the BBS.

In <u>*U.S. v. Upton*</u>, *763 F. Supp. 232 (S.D. Ohio 1991)*, police officers were lawfully conducting a search pursuant to a search warrant when they overheard the defendant's answering machine receive a call from an individual believed to be involved in narcotics trafficking with the defendant. The officer then seized the answering machine and related tapes. Subsequently they listened to the taped messages on the machine without obtaining an additional search warrant.

As a defense, the defendant claimed that the officers had illegally intercepted "wire, oral, or electronic" communication in violation of the ECPA. In refusing the defendant's defense, the court held that the officers were properly on the site and had not "intercepted" the communications in narcotics trafficking sued the intermediary banks which, pursuant to government direction, had seized the funds transferred in anticipation of government forfeiture actions.

The Second Circuit held that the beneficiaries of the funds transfers were not "customers" within the meaning of the Right to Financial Privacy Act (12 U.S.C. §3412(e)). The court also held that the banks had no liability under the ECPA because they were acting under government direction. Moreover, the court held that there is no liability under the ECPA for the interception of electronic communications in transit or in electronic storage where one party to the communication (here the banks) consented to access. Finally, the court noted that good faith reliance on a court warrant or order is a complete defense under the ECPA. 18 U.S.C. §2520(d). *Industrias Marathon LTDA v. Manufacturers Hanover Trust Co., 792 F. Supp. 180 (E.D.N.Y. 1992).*

Conclusion

As noted above, preserving and protecting copyrights, patents, and trade secrets has never been more important. Companies must aggressively protect their intellectual property rights up to and including litigation in the world-wide Internet environment. Since this litigation may be costly, companies should consider specific insurance coverage.

The language of the coverage should also receive substantial attention in view of current case law. In *Irons Home Builders v. Auto-Owners Insurance, 30 U.S.P.Q.2d 1059 (E.D. Mich. 1993),* a Michigan court held that an insurer had a duty, pursuant to a policy covering personal or advertising injury, to defend an insured against a copyright infringement action alleging that the insured copied a set of house plans and then built houses based upon those plans.

In contrast, the Ninth Circuit has held in *Microtec Research, Inc. v. Nationwide Insurance Co., 35 F.3d 571 (9th Cir. 1994) and Intex Plastic v. United National Insurance, 30 U.S.P.Q.2d 1652 (9th Cir. 1994),* that an insurance policy covering litigation expenses for "advertising injuries" and "piracy" did not provide coverage against suits for copyright and patent infringement.

Comprehensive General Liability Insurance (CGL) can be used to pay the cost of defending various intellectual property claims including copyright infringement, trade secret misappropriation, unfair competition, and patent infringement.[20] Intentional wrongs committed by an insured are not covered because such coverage would be against public policy. However, the type of intent involved may dictate the obligation of the insurer. See *State Farm Insurance v. Flynt, 17 Cal. App. 3d 538, 547 (Cal. App. 1971)* and *Logan v. John Hancock Mutual Life Ins. Co., 41 Cal. App. 3d 988 (Cal. App. 1974).* Other types of insurance that cover failure to exercise due diligence should also be explored. They include Errors and Omissions Insurance and Directors and Officers Liability Insurance.

For a complete discussion of this critical issue see "Strategies for Corporate and Intellectual Property Counsel in Obtaining Coverage for Intellectual Property Lawsuits" *Licensing Law and Business Report, Vol. 17, Nos. 3 & 4.*

[1] © William J. Cook, Chicago, Il., 4/3/95 . Cook is a trial attorney with the intellectual property firm of Willian Brinks Hofer Gilson & Lione in Chicago. Before working at Willian Brinks, Cook was a trial attorney in the U.S. Attorney's Office in Chicago for 16 years. Cook can be contacted at 312-321-4788, F 312-321-4299, COOKER2@aol.com; wbhgl @msc.com (BCook); B.Cook@search.org; or VHGP26A@prodigy.com. This paper can be located on the Internet at ftp://coast.cs.purdue.edu/pub/doc/law+ethics/Cook_William_Network_Law_M95.ps.z

[2] This October 31, 1994 Times article has been more recently echoed by other publications,"Stop! Cyberthief!" Newsweek, February 6, 1995, pp. 36-39 and "Computer Experts See Hackers Gaining An Upper Hand in Fight Over Security," Wall Street Journal, January 24, 1995.

[3] Jurisdiction in a network environment is a difficult issue. An individual in the U.S. that uploads copyrighted software onto the Internet will be responsible for damages caused by further infringement overseas. See, e.g., Zenger-Miller, 757 F. Supp. 1062 (N.D. Ca. 1991). And, in some circumstances, an individual overseas will be responsible for damages caused by infringement. See, e.g., Modern Computer Corp. v. Ma, 32 U.S.P.Q. 2d 1586 (E.D.N.Y. 1994).

However, an American that merely authorizes copyright infringing acts to take place outside the U.S. is not subject to U.S. copyright laws as long as all infringing activities take place outside the U.S. See, e.g., Subafilms, Ltd., 31 F.3d 812 (9th Cir. 1994).

[4] See 18 U.S.C. 2511. See also *United States v. Poulsen I, CR 89-21133 (N.D. Ca. 1989) reversed 41 F.3rd 1330 (9th Cir. 1994) and United States v. Poulsen II, (C.D.Ca. 4/21/93)* (discussed below).

[5] Telerate Systems v. Caro, 689 F. Supp. 221 (S.D.N.Y. 1988) and Technicon Data Systems Corp. v. Curtis 1000, Inc., 224 U.S.P.Q. 288, 292 (Del. Ch. Ct. 1984).

[6] See 18 U.S.C. 2512. The interception and unauthorized viewing of intercepted satellite communications has been recognized by the Fifth, Sixth, Seventh, Eighth, Ninth, and Tenth Circuits as a violation of the federal wiretap law, 18 U.S.C. §2512. *United States v. One Macom Video Cipher II, 985 F.2d 258 (6th Cir., 1993).*

The trojan horse program trafficked by Leonard Rose might also have been prosecuted as a device manufactured to intercept electronic communications under 18 U.S.C. §2512(1)(a), similar to the result in *Cypher II*. *United States v. Rose, 91 CR 214 (N.D.Il. 1991) and JFM-90-0202 (D.Md, 1991).*

[7] 18 U.S.C. 1030, *et seq*.

[8] An internal e-mail control policy is essential for a corporation. In the event of litigation, an insider will claim that his expectation of privacy was violated by the organization's investigation. It is essential that corporate managers, auditors, and security directors be able to point to specific corporate policies that limited the use of e-mail inside the corporation.

[9] Whatever the outcome, critical questions about handling E-mail will be presented by this case: Was Wang's E-mail abandoned on the Borland computers after his departure? Did Wang implicitly consent to Borland's access to his E-mail since he used the company system to send the information? What is Borland's ability to search its own computers for information after those computers were no longer under the control of a departed employee? What is Wang's standing to object to the search of his node of the computer system after his departure?

[10] Many of these cases require that the victim establish the proprietary nature of the information taken. As a general rule, attorneys and system administrators should evaluate their chances of success in litigation based upon the answers to the following questions: Did misappropriation take place (were "adequate" security controls in place based on the anticipated risk)? Does tangible evidence of the theft exist (such as an internal audit trial)? Is the information scientific or technical in nature (versus a mailing list)? What is the value of the information to you or to your competitor? How sound are the licensing and employment agreements that deal with the individual responsible for the theft? Has a complete document search taken place to determine that the information is not, in fact, in the public domain in its current form? How long did you delay before contacting management and/or law enforcement? Will litigation further compromise the technology?

[11] The concept of "export" itself had dramatically changed due to the highly mobile nature of the technology and the people that use it. Thus an "export" of technology can occur when a foreign citizen works for or visits a U.S. plant, or accesses the database of a U.S. plant from overseas, or uses a U.S. supercomputer from overseas. "Exports" of technology also take place when a U.S. citizen carries or transfers technology overseas during his travels or during his international use of E-mail.

[12] See "Data Security, Competitiveness, and Government Controls in Cryptography in the Information Age," Computer Law Reporter, February, 1993, Rosenthal, pp. 1098-1104; "The Clipper Chip and Cryptography Policy: Problems Remain for Exports of Mass Market Software With Encryption Capabilities," Computer Law Reporter, July, 1993, Rosenthal & Miller, pp. 861-867: "Congress Holds Hearings on Encryption, Wiretap Issues," Computer Law Reporter, June, 1994, pp. 697-701.

export controls for encryption technology. According to a former NSA cryptographer who is now a private consultant, "[t]he availability (of) world-wide encryption programs makes export controls a farce."

15 The potential violation of the privacy rights of the male students on the male-only section of the BBS was not addressed in the litigation. It should be noted that the Electronic Communications Privacy Act imposes possible criminal or civil charges on individuals that illegally intentionally access electronically stored communications, i.e., communications on a BBS. See 18 U.S.C. 2701(a)(1) (criminal liability) and 2707 (civil liability).

16 *Electronic Publications and the Limits of the First Amendment*, William J. Cook, January 15, 1992.

17 A "worm" is not a computer "virus." A "worm" is a self-contained program. It looks for a new host to infect, it copies itself to the new host, and it causes a new copy of itself to be executed. A "virus", on the other hand, attaches itself to existing programs. When the program is executed, the virus code is also executed.

18 Other recent cases, referred to as "trade show organizer" cases, may be used in the future as authority for the expansion of vicarious liability to network service providers. In Artist Music v. Reed, 93 C 3428 (S.D.N.Y. 5/17/94), a federal court in New York held that a trade show organizer is not vicariously liable for infringing performances of copyrighted music at booths during the trade show because the organizer lacked the right and ability to control the exhibitors. The Court observed that the organizer had no more control than a landlord did over his tenants. ASCAP had argued that vicarious liability applied, but the Court rejected this claim, noting the vicarious liability test set forth in Shapiro v. Bernstein, 316 F.2d 304 (2nd Cir. 1963).

A contrary result was reached in Polygram Int'l. v. Neveda TIG, 855 F. Supp. 1314 (D.C. Mass. 6/20/94). Judge Keeton of the federal bench in Massachusetts found that a trade show organizer is vicariously liable for infringing performances of copyrighted music at booths during the trade show because they had the right and the ability to supervise the exhibitors coupled with a direct financial interest in the exploitation of the copyrighted materials. However, infringement was not found because the plaintiffs failed to show that the defendant's actions were unauthorized.

19 See also Epps v. St. Mary's Hospital of Athens, 802 F.2d 412 (11th Cir. 1986) (*en banc*) and James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979).

20 See generally on this subject "Insurance Coverage of Intellectual Property Lawsuits," William J. Robinson, 1992.