

Arlene McDonald

Dr. Jack Baldwin LeClair

Cyberlaw LSLW 59

Summer 1999

GOT MAIL: AN OVERVIEW OF E-MAIL, SEXUAL HARASSMENT, AND THE FIRST AMENDMENT

Communications has been in a process of evolution and revolution from the time the first cave person drew pictures on a wall through the inventions of the printing press, the telephone, radio, and television to the most current revolution – the Internet. This paper will attempt to provide an overview into one area of on-line communication: e-mail. More particularly, it will attempt to briefly examine sexual harassment via e-mail and the constitutionally granted rights of the First Amendment. In the interests of brevity and to remain within the parameters of the paper any discussion will exclude workplace sexual harassment, flaming and stalking. The issue of public versus private forum has been discussed in many papers and journals and will not be covered in this paper. We also assume that any reader of this paper has a basic knowledge of sexual harassment issues.

Any discussion of an area concerning the Internet must involve a fundamental understanding of its background and operations. The Internet began in the 1960's as a method of preserving communications in the event of nuclear attack. It originally linked government and university computers. It was placed under the auspices of the Department of Defense's Advanced Research Project Agency and was known as ARPANET. From 1969 to 1979, Dr. John Postel developed a procedure, based on the use of addresses that allowed ARPANET to connect to another network, operated by the National Science Foundation. "...Addresses are long strings of numbers that facilitate the sending of information from one network computer to another...to assist in remembering the addresses Postel and his coworkers assigned each computer a name, which a file on each computer translated into numbers. " With the growth and popularity of the Internet modifications to this system were necessary. "[T]he 'nicknames' were separated into groups called 'domains'. The 'top level' domains consisted of two types: national domains, such as '.us' for the United States or '.ca' for Canada: and generic domains such as '.edu' or '.com'. Separate computers administered each domain and "root server" directed traffic among the domains". The Internet Assigned Numbers Authority (IANA) was responsible for assigning numbers. In 1992 this responsibility was transferred, at the governments' request, to InterNic, administered by Network Solutions. In September 1998, The International Corporation for Assigned Names and Numbers (ICANN) was established to take on this responsibility. ICANN's board of Directors would be comprised of members designated by IANA and NSI would provide technical aide.

All information on the Internet travels via Internet Protocol (IP) from one network to other networks and finally to its destination through packets. "Headers carry addresses for the packet's source and destination and instructions for how to reassemble packets when they reach their destination". Large messages are split into several packets and sent individually to their destination through routers. "IP packets first travel through physical, wired networks like Local Area Networks (LAN's) that connect PC's in most or telephone wires to a central office switch. But to reach a network beyond a LAN, or central office, packets must pass through an IP router that is connected to the LAN or the telephone network. An IP

router sends a packet on the next router that will best relay the packet to its destination. Addresses allow packets to reach their destination. Global organizations assign IP addresses. An address is a series of four numbers each consisting of 1, 2, or 3 digits. The organizations maintain registries of names...{and} establish separate domains – groups of computer servers placed in categories based on the kind of organization they represent: gov. for U.S. government servers; .edu for educational servers; .com for commercial servers; .net for Internet service providers; .org for the servers of non-profit organizations; .uk for servers in the United Kingdom. The Internet provides global communication to anyone with access to a computer. There are three major techniques for communicating on a computer: real time communications, where the message is read and replied to immediately; one to many communications, where a message is sent to a number of individuals to be opened and read in the future; and one to one communications, e-mail, where the communication is sent to a specific individual. "E-mail has been defined as a document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents and any attachments...[or] any other electronic documents, which may be transmitted. E-mail is the most popular form of communicating on the Internet. "In 1994, 812 million [e-mail] messages were sent [via the Internet]. It is projected that 5.3 trillion will be sent in 1999". E-mail is quick and simple: the sender creates a message and sends it through an ISP mail server; the ISP sends it to the mail server of the person to whom the message is addressed; along its path, the message may travel through several servers until it reaches its destination and; it will remain in the destination server until pulled up by the addressee. "Each e-mail address you send is made up of certain components that help route it to the proper recipient: [e.g. in i101@famvid.com]the user name or identification number [i101] the @ (at) sign serves as a divider between E-mail sections [the] Domain name, which is the name of the user's internet system or location [famvid] the type of institution [.com]"

The process of transmitting messages on the Internet makes it possible to send messages anonymously. Service providers will allow customers to select a name of their choice, or will assign one to them. It is also possible to send a message without any name. All that is needed for anonymity is the ability to encrypt your message and to use a remailer. Remailers are individuals who voluntarily act as intermediaries between the sender of a message and the recipient.. Complete anonymity can be achieved by the use of several remailers. "[B]y multiply encrypting ...message, in layers, ... As each remailer receives...[a] message, it discards the headers identifying the e-mail 's origins and then decrypts the message with its private key, revealing the next address, but no more".

Anonymity is a much-debated issue in Internet commerce. Those opposed to anonymity point out that it can cause aggressiveness, allow evasion of punishment for illegal activities, increase violations of intellectual property laws and trade secrets, and encourage harassment. Opponents claim Internet anonymity has a detrimental effect on society: "...producing a society of strangers...[who are] people

about whom one know[s] little or nothing [and] are harder to trust; they can be feared ... [and are] without any risk of being held accountable". On the other hand, those in favor of anonymity point out that anonymity encourages whistle blowing; allows criticism of governments or religion without reprisal; permits individuals, who otherwise would be reluctant, to access health information and; "encourage discussions that concentratae on the merits of speech rather than the presumed qualities of the speakers." First amendment concerns are a major issue involving Internet speech, particularly e-mail. The First Amendment to the Constitution states that "Congress shall make no law... abridging the freedom of speech or of the press" It does not protect all speech nor does it protect equally. . Some exceptions to protection include fraud, child pornography, obscenity, causing panic, incitement to crime, sedition, discriminatory job advertisements, defamation and threats. Speech that is partially protected includes false or misleading advertising and sexually explicit speech. Speech that is completely protected includes

- "Speech about Politics, society, religion, philosophy, and science.
- Art and Literature, music, poetry
- Jokes, gossip, entertainment, and casual chitchat.
- Pretty much anything else that doesn't fall into the valueless or intermediate categories

Free speech may also be limited if there is a compelling interest on the part of federal, local or state governments. However, this interest must be the least restrictive means available. The First Amendment to the Constitution protects interference from the government only; individuals and private corporations do not fall under the First Amendment prohibitions. Although there is no specific protection under the Constitution for anonymous speech, the United States has a history of favoring anonymity that goes back to the Federalist Papers. Past judicial rulings show a tendency of the courts to favor anonymity. The court in A.C.L.U v. Miller 977 F. Supp.1228 (N.D, Ga. 1997) overruled a state law prohibiting anonymous Internet communications. The holding of the court in McIntyre v Ohio Elections Commission 514 U.S. 334 (1995) was that the distribution of anonymous leaflets was protected by the First Amendment. In NAACP v Alabama, 357 U.S. 449 (1958), the Court upheld the right of an organization to refuse to surrender its membership list to the State.

The nature of the Internet has made E-mail a form of communication with unique characteristics:

E-mail users are often blunt and direct; they are less concerned with the possible impact their speech may have. The words they choose are more harsh or crude than those used in other contexts. One result is that male users frequently address female users in ways not ordinarily considered polite in a face to face conversation...(No statistics are available for the make up of the Internet community as a whole...Compuserve reports that 90 percent of their 1,5 million subscribers are male, America Online is 85 percent male, and Prodigy's customers are 70 percent male) These unique characteristics of e-mail and the use of anonymity have, allegedly, contributed to sexual harassment on the Internet. Harassment is

defined as a course of conduct directed at a specific person that causes substantial emotional distress in such person and serves no legitimate purpose.' 18 U.S.C.A. §1514(1). Term is used in a variety of legal contexts to describe words, gestures, and actions which tend to annoy, alarm (verbally) another person.

It is estimated that there were two hundred million individuals using the Internet in 1998. With this rapid increase in Internet use, it should be expected that sexual harassment will also increase. In 1997 the Web Police documented 13,000 complaints of Internet abuse. By November of 1998, 47,000 were received, 30 percent of which were about harassing or threatening e-mail. Laws have not kept pace with the increase in Internet use and development. Federal laws, modified from laws to regulate the telecommunications, print and broadcasting industries, are used to regulate e-mail harassment. The Communications Act of 1964 prohibits obscene or harassing telephone calls and "telephone call, whether or not conversation ensues, without disclosing his identity and with the intent to annoy, abuse, threaten, or harass any person at the called number; makes or causes the telephone of another to repeatedly or continuously ring, with the intent to harass any person at the called number; or makes repeated telephone calls, during which conversation ensues, solely to harass any person at the called number (U.S.Code §223 (a) (1) (B) (C) (D)). Neither the 1964 Act nor the 1989 amendment to this act included any provisions regarding e-mail. Although E-mail is a written, electronic communication and the language of the Acts specifically refers to "telephone" and "conversation", its adaptation to e-mail harassment has been defended. Since e-mail is transmitted over telephone lines it should come under the Communications Act. Once an E-mail message has been transmitted it is stored until the receiver opens it. This process has been compared to answering machines that are covered under the Communications Act.

The Electronic Communications Privacy Act of 1986 (18 U.S.C. §§2510-2521, 2701-2710) forbids the "interception of electronic communications, on a public system, while in transmission and unauthorized intrusion into electronic communications stored on a system. " Title I prohibits interception while in transmission. There are two exceptions to Title I. The first is expressed or implied consent and the second is business necessity for the provider of wire or electronic communication service. Title II prohibits accessing of stored messages. Under Title II, systems providers are exempt from the access provision of the EPCA. The language of the EPCA is confusing; questions arise as to the definition transmission, storage and of service providers.

The Communications Decency Act of 1996 Title V of the Telecommunications Act of 1996 (CDA) 947 U.S.C. §223(a) sought to protect children by prohibiting indecent and obscene material being sent to those under the age of 18. This Act also prohibits "on line communications that are obscene, lewd, lascivious, filthy or indecent with the intent to annoy". Reno v ACLU 117 S. Ct 2329, 521 U.S. 844, overturned the CDA, in part. In Reno, the Supreme Court upheld the lower courts ruling that the provisions concerning child pornography were overly broad and vague. In its ruling, the Supreme Court

"found that ... the Internet is a unique communications media that has never been subject to government regulations and thereby afforded it the highest level of First Amendment protection" The portion of the CDA concerning annoying, indecent communications was challenged in Apollomedia Corp v. Reno, 19 F.Supp.2d 1081, 1998 U.S. Dist. LEXIS 150406 (N.D. Cal. 9/23/98), *Aff'd* 1999 U.S. LEXIS 2575 (S.Ct. 4/19/99) . The Supreme Court upheld the district court ruling that "'Indecent' communications could be construed as constitutional by limiting the statutory ban to 'obscene' communications

The increased use of the Internet along with the sacristy of federal laws concerning e-mail outside the workplace make it difficult to prove sexual harassment online. Law enforcement agencies find it difficult to determine when alleged harassment is illegal or only annoying. In most cases, individuals can obtain help from law enforcement agencies only if they can prove that they have been threatened. The Court has ruled, in US v Machado 457 F.2d. 1372 (9th Circuit 1998), that the first Amendment does not protect e-mail threats. Two Supreme Court cases have suggested tests to determine when an action is a threat. In Watts v United States 394 U.S. 705 (1969) the court held that was not necessary to show that there was intent to carry out the threat. In the dissent a two-prong test for threats was suggested. "1) the defendant makes an alleged threat with the specific intent to execute it, and 2) in the context and circumstances, the statement unambiguously constitutes a threat". In Rogers v United States 422 U.S.35 (1975), Justice Marshall suggested a threats test that required "the defendant intended that his statement be taken as a threat, even if he had no intent of actually carrying out the threat; and 2) the statement made was in fact threatening. Several Circuit court cases have provided tests for determining when an action is a threat. United States v Kelner 534 F.2d 1020 (2d Cic 1976) the threat must be "unequivocal, unconditional, immediate and specific...not have to prove that the defendant had a specific intent or a present ability to actually carry out the threat". Roy v United States 416 F.2d. 874 (9th Cir. 1969) held a threat existed if "1) the defendant intentionally makes a statement, whether written or oral; 2) the statement is made in a context or under such circumstances that a reasonable person would foresee that the statement would be interpreted by those to whom it was communicated as a serious expression of intent to inflict harm; and 3) the statement is not the result of mistake, duress or coercion.

In U.S. v Baker 104 F.3d. 1492 (6th Cir. 1997), the court held that speech is a threat and not protected by the First Amendment when " a reasonable person would: 1) take the statement as a serious expression of an intention to inflict bodily harm, and 2) perceive such expression as being communicated to effect some change or achieve some goal through intimidation".

Communications in cyberspace differ from traditional forms of communication. The Supreme Court, in upholding certain provisions of the CDA, has given speech on the Internet First Amendment protection but the regulation of speech is still complicated. Laws in cyberspace have been adapted from older laws passed to deal with problems created in the print, broadcast and telecommunications industries. These

modifications do not always allow for appropriate remedies to abuses in cyberspace. The telecommunications laws regarding phones are the easiest to relate to e-mail. In telephone communication there is a one to one communication, calls are an intrusion in the home; there is direct communication, and the receiver is able to hear the callers voice with his/her inflections and tone of voice. E-mail is also a one to one communication. However, e-mail is neither an intrusion into your home nor a direct communication in which the listener can judge the intent of the conversation from the caller's voice. It is also easier to trace a phone conversation than an e-mail transmission. The broadcast industry is a one to many communication and is an intrusion into the home. It is also an area in which there is a limited number of frequencies available for use. Unlike the broadcast industry, there is, at this time, no limit to the number of individuals who can send and receive e-mail; all you need is a computer and access to the Internet. The print industry, with editorial review, has the most First Amendment protection of the older industries. It is also a one to many form of communication. Unlike e-mail, the print and broadcast industries are not interactive. The Internet cannot be compared to any one of these former technologies. The technology of Internet creates an overlap, combining parts of all the more traditional forms of communication. With the new broadband technology more and more individuals will have access to the new technologies and to e-mail. It is important that we keep pace legally with the new technology but it is equally important that we do so not as a swift response to actions but as a well thought out process. Our lawmakers and judges must be educated about the new technologies before they can make new laws or changes to existing laws. Internet users must be educated to the severity and consequences of abusing e-mail harassment.

Anonymity definitely influences behavior that would not be tolerated in face to face communications. This, in turn, can increase the incidents of harassment. However, outlawing anonymity is not the answer. The global nature of the Internet would make it implausible, if not impossible to enforce such a ban. There are many advantages to anonymity. The many advantages anonymity provides to society must be weighed against the disadvantages. Judicial rulings tend to protect anonymity; any change in that trend would jeopardize the protections granted by the First Amendment. Case law provides tests for threats but there is no federal law specifically prohibiting e-mail harassment. Harassment laws will have to be tailored to the Internet. What would not be permitted in face to face communications or the workplace must not be allowed in cyberspace. Lawmakers will have to pass laws that clarify and define on-line harassment similar to those that address the issue of sexual harassment in the workplace. By prohibiting indecent communications with the intent to annoy, the CDA gives us a foundation on which to build. The Apolomedia court specified that "indecent" was to be considered "obscene. But, in her dissent, Judge Illston questions this decision in view of Reno where prohibitions against obscene speech were allowed but those of indecent speech were not.

Although federal law is does not properly protect individuals from online sexual harassment, safeguards for individuals are available in the private sector and in many individual states. In the private sector, companies are developing software similar to Caller ID and are improving filtering and blocking products that will assist in combating e-mail abuse. Individual states are prohibiting harassment and stalking. Service providers are instituting policies that ban harassing behavior. However, until federal legislation catches up to modern technology, protection from e-mail harassment is primarily the responsibility of individuals. Harassment must be reported to the authorities and service providers; those individuals sending harassing e-mail must be informed that the receiver does not want the harassing behavior to continue; e-mail from known offenders or strangers should not be opened.

BIBLIOGRAPHY

- Andrews, Anna S. "When is a Threat Truly a Threat Lacking First Amendment Protection? A Proposed True Threats Test to Safeguard Free Speech Rights in the Age of the Internet," The UCLA Online Institute for Cyberspace Law and Policy (May 1999)
<http://www.gseis.ucla.edu/iclp/aandrews2.htm>
- Barton, Gene. Note and Comment: Taking a Byte out of Crime: E-Mail Harassment and the Inefficacy of Existing Law." Washington Law Review 70 (April 1995): 465-490. On-line. Available from WestLaw @ Legal Texts and Periodicals File: TP-ALL
- Cottingham, Scott, "What is the Internet," Internet 101, (1999) 1-2 Online.
<http://www2.famvid.com/i/internet.html>
- Bell, Vicki and Denise La Rue, "Gender Harassment on the Internet," Georgia State University College of Law Paper for Law on the Internet. Online (June 1995) 1-27
<http://www.gsu.edu/~lawppw/lawand.papers/harass.html>
- Black, Henry Campbell, By the publishers editorial staff co-authors Joseph R. Nolan and Jacqueline M. Nolan-Haley, contributing M.J. Connolly, Stephen C. Hicks and Martina N. Alibrandi .
Black's Law Dictionary Sixth Edition (1991) St.Paul: West Publishing Co
- Cottingham, Scott, "What is the Internet," Internet 101, (1999) 1-2 Online.
<http://www2.famvid.com/i/internet.html>
- "Developments – The Law of Cyberspace" Harvard Law Review, vol 112 (May 1999) 1577-1659. Online <http://www.harvardlawreview.org/vol112.html>
- Determining the Legality of a threat," Legal Analysis. <http://www-cse.stanford.edu/class/cs201/current/Projects/nuremberg-files/legal.html> 1
- Philip, Dorf,. Philip The Constitution of The United States with a Detailed Clause-by-Clause Analysis New York: Oxford Book Company, 1957)
- "First Amendment/Free Speech/ Media," Perkins, Coie Internet Case Digest, Perkins, Coie LLP
(Oct. 1999) 1- 11. Online. <http://www.perkinscoie.com/resource/ecommm/netcase/Cases-12.htm>
- Froomkin, Michael. "Flood Control On the Information Ocean: Living with Anonymity, Digital Cash and Distributed Databases," U. Pittsburgh Journal of Law and Commerce vol 15 395 (1996) reproduced online <http://www.law.miami.edu/~froomkin/articles/ocean1.htm> 1-46
- Garcia, Erick C. "E-mail and Privacy Rights," Computers and the Law (Fall 1996) 1-7. Online. <http://wings.buffalo.edu/law/Complaw/CompLawPapers/garcia.html>

Hatcher, Michael, Jay McDannell and Stacy Ostfield, "Computer Crimes," American Criminal Law Review vol 36 (Summer 1999) 397 - 444 Online. Available from WestLaw database Journals and Law Reviews, file: AMCRLR

Hudson, David, "Federal Court Rules That Annoy.com May Continue to Annoy," Freedom Forum (Sept. 1998) 1-2. Online. <http://www.freedomforum.org/speech/1998/25annoy.asp>

"Welcome to IP @ AT&T," IP@ AT&T. Online <http://www.att.com/technology/ip> (Homepage that leads to IP Primer IP Tour, IP Video)

"IP Primer," IP @AT&T. Online. <http://www.att.com/technology/ip> chapters 01-09

Lessing, Larry, David Post, Eugene Volokh. "Government as Sovereign," Cyberspace for NonLawyers (1991) 1-2. Online. <http://www.ssrn.com/update/lsn/cyberspace/lessons/fresp04.html>

Masters, Brooke A. "Cracking Down on E-mail Harassment," Washington Post, Nov. 1, 1998

McGraw, David, "Sexual Harassment, the Problem of Unwelcome E-mail," 20 Rutgers Computer & Texhnology Law Journal. (1997 last modified Feb. 1998) 491 . Reproduced Online 1-17. <http://miser.suffolk.edu/law/hightech/classes/sp98cyber/wk7art1.htm>.

Rappaport, Kim L. "In the Wake of Reno v ACLU: The Continued Struggle in Western Constitutional Democracies with Internet Censorship and Freedom of Speech," 13 American University International Law Review (1998) 765-814. Online. Available from WestLaw database Journals and Law Reviews file: AMUILR

Reno v ACLU electronic Privacy Information Center Online. No. 96-511 Argued March 19, 1997 - Decided June 26, 1997_ http://www2.epic.org/cda/cda_decision.html

"Supreme Court Affirms a Portion of the Communications Decency Act," Cole Raywid & Braverman, LLP (1999) 1. Online <http://www.crblaw.com/1999/04219901.htm>

Apollomedia Corporation v Reno No. C-97-346 MMC Sept. 23, 1998 Cole, Raywind & Braverman, LLP (1999) Online. <http://www.cbllaw.com/text/apollo.htm>

Turner, William Bennett. "What Part of 'No Law' Don't You Understand?" Wired (March 1996) 1-7. Online. http://www.wired.com/wired/4.03/no.law_pr.html

Jenna Wischmeyer, Jenna, "E-mail and the Workplace," <http://raven.cc.ukans.edu/~cybermom/CLJ/wisch.html>