DON'T CALL IT CYBERLAW (TM)!
(RECENT DEVELOPMENTS IN THE LAW AND POLICY OF TELECOMMUNICATIONS AND COMPUTER DATABASE NETWORKS)

by Anita Susan Brenner, Esq.
301 E. Colorado Boulevard, Suite 614
Pasadena, CA 91101

Once Doonesbury discovered The Internet[1], lawyers were not far behind. It is rumored that in 1985 only one lawyer had Internet access. Questioned about his activities, he complained that business was slow, but he kept busy playing asteroids. Today, the same lawyer has a new car and a booming practice. He is constantly in court, arguing the merits of Cubby, Inc. v. CompuServe, or defending electronic bulletin board owners. Questioned about his new-found success, he explained, "Another lawyer logged onto the Internet and now we sue each other."

TRADEMARKS AND TRADE NAMES

Today, lawyers roam the networks, debating ownership terms such as "Cyberlaw", and speculating on the future of computer networks.

Much litigation concerns what lawyers refer to as, "intellectual property": the ownership of ideas, inventions, software and names.

For example, attorneys have disputed the ownership of the term "Cyberlaw". Cyberlaw is defined as the law arising from the growth and proliferation of computer-assisted telecommunications, electronic mail, information and data exchange systems. It derives, in part, from existing laws of contracts, privacy, slander, intellectual property, criminal

procedure, as well as legislation and treaties, including the proposed North American Free Trade Agreement ("NAFTA"), the Electronic Communications Privacy Act ("ECPA") and similar State and local statutes.

Whether "Cyberlaw" is a generic term is debated. Thus, the Cylerlaw List Service, run by Professor Trotter Hardy of the Marshall-Wythe School of Law, College of William and Mary, ran afoul of the Cyberlaw (tm) CyberLex (tm) online educational service published by Jonathan Rosenoer. It should be noted that although the term "Cyberlaw" is well known to attorneys on the Internet, a search of the traditional legal databases (WestLaw and Lexis) revealed that no federal case has ever used that term, and that the only case to use the term "internet" is United States v. Morris[2], which affirmed the conviction of Robert Tappan Morris for launching the Internet worm. Obviously, "Cyber lawyers" are in the minority (or cutting edge) of the legal profession.

PUBLIC AND PRIVATE WORKPLACE ELECTRONIC MAIL

The rights and obligations of parties concerning electronic mail, or "e-mail", has become a fertile field for litigation.

The Electronic Communications Privacy Act (ECPA) and a number of state laws treat unlawful access to stored electronic communications as a federal crime. (See 18 U.S.C. 2701). One hotly litigated issue is the right of the employer to monitor telephone and computer communications during the course of

business. The monitoring of workplace telecommunications or computer-stored data and communications appears to be permissible under the ECPA, particularly if the employee is placed on written notice of the employer's intention. Some argue that this is an unwarranted invasion of the employee's privacy. Last term, legislation was introduced, entitled The Privacy for Consumers and Workers Act (Bill No. S984, HR 1900), which would have required employers to notify employees whenever monitoring begins. Employers argued that private communications decrease productivity and service to the customer.[3]

The nature of Whitehouse and other public e-mail has been the subject of a series of published opinions, collectively known as the Armstrong cases.[4]

On consolidated appeal in Armstrong v. Executive Office of the President (1993) 1 F.3d 1274, the United States Court of Appeals for the District of Columbia Circuit held that government agency e-mail could not be destroyed. It further held that government agencies did not reasonably discharge their obligations under the Federal Records Act by instructing employers to print out a paper version of electronic communications because pertinent information present in the e-mail system, concerning who sent the document and who received it, was not always preserved on the paper print out. The court held that if a document qualifies as a "record" under the Federal Records Act, it cannot be discarded without approval of the Archivist pursuant to the Act. The electronic data constituted a

"record" under the Act.

The court remanded portions of the Armstrong cases, most notably the contempt issues, to the lower courts. Freedom of Information Act challenges concerning the computer tapes of the communications of Casper Weinberger and others will continue to be litigated.

Recovery of workplace electronic mail messages formed the basis of the grand jury indictments of several Symantec executives for conspiracy to steal trade secrets from Borland International. After Eugene Wang resigned as vice-president of Borland International to work at rival Symantec Corporation, a number of incriminating electronic mail messages were found on Wang's office computer. These messages had been sent to the electronic mail box of the Symantec chief executive officer, Gorden Eubanks. The messages formed the basis of a search warrant for Wang's home and laptop computer, which had been purchased for Wang by Symantec. The data in the laptop supported grand jury indictments of Wang and other Symantec executives.

The Symantec case illustrates a number of evidentiary issues in this area, including the admissibility of computer files, including restored deleted files, spoliation of or alteration of evidence, chain of custody, as well as search and seizure issues.

INTELLECTUAL PROPERTY: COPYRIGHT AND TRADE SECRETS

The Symantec case is also noteworthy for its subject matter, the theft of trade secrets, because intellectual property

issues are the most frequently litigated in the field of computer telecommunications.

The economic importance of the telecommunications infrastructure, as well as the increasing role of commercial competition in this industry have been driving forces in the Clinton administration's plan to have the United States government serve as a catalyst for the development by the private sector of an advanced national telecommunications network, or "information highway."[5]

Among the recent intellectual property decisions is the Ninth Circuit opinion in MAI Systems Corp. v. Peak Computer, Inc.,[6] which held that the mere loading of computer software into random access memory may violate copyright law.

THE CLIPPER CHIP

The Clinton administration has also endorsed the Clipper chip, manufactured by Mykotronx, Inc. of Torrance, California, which contains a highly sophisticated encryption algorithm. Cryptography has long been proposed as a solution to e-mail privacy issues; however, the Clipper chip proposal will allow the government to hold the decryption keys. The National Security Agency (NSA) and the National Institute for Standards and Technology (NIST) have presented a proposal whereby the keys to decrypting the Clipper-encrypted communications will be held by two separate agencies. A number of organizations have expressed concern about the Clipper chip, including the American Civil Liberties Union and the Electronic Frontier Foundation.

As a corollary to the clipper chip controversy, the encryption program known as "Pretty Good Privacy" (PGP) has been embroiled in an intellectual property dispute between RSA Data Corporation and its creator, Phil Zimmerman. (See Levy, Crypto Rebels, Wired (May/June 1993) p. 54) PGP has been available worldwide through the Internet, but legal experts expect to see further challenges to the various versions of PGP based on intellectual property theories.

CRIMINAL PROSECUTIONS

Criminal prosecutions of "hackers" will continue. Phiber Optick (Mark Abene), aged 21, plead guilty on July 2, 1993, to charges that he was part of a group that broke into telephone company computers in 1991. Court-authorized wiretaps were used to obtain voice and data transmission of these young people. Many feel that law enforcement has overreacted to "mere" pranks. By the same token, high tech crime task forces will address global issues of software piracy, theft and computer crime.

Suspects were recently arrested in a case where two men placed an ATM in a shopping mall and distributed $20 bills while capturing personal identification numbers (PIN).

In United States of America v. Brady, an indictment was set aside where a defendant was charged with using and trafficking in a counterfeit access device consisting of an altered cellular telephone which permitted unauthorized access to telephone services. Chief Judge Jenkins held that the cellular

telephone used for the purpose of a "free ride" on the telephone system was not an "access device" within the meaning of the federal statute.[7]

The shoe was on the other foot in the recent decision in Steve Jackson Games v. United States Secret Service, where the operator and users of a computer bulletin board sued the Secret Service for an unauthorized search, seizure and eventual destruction of materials. The search was pursuant to a search warrant.[8]

Although one agent was an attorney, he was not aware of the Privacy Protection Act.[9] The Court held that: (1) the seizure was a violation of the Privacy Protection Act; (2) seizure, reading, and destruction of materials did not constitute unlawful "interceptions" within the meaning of the Wire and Electronic Communications Interception and Interception of Oral Communications Act; but (3) seizure constituted a violation of the Stored Wire and Electronic Communications and Transactional Records Access Act. Appropriate sanctions were permitted.

Noteworthy criminal cases will continue. The Electronic Frontier Foundation and other organizations will litigate the breadth of police searches, and assert the First Amendment right to privacy and the Fourth Amendment right against unreasonable searches and seizures.[10]

CIVIL DEFAMATION ACTIONS

Defamation and related civil lawsuits are a developing area. There is continuing concern regarding the liability of the

BBS owner of the uploading and downloading of files and the communication of messages by the users of the BBS.[11]

One case, Cubby, Inc. v. CompuServe, concerned a libel suit brought against CompuServe for statements made by users on the service.[12] The court held that CompuServe acts as a "bookstore owner", who is not liable for the subjects published in books, as opposed to a newspaper or television station, who are liable for defamation as the "republishers".

In the case of Medphone v. DeNigris, a Prodigy subscriber was sued by a publicly traded corporation. The subscriber, Peter DeNigris, made statements on a Prodigy forum maligning Medphone. After the company's stock plunged from approximately $.86 per share to $.20 per share, the company sued DeNigris, claiming that his statements caused the stock to lose value. Medphone highlights the most seductive feature of the telecommunications medium, the illusion of anonymity, as well as the great danger of instant global transmission.

A related area of public concern, which will undoubtedly lead to litigation, is the recent publicity regarding recreational material on the Usenet. Even Doonesbury seems headed toward a discussion of this issue; lawyers will be right behind. In an era of "PC" debates, we expect continuing litigation regarding campus disputes over access and the right to free speech under the First Amendment to proliferate.

NOTES

1. Doonesbury by Garry Trudeau 10-18-93 and 10-19-93. Mike has discovered "a late night party on the Net..."

2. United States v. Robert Tappan Morris 928 F2d 504 (2d Cir. 1991)

3. This is not an academic issue: the St. Petersburg Times recently reported a survey of 301 participating companies, where 21.6 percent said that the company searched employee files, including electronic work files, e-mail, network messages and voice mail. Only 30.8 percent of the companies warned their employees of the monitoring activities. (St. petersburg Times, 6/23/93, cited by ssteele@eff.org)

4. Armstrong v. Executive Office of the President 1 F.3d 1274 (D.C. Cir. Aug. 13, 1993); Armstrong v. Executive Office of the President __ F.Supp __, 1993 WL 346049 (D.D.C Sep. 3, 1993); Armstrong v. Executive Office of the President 823 F.Supp. 4 (D.D.C. June 8, 1993); Armstrong v. Executive Office of the President 821 F.Supp. 761 (D.D.C. May 21, 1993); Armstrong v. Executive Office of the President 810 F.Supp. 335 (D.D.C. Jan. 6, 1993); Armstrong v. Bush 807 F.Supp. 816 (D.D.C. Nov. 20, 1992)

5. Gould, U.S. Telecommunications Infrastructure: Projected Future Revolution (Congressional Research Service 1993)

6. MAI Systems Corp. v. Peak Computer Inc. __ F2d __ (9th Cir. 1993)

7. United States of America v. Brady 820 F.Supp. 1346 (D. Utah C.D, April 7, 1993)

8. Steve Jackson Games Inc. v. United States Secret Service 816 F.Supp. 432 (W.D. Texas, March 12, 1993)

9. 42 USC 2000aa

10. Hafner & Markoff Cyberpunk: Outlaws and Hackers on the Electronic Frontier (Touchstone, 1991); Muggs, Soma & Sprowl, ComputerLaw, (West Publishing 1992); Sterling, Bruce, The Hacker Crackdown: Law and Disorder on the Electronic Frontier (Bantam 1992); Stoll, Cliff, The Cuckoo's Egg; Seline, Christopher J., "Eavesdropping on the Compromising Emanations of Electronic Equipment: The Laws of England and the United States", 23 Case W. Res.J.Int'l L. 359 (1991); Solum, Lawrence B., "Legal Personhood for Artificial Intelligence", 70 North Carolina Law Review

(1992); Tribe, Lawrence, "The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier, Keynote Address at the First Conference on Computers, Freedom and Privacy" (proposing Constitutional amendment to address conjunction of privacy and technology), cited in Robert Gracia, "Garbage In, Gospel Out": Criminal Discovery, Computer Reliability, and the Constitution, 38 UCLA L.Rev. 1043 (1991); and Note, "Computer crime in Virginia: A Critical Examination of the Criminal Offenses in the Virginia Computer Crimes Act" 27 Wm. & Mary L. Rev. 783 (1986); and Becker, The Liability of Computer Bulletin Board Operators for Defamation Posted by Others, 22 Conn.L.Rev. 1989

11. Becker, "The Liability of Computer Bulletin Board Operators for Defamation Posted by Others", 22 Conn. L. Rev. (1989); Burnside, Russell S., "The Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunication Technologies", 13 Rutgers Computer & Tech.L.J. 451, 494-95 (1987); Meyer, Fred Jay, "Don't Touch That Dial: Radio Listening Under the Electronic Communications Privacy Act of 1986", 63 N.Y.U.L. Rev. 416, 434 (1988); Note, "An Electronic Soapbox: Computer Bulletin Boards and the First Amendment", 39 Fed. Com L. J. (1987); Note, "Computer Bulletin Board Operator Liability for User Misuse", 54 Ford.L. Rev. (1985);

12. Cubby, Inc. a Corporation dba Skuttlebut, and Robert G. Blanchard v. Compuserve, Inc., dba Rumorville, and Don Fitzpatric, individually (1991) 776 F.Supp 135; United States of America v. Robert J. Riggs, also known as Robert Johnson, also known as Prophet, and Craig Neidor, also known as Knight Lightning, (1990) 739 F.Supp. 414

SECOND INTERNATIONAL SYMPOSIUM: NATIONAL SECURITY & NATIONAL COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, 1993 Volume I - Link Page

Previous	The Linear File(reprinted from DATABASE)
Next	Talking Points for the Director of Central Intelligence

Return to Electronic Index Page