Unsolicited Commercial E-mail, the Internet and the First Amendment: Another Free Speech Showdown in Cyberspace?

Jan H. Samoriski

This study examines and analyzes efforts to deal with unsolicited commercial e-mail or "spam." Using the Central Hudson test for commercial speech as a benchmark, various legislative proposals to address the spam problem are categorized and evaluated. With legal and technical solutions at hand, the author argues that source-based, content restrictions on unsolicited commercial e-mail are potentially unconstitutional. The impact of lawsuits against spammers and the prospects for industry self-regulation are also discussed.

Late in 1997, the on-line industry stepped up its efforts to fight the growing problem of unsolicited commercial e-mail (UCE). UCE, also known as junk e-mail, or "spam,"[1] had become so pervasive and the methods used by bulk e-mailers or "spammers" so unscrupulous, that some Internet Service Providers (ISPs) resorted to high tech, electronic "bombings" to shut junk e-mailers down.

Most of the disputes, however, shifted to the courtroom. The nation's largest on-line service provider, America Online (AOL), declaring the equivalent of war against spammers, filed dozens of civil lawsuits against bulk e-mailers ("America Online again takes aim at operators of pornographic Web sites,"1998). In Washington, lawmakers responded with controversial legislation to label, limit or altogether outlaw unsolicited e-mail. With on-line users, ISPs, the marketing industry, public interest groups and a host of other constituencies taking sides, the First Amendment, once again, moved center stage for a potential free speech showdown in Cyberspace.

The Internet has become fertile ground for regulatory exploration. Given the magnitude of the spam problem, it appears likely that unsolicited commercial e-mail will become the next target for government regulation. If Congress steps in to impose content-based UCE regulation or labeling requirements, the unsolicited e-mail controversy could find its way to the Supreme Court.

This study will examine and analyze efforts to address and regulate commercial

Jan H. Samoriski *(Ph.D., Bowling Green State University, 1995) is an Assistant Professor of Communications at the University of Michigan-Dearborn. His research interests include new media technology, law and policy, and the First Amendment.*

 Journal of Broadcasting & Electronic Media 43(4), 1999, pp. 670-689

e-mail. The author will argue that source-based, content restrictions and labeling requirements on unsolicited commercial e-mail are problematic and place the government in the disfavored constitutional position of regulating speech when alternative, less restrictive means are available. Given the democratizing potential of the Net as a mass medium with no central control point, the free flow of ideas and information would be better served by user-based options, rather than industry or government initiatives, as a means to maximize user control over Internet content.

The study is organized in seven sections. Part one provides an overview of the unsolicited e-mail problem. Part two examines the evolution of protection for "nuisance" speech in the context of the First Amendment. Part three summarizes recent civil cases concerning unsolicited commercial e-mail, followed by a First Amendment analysis of proposed government regulation in part four. Industry regulation and receiver-based solutions are discussed in parts five and six. The last section is conclusion.

The Rise of Spam

Unsolicited commercial e-mail is a product of the success of the Internet. As the Net has expanded and more people have gone on-line, the problem has grown exponentially. Although percentages vary, America Online, with over 15 million subscribers, at one time estimated that up to 30 percent of all incoming e-mail was junk (Cohen, 1997). Other statistics more realistically estimate that spam may comprise between 5 and 15 percent of Internet traffic (Cranor & LaMacchia, 1998).

Junk e-mail is often analogized to the junk mail delivered by the U.S. Postal Service ("A brief history of junk," 1998). Junk e-mail is sent in bulk by marketers, both legitimately and deceptively, to consumers as a way to sell products and services on-line. Electronic mailers obtain lists of e-mail users, often from companies that specialize in "harvesting" e-mail addresses from the Net, and electronically transmit up to millions of unsolicited e-mail messages to Internet "mailboxes." Although legitimate marketers do not use the word "spam" and distance themselves from the practice (Hall-Smith, 1997), by late 1997 the business of sending junk e-mail had become highly profitable (Simons, 1997). The Internet community became increasingly concerned with the growth of UCE, particularly with the questionable nature of products and services, including pornography, that was being offered on-line (*America Online, Inc. v. Cyber Promotions, Inc.*, 1996). The Federal Trade Commission during 1998 Senate hearings into the Spam problem characterized UCE as "the fraud artist's calling card on the Internet" (Prepared Statement of the Federal Trade Commission, 1998, p.1).

Whereas regular junk mail costs the sender printing, handling and postage for each piece of mail sent, the expense associated with sending hundreds of thousands of junk e-mail messages is almost negligible once an operation is set up and the first message sent. Becoming established in the bulk e-mail business can be easily accomplished by anyone with minimal knowledge about how the Internet works, a

computer, a list of e-mail addresses and an Internet connection. According to one court document:

> The cost to the sender of transmitting one e-mail message to two million recipients is the same as the cost of transmitting the same message to just one recipient -- virtually nothing. This fact has made spamming on the Internet an irresistibly tempting marketing method for desperate, poorly funded and disreputable would-be entrepreneurs. The further opportunity for virtual anonymity in sending spam with forged headers has led to the frequent use of this technique by swindlers, charlatans and purveyors of sleazy merchandise (*Juno Online Services, L.P., v. Scott Allen Export Sales*, No. 97 Civ. 8694 (S.D.N.Y, 1997, p. 5).

Software programs specifically designed to send bulk e-mail, called "spam generators" are also available. Some such programs, ironically, have been marketed through unsolicited commercial e-mail offers.[2]

Unsolicited e-mail became controversial for both technical and non-technical reasons. On the technical side, opponents complained that unsolicited e-mail costs everyone money and clogs up the Net (Deck & Hamblen, 1997). The costs were being reflected in, for example, on-line fees where service providers charge by connect and download time and by fees imposed on stored mail. Unsolicited e-mail was also imposing burdens on ISPs, where spam consumes bandwidth, takes up space and requires staff time to manage (Voters Telecommunications Watch, 1997). In some cases, phone lines tied up by marketers delivering bulk e-mail were making it impossible for regular subscribers to get through. Users and service providers argued that they were being unfairly burdened and forced to pay for unsolicited e-mail that they had little control over.

To complicate detection, bulk e-mailers were disguising the origin of unsolicited bulk e-mail. Unscrupulous spammers were fraudulently using the names of legitimate companies and service providers in e-mail headers to thwart software designed to filter spam.[3] To avoid being identified, spammers frequently changed Internet addresses and service providers so that recipients would have a hard time tracking them down. The techniques that targets of bulk e-mailings used to retaliate became increasingly sophisticated. One retaliatory practice, known as "bombing," redirects undelivered spam back to its source.[4] Bombing can overload and shut down servers, computers used by Internet companies and service providers to send, receive and store data. Some electronic attacks and counter attacks wound up in court (discussed *infra*).

Many of the non-technical issues stem from the frustration and inconvenience that users, service providers and bulk e-mailers have experienced with unsolicited e-mail. At one end of the spectrum are complaints regarding fraud, deception, indecency and privacy, areas that currently fall under the jurisdiction of federal and/or state agencies such as the U.S. Postal Service, Federal Trade Commission (FTC) or state Attorney General. At the other end are First Amendment issues involving content regulation, commercial speech, anonymity and the right to send and receive information. Like

other communications technologies when they were new, the boundaries and rationales for government regulation of the Internet have yet to be clearly defined.

Until 1996, unsolicited e-mail was not a problem on the Internet ("A brief history of junk", 1998), so there was no reason for the government to become involved in regulation. While most Internet users would agree that unsolicited e-mail has become a nuisance and that something needs to be done about it, not everyone is in agreement about *what* should be done. Those hurt the worst by spammers, however, have fought back. In a development that has caught the Internet community by surprise, on-line companies and ISPs have taken spammers to court in an effort to protect themselves from being inundated by spam.

If unsolicited commercial e-mail is a nuisance, what kind of protection is it entitled to under the First Amendment?

Telephones, Faxes, Floppies, Frustration, and the First Amendment

Reduced to its simplest form, the regulation of unsolicited commercial e-mail presents an old problem with a new technological twist: how to deal with a nuisance by keeping "right" things out of wrong places – how to keep the "pig" out of the parlor (*Federal Communications Commission v. Pacifica Foundation*, 1978). Spam presents a particularly difficult problem, because every time the door is closed, the nuisance finds another way to get in. To deal with the technical challenges posed by UCE, regulators have been considering legislative options, but some of the options under consideration are likely to run afoul of the First Amendment.

The Supreme Court has observed that the "ancient concept that 'a man's home is his castle' into which 'not even the king may enter' has lost none of its vitality" (*Rowan v. U.S. Post Office Dept.*, 1970 at 737). In upholding a Postal statute that allowed a homeowner to instruct the Postmaster to order the sender of unwanted mail to remove the recipient's name from a mailing list, the Court held that the "right to communicate must stop at the mailbox of an unreceptive addressee" (*Id* at 737, 738). The Court held that the government may help individuals stop junk mail by putting in place regulations that assist them, as long as the choice of which mail to stop is left to the individual and not government.

The problem of "junk" communications entering the home has since been addressed with the telephone through the Telephone Consumer Protection Act of 1991 (TCPA) and the fax machine (*Destination Ventures, Ltd. v. F.C.C.*, 1995), but not with an interactive technology such as the Internet.

Federal law regulates unsolicited telephone calls through a modified time, place and manner restriction. The law places constraints on prerecorded messages, requires solicitors to identify themselves, limits times at which solicitors may call, and grants telephone subscribers the right to have their names deleted from telephone solicitation databases (TCPA *supra*).

With fax machines, the TCPA goes further by completely banning unsolicited commercial faxes altogether. In a test of the TCPA in *Destination Ventures* (*supra*), the

9th U.S. Circuit Court of Appeals upheld the government's ban on junk faxes, based primarily on the principle that junk faxes shift advertising costs, in the way of paper and toner, to the recipient. At least one attempt has been made to apply the TCPA's prohibition against junk faxes to junk e-mail by analogizing a computer with a fax/modem board and attached printer to a telephone facsimile machine (*Douglas K. Snow v. Daniel Doherty*, 1997), but a close reading of the TCPA leaves little doubt that Congress meant the statute to apply only to fax machines.

The technology of the fax machine and the technology of the Internet, while they both shift transmission costs to receivers, differ in other important aspects. The legislative history of the TCPA and the subsequent ruling in *Destination Ventures* provide specific evidence of Congressional intent behind the ban on commercial junk faxes and how the law should be interpreted. Any evaluation of the distinction between fax and e-mail communication should also consider how each is used. Faxes are used primarily for legitimate business-to-business communication. The bulk of unsolicited commercial e-mail, much of which is deceptive or fraudulent in nature, is directed at private citizens.

Technically, the fax machine is a point-to-point technology that communicates discretely with another fax machine. While a fax is being transmitted, the fax machine and the connecting phone line are busy. Other faxes can neither be sent nor received. Congress, in passing junk fax legislation, recognized that fax advertisers took advantage of a fax machine's design to accept and print all messages that arrive (H.R. Rep. No. 317, 1991). While a fax machine is processing junk faxes, something that could go on for hours with the "explosive" growth in unsolicited facsimile advertising, Congress noted the machine could not receive legitimate business faxes (*see* Destination Ventures, Ltd. v. FCC).

On the other hand, the high-speed, packet switching technology of the Internet can process thousands of e-mail messages per second. While bulk e-mail may slow the network, messages are not blocked at the recipient's mail box by a busy signal. Nor does the receipt of an e-mail message keep a user from sending another message. The same technology, however, presents problems of a different nature.

Unlike the older technology of the fax where senders had to know the phone number of the fax machine, software programs allow junk e-mailers to harvest millions of e-mail addresses from the Net with very little effort. From the lists, millions of messages can be generated and sent electronically without the need to dial each computer discretely. In this regard, the computer-based infrastructure of the Net is more complex.

At the time Congress passed the ban on unsolicited commercial faxes, technology had not reached the point where fax machines could be programmed to block the receipt of unwanted faxes. In the appeal of *Destination Ventures*, the court rejected the appellant's argument that advances in computer technology were in the process of minimizing the problem. The court said what mattered was the problem as it existed when Congress passed the TCPA, not speculation about solutions that may appear in the future. In subjecting the ban on commercial junk faxes to First

Amendment scrutiny, the court found the TCPA met the *Central Hudson* test for restrictions on commercial speech (discussed *infra*), *at the time* (emphasis added).

Simply extending the TCPA to include unsolicited commercial e-mail ignores the differences in the media and runs counter to the Supreme Court's position in *Red Lion* that "differences in the characteristics of new media justify differences in the First Amendment standards applied to them" (U.S. 367 at 386). In 1991, Congress did not have an alternative to a ban on junk faxes. The technology of the "unique and wholly new medium" (Reno v. ACLU, 1997, footnote 4, finding 81) of the Internet, however, now presents other means of addressing the junk e-mail problem.

The highly-interactive Internet is better suited to a receiver-based regulatory model than the telephone or the fax. Rather than analogizing the Net to existing technologies, society's interest in the free flow of ideas and information would be better served by an approach that favors audiences over speakers, particularly with the Net's mass media characteristics. With the technical means available to remove government from the disfavored constitutional position of regulating speech, there is little reason to continue the scarcity-based broadcast model of regulating speakers when less restrictive means are available to address the UCE problem.

The Court applies an intermediate scrutiny test when reviewing restrictions on commercial speech, the speech that best describes unsolicited commercial e-mail. The current test extends from the Supreme Court case, *Central Hudson Gas & Electric Corporation v. Public Service Commission of New York* (1980). Under *Hudson*, for commercial speech to be protected by the First Amendment it must concern lawful activity and not be misleading. Next, it must be determined whether the asserted governmental interest to be served by the restriction on commercial speech is substantial. If both inquiries yield positive answers, it must then be decided whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest (at 564).

The government's interest in regulating commercial speech is "substantial" if the government is able to show that the harms it seeks to prevent are real, and that the restriction will in fact alleviate them to a material degree (*Edenfield v. Fane*, 1993 at 761). In order to show that the regulation is not more extensive than necessary, the regulation must be narrowly drawn, but it does not have to be the least restrictive means (*Board of Trustees of the State University of New York et al. v. Fox et al.*, 1987, at 476). The government must also demonstrate that there is a "fit" between the means and the ends chosen to accomplish them (at 480). Other alternatives are relevant in determining whether the "fit" between the means and ends is reasonable (*City of Cincinnati v. Discovery Network, Inc., et al*, 1993).

Any government ban or content-based restriction on unsolicited commercial e-mail will have formidable First Amendment barriers to overcome. Past experience with "junk" communication tells us that private citizens are entitled to protect themselves from spam, but when the government gets involved certain criteria must be met.

ISPs Fight Back with Lawsuits, Injunctions, and Judgements

The number of civil and criminal complaints involving unsolicited commercial e-mail have soared in recent years. From just a few lawsuits initially, the list now includes dozens of cases.[5] Internet Service Provider AOL, with several high profile judgements against spammers, has led the way with an aggressive campaign against junk e-mail. The online provider targets and pursues spammers through "AOL's 10 Most Wanted Spammer List" (AOL Legal, 1998). AOL has been joined by other operators and service providers in an unprecedented effort to use civil and criminal law to discourage spamming. This development may affect how much emphasis is placed on regulating the UCE problem and, in the end, how the problem is resolved. Some of the earlier, more significant cases are described here.

In the past, service providers relied heavily on civil remedies to stop distributors from sending mass e-mailings through their systems and to recover damages. But as spammers became more high-tech and brazen in their disguise and routing of bulk e-mail, their actions have breached federal laws. In addition to common law fraud, misappropriation, and misrepresentation, lawyers representing ISPs turned to sections of the United States Code that cover fraud and related activity in connection with computers (*Computer Fraud and Abuse Act*, 1996), unauthorized access and destruction to stored communications (*Electronic Privacy Communications Act of 1986*), trademark infringement (15 U.S.C. 1114), and false designations of origin and false description (15 U.S.C. 1125) to prosecute originators of unsolicited e-mail. The success that service providers have had in obtaining restraining orders and judgements against spammers has been remarkable.

The most significant judgement against an originator of unsolicited commercial e-mail to date was in the case of *America Online, Inc. v. Cyber Promotions* (*Supra*). In AOL, U.S. Circuit Court Judge J. Weiner ruled that Cyber Promotions had no right under the First Amendment to send unsolicited commercial e-mail to members of AOL. Because there is no such right, Judge Weiner further concluded that AOL, in the absence of state action, was entitled to block any attempts by Cyber Promotions to send unsolicited e-mail to AOL members. The case stemmed from AOL's attempts to protect itself from spam by "bombing" Cyber Promotion's ISP, Apex Global Internet Services (AGIS), with undelivered e-mail. In this case, AOL was able to cripple the service provider's mail server.

In ruling the case suitable for summary disposition, Judge Weiner found that there were no First Amendment related facts in dispute. The main issue centered on the legal question of whether AOL's conduct involved, or could be considered, a form of state action.

Cyber Promotions argued that since AOL opened part of its network for public use, AOL had created a public forum to which it was entitled access. Judge Weiner disagreed, ruling that since AOL was not exercising any municipal power or performing any public service, AOL "does not stand in the shoes of the state"(at 7). Moreover, Judge Weiner said that Cyber Promotions had alternative ways of sending

advertising to AOL members, including non-Internet avenues, such as United States mail and traditional marketing media.

After eliminating AOL as a state actor under the exclusive public function test, Judge Weiner determined that none of AOL's activities implied state action. In a last ditch effort, Cyber Promotions attempted but failed to prevail in an attempt to invoke a right to send unsolicited e-mail under the Constitutions of Pennsylvania and Virginia. Neither Constitution, nor theory under which a broader free speech right might exist under state law, said Judge Weiner, could be interpreted as granting Cyber Promotion a right to AOL's forums.

The essence of Judge Weiner's decision highlights the First Amendment's guarantee of free speech as a protection from abridgement by government, not private entities. As private, stockholder held companies, as long as AOL, and other ISPs isolate themselves from the state, there is no First Amendment access to their forums. Because there is no constitutional guarantee of access, AOL can also logically protect itself from unauthorized access.

Cyber Promotions has been sued by several ISPs for its unsolicited commercial e-mail practices. Among the lawsuits are complaints and, in some cases, judgements against Cyber Promotions for violating the Electronic Communications Privacy Act (*Supra*) (*Concentric Network Corporation, Inc. v. Sanford Wallace and Cyber Promotions*, 1996), service mark infringement and dilution (*Bigfoot Partners, L.P. v. Cyber Promotions, Inc. and Sanford Wallace*, 1997), misrepresentation (*Prodigy v. Cyber Promotions, Inc.*, 1996), unauthorized use of a computer network, computer systems, equipment and servers without prior authorization (*Earthlink v. Cyber Promotions, Inc.*, 1997), and causing, authorizing, participating in, or assisting others in sending commercial or promotional messages or solicitations (*CompuServe Inc., v. Cyber Promotions, Inc. and Sanford Wallace*, 1996). Despite the legal trouble and bad publicity, Cyber Promotions continued to generate record revenues from the estimated 15-20 million unsolicited commercial e-mail messages it generated daily. In 1997, Cyber Promotion's revenues were expected to climb to nearly $4 million from $800,000 the previous year (Simons, 1997). A large settlement in one lawsuit eventually forced Cyber Promotions out of business (Branscum, 1998).

Since the *AOL v. Cyber Promotions* ruling, originators of unsolicited bulk e-mail have become more sophisticated in how they operate. Instead of using their own return e-mail address, spammers were substituting phony e-mail addresses, sometimes with those of innocent third parties, in order to protect themselves from e-mail bombs and complaints. Originators of UCE were also substituting the names of legitimate service providers on their messages to thwart filtering programs designed to block e-mail from known spammers.

For example, in *America Online v. Over the Air Equipment, Inc.* (1997), a Federal Judge in Virginia issued an injunction to enjoin Over the Air Equipment from sending any more unsolicited e-mail to AOL members after the company allegedly forged AOL's return address in the e-mail headers. The e-mail messages, created to resemble a letter from a female author, included a built-in hypertext link to an adult

entertainment Web site. AOL said the e-mailing was made to look like it originated from accounts at "aol.com" and incorporated AOL's registered trademark and service mark (complaint page 6). In ordering Over the Air Equipment to stop sending the messages, the court said there was substantial evidence presented that AOL would prevail under the Computer Fraud and Abuse Act in its claims of trespass and computer fraud. Over the Air Equipment agreed to pay AOL what was described as a substantial, but undisclosed amount in damages ("AOL victorious in spam skirmish", 1997).

Alleging false designation of origin and false description under 15 U.S.C. § 1125, Juno Online Services, the world's second-largest on-line service provider, late in 1997 filed a $5 million dollar lawsuit against five known spammers and 10 that had yet to be identified for using its name as a return address in e-mail headers (*Juno Online Services, L.P., v. Scott Allen Export Sales,* 1997). Juno said its domain name, "juno.com" was designated as the origin of thousands of "dubious commercial offers and financial schemes peddled on the Internet," resulting in substantial and irreparable damage to its reputation (at p. 10). Juno also filed civil charges for misappropriation of name and identity, misrepresentation and common law fraud.

In 1998, the lawsuits continued to become more complex and, in some cases, service providers had invoked state laws to deal with spammers. In *America Online, Inc. v. Prime Data Systems* (1997), millions of unsolicited e-mail messages advertising computer software programs designed to enable users to create and transmit their own bulk e-mail were involved. AOL filed suit under Federal computer law, Virginia computer law and Virginia common law.

Adding to on-line consumer distaste for unsolicited e-mail is the fraudulent nature of some spam offers. Although beyond the scope of this discussion, legal questions about the products being offered, in addition to the delivery mode, are compounding complaints about unsolicited e-mail.

Among the spam-related consumer lawsuits:

- A judgement in a Texas court against a spammer who fraudulently used the domain name "flowers.com" as an electronic return address to send millions of unsolicited bulk e-mail messages (*Parker v. CN Enterprises,* 1997). The mailing offered "valuable" information about how to obtain "Free Cash Grants" (at 17).
- A lawsuit filed by the New York Attorney General against Woodside Literary Agency for using the Internet to attempt to defraud aspiring writers out of hundreds of dollars. The company allegedly posted messages on the Internet promising to sell literary work to major publishers in exchange for reading and contract fees (*New York v. Woodside Literary Agency,* 1997).
- A ruling in New York upholding the Attorney General's power to shield consumers from misleading on-line advertisements. The case involved a scam to entice consumers into sending money for magazine subscriptions that were never delivered (*People v. Lipsitz,* 1997).

The Federal Trade Commission and U.S. Postal Inspection Service both monitor junk e-mailers for fraud and report that the agencies have put more than a thousand

bulk e-mailers on notice that they will be tracked (Federal Trade Commission, 1998). Both agencies can prosecute unsolicited commercial e-mailers who violate the FTC Act or U.S. Postal Statutes, but only for fraud or when false and deceptive advertising is involved. Neither agency has any specific jurisdiction over unsolicited commercial e-mail. Such authority, assuming legislation could be drafted to satisfy the First Amendment, would have to come from Congress.

In summary, there have been legal developments arising from civil and criminal lawsuits against originators of unsolicited e-mail. Spammers have faced prosecution under civil, federal, and in some cases, state law. In *AOL v. Cyber Promotions*, a Federal District judge ruled that there is no right to send unsolicited e-mail under the First Amendment. In other cases, the courts have ruled that bulk e-mailers violate federal law when they disguise and misrepresent the origin of e-mail, trespass on private computer systems, overload computer servers, and infringe on trademarks. The Electronic Communications Privacy Act has also been enforced against spammers.

Although the development of case law to support the prosecution of spammers may be helpful in solving the UCE problem, relying on lawsuits as a deterrent does not directly address the problem at its source. Spammers are still free to send unsolicited e-mail and will continue sending it as long as there are economic incentives to do so. Lawsuits and injunctions may help create an environment where spamming is discouraged, but the threat of legal action does not place control over unsolicited e-mail with the receiver. ISPs are relying on lawsuits primarily as a way to protect their economic interests, not the interests of end users.

ISPs themselves and others in the Internet community realize that if they are going to be successful in bringing the UCE problem under control, they are going to have to get the attention of Congress.

Legislation

Lawmakers at both the federal and state level have reacted to complaints about junk e-mail with legislation. Proposals to regulate spammers vary widely in what they would require, from consumer protection and labeling requirements to a ban on UCE. A number of the bills have been written to amend existing laws that regulate junk faxes and telephone solicitation. Most of the proposals are controversial, either because they do too little, too much or are too market driven (Jacobs, 1997). Legislative proposals have attracted criticism from the Internet community, public interest groups, and the marketing industry. In this section, legislative solutions are discussed and analyzed in the context of the First Amendment and the test for commercial speech described in the second section.

Legislation that would regulate unsolicited commercial e-mail can be grouped into three categories for First Amendment analysis. In the first category are bills that would impose a ban on unsolicited commercial e-mail unless specific labeling requirements were met, such as H.R. 1748, the Netizens Protection Act of 1997 *(H.R. 1748,*

Netizens Protection Act of 1997). In the second category are bills such as S. 1618 and its House companion, H.R. 3888, The Anti- Slamming Amendments Act (*S. 1618: The Anti-Slamming Amendments Act, 1998*) (*H.R. 3888: The Anti-Slamming Amendments Act, 1998*), that would not ban UCE, but would require labeling requirements and consumer advisories, message elements regarded as forced speech. Legislation that would call for industry self-regulation and voluntary guidelines, such as H.R. 2368, The Data Privacy Act of 1997 (*H.R. 2369:The Data Privacy Act of 1987, 1987*), is grouped into a third category. Miscellaneous legislation such as H.R. 4124 (*H.R. 4124: E-Mail User Protection Act of 1998*) and H.R. 4176 (*H.R. 4176: Digital Jamming Act of 1998*), neither of which raise First Amendment issues, are addressed separately.

Under the first prong of the intermediate scrutiny test the court has developed for commercial speech, fraudulent and misleading UCE, an umbrella category under which most Spam can be placed,[6] receives no First Amendment protection. While eliminating most Spam, determining which marketing schemes and messages are fraudulent creates another problem that, depending on the nature of the scam, could be both difficult and time consuming to establish.

Eliminating unlawful and misleading Spam would subject "legitimate" UCE to the remaining three prongs of the commercial speech test. Under the second prong, the government's substantial interest in regulating UCE could be justified based on either the detrimental clogging effect that bulk e-mailings have on data networks or on a cost shifting rationale similar to the one that was upheld by the court in the regulation of junk faxes (*Destination Ventures, infra*). If legislation were to be narrowly drawn so as to directly advance the government's interest in alleviating the financial burden imposed on ISPs and users, limitations on commercial speech could survive the remaining third and fourth prongs of the commercial speech test. Since regulations do not have to be the least restrictive means necessary, the legislature would have some flexibility in drafting a spam bill.

Legislation in the first category that would impose a ban on unsolicited commercial e-mail unless the sender already has a preexisting and ongoing relationship with the recipient or unless the message contains labeling requirements would be unlikely to survive constitutional review. A ban on UCE amounts to a content-based restriction on speech that, absent a compelling government interest under strict scrutiny, would violate the First Amendment. In addition, the bill is more extensive than necessary to serve the government's interest in alleviating the UCE problem.

By amending the TCPA to apply to UCE, Congress would also be inappropriately extending telephone and fax law to the interactive environment of the Net, an approach that does not consider the unique attributes of the medium (discussed *supra*). S. 1748 also imposes restrictions at the source, rather than at the receiver end where user choice is preferable.

Labeling requirements and consumer advisories in the second category that would require senders of UCE to label messages as advertisements and include information regarding the sender's e-mail address, postal address, real name and phone number is

forced speech. Before labeling can be imposed on UCE, consideration would have to be given to the First Amendment issues that are raised by compelling senders of UCE to identify their messages.

At the heart of the labeling issue is the requirement that speakers provide information about the nature and origin of a message that they would not ordinarily include. In the past, the Supreme Court has struck down labeling requirements. For example, in *Riley v. National Federation of the Blind* (1988), the Supreme Court invalidated a North Carolina statute that required professional fund raisers to disclose to potential donors the percentage of charitable contributions that were actually turned over to charity. The Court said that the requirement was content-based, because, "mandating speech that a speaker would not otherwise make necessarily alters the speech's content" (at 781). Riley follows a series of Supreme Court cases where compelled speech has been held to violate the First Amendment. *See e.g. Pacific Gas & Electric Co. v. Public Utilities Comm'n* (*Infra*); *Wooley v. Maynard* (1977); *Miami Herald Publishing Company v. Tornillo* (1974).

The Supreme Court, addressing anonymous speech in *McIntyre v. Ohio Elections Commission* (1995), invalidated as unconstitutional an Ohio statute that prohibited anonymous leafleting. The court, in a vigorous defense of anonymous speech said:

> The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation my be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry (at 7).

Anonymity, the Court said, was grounded in the tradition exemplified by the secret ballot and extended beyond the literary realm.

Considering the Court's position in *Riley* and *McIntyre*, any labeling requirement for UCE would have to be narrowly drawn so as to allow senders to protect their anonymity. Legislation requiring the name, physical address, e-mail address and telephone number of the person who created the message would likely be challenged, particularly if the message contained elements of non-commercial speech. Category two labeling requirements like those proposed by S. 771, S. 1618, and H.R. 3888 are, in their present form, unacceptable.

Other legislative requirements that address some of the more sophisticated tactics that spammers have been using to send bulk e-mail are not as problematic as labeling requirements. Regulations like those proposed by H.R. 4124 that would make it illegal to send unsolicited e-mail from unregistered or fictitious Internet domains to prevent recipients from replying could be addressed through statute, as long at the requirement does not encroach on the sender's right to remain anonymous. UCE sent from fictitious domains could be considered misleading under the first prong of the test for commercial speech. False designation of origin and false description is also a violation of federal law (15 U.S.C. 1125). Technical regulation could be imposed to

address techniques that spammers use to avoid mail filtering programs. Legislation that would require senders to comply with a recipient's request to stop sending future messages and measures, such as H.R. 4176, that would establish a national "do-not-contact" database for those who do not wish to receive UCE do not burden the First Amendment.

Category three legislation, or industry self-regulation proposals such as H.R. 2368, do not raise substantive constitutional questions. But industry self-regulation does raise issues to be discussed in the next session.

In summary, legislation aimed at regulating unsolicited commercial e-mail can be broadly grouped into three categories: Legislation that bans UCE and would run afoul of the First Amendment, bills that would require labeling of UCE and raise substantive First Amendment questions, and legislation that would create guidelines for industry self-regulation. Thus far, the legislative response to the UCE problem has fallen short of providing a user-based solution that would encourage, particularly with respect to anonymity, the free flow of ideas and information on the Internet.

Industry Self-Regulation

The fear that government might step in and regulate the Internet has, as it did with broadcast advertising in an previous era, spawned an industry response. Distinguishing between the different interests, especially when it comes to separating "legitimate" marketers from spammers, is not easy. Given the emergence of a new medium and its multi-billion dollar potential, it was inevitable that industry interests would surface in Congress.

Industry interests are reflected in legislative proposals such as H.R. 2368 and language in other bills that allow marketers to send UCE to people with which they have a preexisting and ongoing relationship. The Data Privacy Act would set up an industry group to establish voluntary guidelines for the interactive computer industry, including rules for the distribution of unsolicited commercial e-mail.

The marketing communication industry is using legislation to distance itself from spammers and to legitimize UCE. For example, marketers use terms like "direct e-mail," "electronic," and "database" marketing to distinguish the way they conduct business over the Net from the way spammers do (Hall-Smith, 1997, p. 48; Crotty, 1997, p. 36). The Direct Marketing Association (DMA) considers the over 50 million Americans connected to the Internet as a "direct marketing opportunity" and the Web as having "enormous potential" ("Direct Marketing Association," 1998). The DMA opposes UCE legislation, its president asserting that, "everyone will best be served by self-regulation" (Crotty, 1997, p. 36). The DMA's flashy, Java-driven Web site hawks the virtues of the Net and promotes an upcoming DMA conference on how to take advantage of the opportunities for Internet marketing. Whether unsolicited commercial e-mail is "marketing" or "spam" seems to be a matter of perspective.

The DMA maintains mail preference and telephone preference services, which allows consumers to remove their addresses and phone numbers from direct

marketing lists. The organization is also in the process of setting up a similar system for e-mail addresses (Deck & Hamblen, 1997). In addition to preference lists, the DMA promotes privacy and responsible marketing

The problem with industry self-regulation is that not everyone belongs to the DMA or similar organizations, which renders the DMA's lists and other efforts to promote responsible e-mail marketing marginally effective. The on-line industry and ISPs also have interests other than those of the DMA, as do the individuals and organizations that make up the broader Internet community. For competitive reasons, most in the industry keep to themselves. They do not share secrets and few will cooperate with efforts to track down spammers without a court order (Deck & Hamblen, 1997).

The industry self-regulation suggested by H.R. 2368 and similar legislative proposals is reminiscent of "codes" and rules of conduct that have been tried before. The National Association of Broadcasters (NAB) created rules for its members in an attempt to keep the government from imposing regulation on advertising only to have its NAB Code "widely ignored" (Barnouw, 1990, p. 356). The worst that could happen to a member for breaking a rule or regulation was expulsion from the association, which the NAB was reluctant to do. The NAB Code became controversial, the subject of a Department of Justice lawsuit and was later abandoned. The Justice Department said that advertising guidelines coerced broadcasters (Head & Sterling, 1987, p. 463). In the absence of evidence to the contrary, any argument that a similar code of Internet advertising conduct would fare any better than the NAB Code is unconvincing.

Given the choice between what will produce revenue and what will maximize user choice, profit will prevail over user preference. To the advertising and marketing industry, the Net represents a largely untapped source of revenue. The industry is unlikely to promote measures that will make it harder to market on the Net. With public trust in anti-competitive Internet giants such as Microsoft waning and the Justice Department's continued interest in Microsoft's operating practices ("The Feds' Case Against Bill Gates," 1998), Net users would consider ludicrous the suggestion that the Internet be left to industry self-regulation.

The Filtering Alternative

When measured against the original goals of solving the UCE problem with minimal government regulation and maximum user choice, none of the options discussed to this point have been entirely satisfactory. Although civil and criminal judgements against originators of UCE have helped establish legal precedents and may have created a deterrent to spamming, lawsuits by themselves will probably not completely eliminate the problem. Content-based government regulation of UCE is potentially unconstitutional, especially given the existence of source-based filtering technology that could, along with minimal structural regulation, provide a viable, First Amendment friendly solution.

Filtering technology is not new to the mass media. Filtering allows content to be

screened anywhere between the sender and receiver to block, or let through, material that meets certain criteria. Filtering software programmed to identify material that parents may find inappropriate for their children to access is growing in use.

For example, filtering technology is behind the television V-Chip, which was designed to block television programs that parents do not want their children to see. With the V-chip, programs are encoded by broadcasters before they are transmitted and screened at the receiver's television set. The way the V-chip evolved, however, did not make full use of the capabilities of the technology. Although the V-chip's inventor intended for parents to be able to set levels of violence, language and sex, the industry-developed structure, a legislative compromise, produced a movie-like rating system ("Jack of all trades: The man in the middle of the V-Chip,"1996).

With Web filtering software, a list of objectionable Web sites is compiled and then programmed into a browser, against which selected Web sites are compared. If content is encountered which is not acceptable according to the filter's pre-programmed rules, the material is blocked.

Computers that handle electronic communications can be programmed in much the same way. Currently, end users and ISPs can use e-mail filtering programs to reject e-mail that does not meet certain criteria. E-mail filtering can be accomplished in one of two ways, "opt-in" or "opt-out" filtering.[7] With opt-in filtering, users receive no mail unless incoming e-mail meets certain criteria. For example, unless a particular e-mail address is on a user's opt-in list, mail is rejected. Opt-out filtering works in the opposite manner. All e-mail sent to a user's mailbox is accepted unless the user has specifically instructed the software to reject mail from certain addresses. Users can turn filtering on or off, obtain lists of known spammers from their ISPs, or have their service provider filter mail for them.[8]

The filtering alternative, when subjected to the First Amendment test for commercial speech articulated by the Court in *Hudson*, provides a more viable solution to the spam problem. Under the first prong of *Hudson*, fraudulent and misleading UCE falls by the wayside as unprotected speech, leaving legitimate junk e-mail to face the remaining three prongs.

Under the second part of the *Hudson* test, the asserted government interest served by a labeling requirement allows ISPs and users to employ software to rapidly screen incoming e-mail for unsolicited commercial messages. In this role, the government helps ISPs and private individuals by putting in place regulations that assist them, thereby staying out of the decision process, consistent with *Rowan (infra)*. The requirement is no more intrusive on the First Amendment than consumer laws that require the contents of food packages to be identified. The decision to block spam is left to the recipient. Thus, the government's substantial interest in keeping UCE from inundating mailboxes and imposing costs on recipients is thereby achieved.

Requiring that spam be labeled only as commercial in nature avoids the issues associated with anonymous speech since the speakers themselves would remain nameless. The requirement would not block unsolicited commercial speech altogether, since marketers and advertisers would still have other means to reach

potential customers through consent arrangements, Web pages, the U.S. postal service, and conventional media.

One disadvantage of filtering as described here is that a simple labeling requirement can be used to block all unsolicited commercial e-mail, a proposal that is likely to draw fire from the advertising and marketing industries. This is where legislation could be written to allow the industry the option of coming up with a system under which consumers are given options, through industry supplied software, so consumers can choose what kinds of commercial messages they want to receive, when and from whom. More detailed screening, or granularity, could be permitted as long as the broad commercial labeling requirement was observed. This approach would also allow organizations like the DMA to put "opt out" lists to use. Software provided by Internet broadcaster Pointcast currently allows users to customize news and information services (Pavlik, 1998). Software programs and browsers could be easily modified to screen commercial messages, much as they are for indecent and pornographic content.

Although filtering could imposes costs on the receiving end because it requires an initial investment for software and time to maintain, filtering is preferable to censorship. Filtering parameters could also be difficult to maintain. However, if labels are kept simple, software maintenance will not be complicated nor time consuming.

Conclusion

Current First Amendment jurisprudence does not support a complete ban on UCE. Labeling requirements that would require senders to identify themselves may also be challenged on free speech grounds. The simplest solution, legislation to require message headers designed to identify UCE as "advertisement," would present a narrowly-tailored means to achieve the government's interest in enabling Internet users to filter unsolicited commercial e-mail.

The likelihood of any legislation that might upset the powerful, commercial media interests that are driving the development of the Internet is doubtful. Congress, sensitive to the media it must rely on to be re-elected, has attempted to straddle the fence between what the industry wants and what users would prefer. The result has been the appearance of legislation that may be unconstitutional, does too little, favors industry interests and/or is directed at legitimizing UCE for marketing by putting "spammers" out of business. If the industry is given the option of putting in place a voluntary system under a broader labeling requirement, other questions arise. Would the marketing industry do so without being forced? And if the industry did, would the resulting system be plagued by industry-mediated problems similar to the ones that characterize the watered-down version of television's V-chip?

The growth in civil and criminal lawsuits against spammers is an unexpected, but relevant development in Internet law. A Federal judge's ruling that the First Amendment does not protect the right to send unsolicited commercial e-mail has established important legal precedent that supports a policy goal of user choice.

Another encouraging development is the effect that a recent $2 million dollar settlement in a case involving Cyber Promotions, a defendant in several spam-related lawsuits, had in driving the company out of business (Branscum, 1998). Given the risky legal climate for spammers and the stigma that has become attached to UCE, there is some evidence that the spam problem may be waning as the Net grows beyond infancy and into its toddler years.

Addressing the spam issue does not require extensive government regulation, nor should industry-influenced legislation legitimize UCE as "direct marketing." If Congress passes anti-spam legislation that places restrictions on UCE, spammers and marketers who do not wish to play by the rules will simply set up their operations overseas, much as have purveyors of adult-oriented Internet smut.

In the end, what is sorely needed is a guide for U.S. communications policy that has at its core the spirit of free speech and the free flow of ideas. If legislation that bans or requires extensive labeling of UCE works its way through Congress and is signed into law, a Supreme Court showdown is likely.

Ultimately, users, not government or private industry, will be called to play the lead role when it comes to addressing the Internet's problems. Problems in Cyberspace should be resolved in favor of the public, rather than commercial interests. Otherwise, the full potential of the maturing Internet as a democratizing medium for society and as conduit for ideas, information and commerce will not be realized.

References

15 USC Sec. 1126. (1996). False designations of origin, false descriptions, and dilution forbidden.

America Online again takes aim at operators of pornographic Web sites. (1998, March 4). [On-line], Available: http://www-db.aol.com/corp/news/press/view?release=291&

America Online, Inc. v. Cyber Promotions, Inc. (1996). 948 F. Supp, 436. E.D. Pa.

America Online, Inc. v. Over the Air Equipment, Inc., and Joe Tajalle, Civil Action No. 97-____. (1997, 4 November). United States District Court for the Eastern District of Virginia, Alexandria Division.

America Online, Inc. v. Prime Data Systems, Inc., Prime Data Worldnet Systems, Inc., and Vernon N. Hale, Civil Action No. 97-____, (E.D. Va., 1997).

AOL Legal. (1998, 3 March). Legal Department @ AOL [On-line], Available: http://legal.web.aol.com

AOL victorious in spam skirmish. (1997, 18 December). Wired News. [On-line], Available: http://www.wired.com/news/ politics/story/9265.htm

Bigfoot Partners, L.P. v. Cyber Promotions, Inc. and Sanford Wallace. (1997, 6 October). United States District Court, Southern District of New York.

Barnouw, Erik. (1990). *Tube of plenty*. New York: Oxford.

Branscum, Deborah. (1998, June 22). The big spam debate. *Newsweek*. pp. 84&86.

Board of Trustees of the State University of New York et al. v. Fox et al., 492 U.S. 469, 476 (1987).

Bolger v. Youngs Drug Products Corp. 463 U.S. 60, 72. (1983).

A brief history of junk (1998, 6 March) Federal Trade Commission. [On-line], Available: http://www.ftc.gov/bcp/privacy2/comments1/junk/variety.htm

Central Hudson Gas & Electric v. Public Service Commission. (1980). 447 U.S. 447, 557.

City of Cincinnati v. Discovery Network, Inc., et al., 507 U.S. 410 (1993).

Cohen, A. (1997, 15 September). Can the Spam: Bills declare war on junk E-mail. *New York Law Journal*, p. 1.

CompuServe Inc., v. Cyber Promotions, Inc. and Sanford Wallace, Case No. C2-96-1070. (1996, 9 May). United States District Court, Southern District of Ohio.

Computer Fraud and Abuse Act (1996). 18 U.S.C. 1039(5)(A).

Concentric Network Corporation, Inc. v. Sanford Wallace and Cyber Promotions [Case No. C-96 20829-RMW(EAI). (1996, 5 November). United States District Court, Northern District of California, San Jose Division.

Cranor, L. & LaMacchia, B. (1998) Spam! Communications of the ACM. [On-line], Available: http://www.research.att.com/~lorrie/pubs/spam/spam.html

Crimes - Electronic Mail Misuse - Penalties [Maryland House Bill 778]. (1997).

Crotty, C. (1997, November). Stopping junk E-mail. *Macworld*, p. 34.

Deck, S., & Hamblen, M. (1997, 18 August). Spam attacks send angry firms to court. *Computerworld*, p. 1.

Destination Ventures, Ltd. V. F.C.C. (1993). 844 F. Supp. 632; 1993 U.S. Dist. LEXIS 19917; 22 Media L. Rep. 1171.

Destination Ventures, Ltd. v. F.C.C. (1995). 46 F.3d 54. United States Court of Appeals, Ninth Circuit.

Direct Marketing Association web site. (1998, 3 March). [On-line], http://www.the-dma.org

Douglas K. Snow v. Daniel Doherty. (1997). *Civil Action File No. 3:97-CV-0635 (RM)*. U.S. District Court for the Northern District of Indiana, South Bend District.

Earthlink v. Cyber Promotions, Inc. (1997, 7 May). L.A. Super. Ct.

Edenfield v. Fane, 507 U.S. 761 (1993).

Electronic Privacy Communications Act of 1986, 18 U.S.C. 2701(a).

Federal Communications Commission v. Pacifica Foundation. 438 U.S. 726 (1978) (Quoting Justice Sutherland in Euclid v. Ambler Realty Co., 272 U.S. 365, 388) (1926).

Federal Trade Commission. (1998, 2 February). Junk E-Mailers [On-line], Available: http://www.ftc.gov/opa/9802/junk.htm

H.R. Rep. No 317, 102d Cong., 1st Sess. p. 10, 1991

H.R. 1748, Netizens Protection Act of 1997 (105th Congress, 1st Session). (1997). Washington, D.C.

H.R. 2368, Data Privacy Act of 1997 (105th Congress, 1st Session). (1997). Washington, D.C.

H.R. 3888, The Anti-slamming Amendments Act (105th Congress, 1st Session). (1998). Washington, D.C.

H.R. 4124, E-Mail User Protection Act of 1998 (105th Congress, 2d Session). Washington, D.C.

H.R. 4176, Digital Jamming Act of 1998 (105th Congress, 2d Session). Washington, D.C.

Hall-Smith, V. (1997, February). Direct your pitch. *Small Office*, pp. 48-49.

Head, S., & Sterling, C. (1987). *Broadcasting in America*. Boston: Houghton Mifflin Co.

Hewitt, M. (1997, 17 July). It's high time for e-mail senders to can the Spam. *Marketing*, p. 16.

Internet E-Mail: The campaign against junk E-mail (1997, March 11). [On-line], Available: http://legal.web.aol.com

Jack of all trades: The man in the middle of the V-Chip. (1996, 18 March). *Broadcasting & Cable*, p. 28.

Jacobs, P. (1997, 3 November). Privacy: What you need to know. *Infoworld*, pp. 111-112.

Juno Online Services, L.P., v. Scott Allen Export Sales, No. 97 Civ. 8694 (S.D.N.Y). (1997, 21 November.).

Macavinta, C. (1997, 20 January). Nevadans against spam. *CNet News*.

McIntyre v. Ohio Elections Commission, 115 S. Ct. 1511 (1995).

Miami Herald Publishing Company v. Tornillo, 418 U.S. 241 (1974).

New York v. Woodside Literary Agency (1997). [On line], Available: http://www.techweb.com/wire/story/TWB19971202500009

Ohio Revised Code Section 2913.01-04. Ohio Fraud and Theft Law. (1996).

Parker v. CN Enterprises (Tex.Travis County Dist. Ct., Sept. 17, 1997).

Pacific Gas and Electric Co. v. Public Utilities Commission of California, 475 U.S. 1 (1986).

Pavlik, J. V. (1998) New Media Technology: Cultural and Commercial Perspectives, 2nd Edition. Boston, Allyn & Bacon. p. 170

People v. Lipsitz, ____N.Y.S.2d____, 1997 N.Y. Slip. Op. 97, 459, 1997 N.Y. Misc. Lexis 382, 1997 WL 555721 (N.Y. Sup. Ct., June 23, 1997).

Prepared Statement of the Federal Trade Commission on "Unsolicited Commercial E-Mail." (1998, June 17). [Senate Hearing]. Hearing before the Subcommittee on Communication of the Senate Committee on Commerce, Science and Transportation. United States Senate. Washington, D.C. [On-line], Available: http://www.ftc.gov/os/9806/email.htm

Prodigy v. Cyber Promotions, Inc. (1996, 13 December). United States District Court, Southern District of New York.

Red Lion Broadcasting Co. v. Federal Communications Commission, 395 U.S. 367 (1969).

Reno, Attorney General of the United States, et al. v. American Civil Liberties Union et al., 521 U.S. 844 (1997).

Riley v. National Federation of the Blind, 487 U.S. 781 (1988).

Rowan v. U.S. Post Office Dept. 397 U.S. 728, 737 (1970).

S. 1618, Anti-Slamming Amendments Act of 1998 (105th Congress, 2d session). 1998. Washington, D.C.

S. 771, Unsolicited Commercial Electronic Mail Choice Act of 1997 (105th Congress, 1st session). (1997). Washington, D.C.

S. 875, Electronic Mailbox Protection Act of 1997 (105th Congress, 1st session). (1997). Washington, D.C.

Service Mark Infringement, 15 U.S.C. 1114(1).

Simons, J. (1997, 12 May). The battle over spam gets ugly. *U.S. News & World Report,* p. 55.

Sullivan, R. L. (1996, 22 January). "You've got spam!" *Forbes,* p. 38.

Telephone Consumer Protection Act of 1991, 47 U.S.C. §227.

The Feds' case against Bill Gates. (1998, 9 March). *Newsweek,* pp. 42-43.

Voters Telecommunications Watch. (1997). *Final Comments to the Federal Trade Commission on Unsolicited Commercial Email.* Washington, D.C.

Wooley v. Maynard, 430 U.S. 705 (1977).

Notes

[1] "Spam" is slang for junk e-mail. Some trace its origin to a Monty Python Flying Circus sketch in which a man repeats the word "spam" over and over until it drives everyone crazy (Cohen, 1997; Hewitt, 1997). Hormel Foods, the company that owns the "Spam" ® trademark is taking advantage of the product's new found fame to market Spam T-shirts, mugs and Spam mouse pads from its World Wide Web (WWW) home page (Sullivan, 1996). Throughout this paper "UCE," "junk e-mail," "spam," and their various forms will be used as equivalents.

[2] The best summary the author found of how easy it is to become a "spammer," including the reference to software programs designed to facilitate spamming, was found in *America Online, Inc. v. Prime Data Systems, Inc, Prime Data Worldnet Systems, Inc., and Vernon N. Hale* (1997).

[3] The practice, known as "forgery," is discussed in the *Juno Online Services, L.P. v. Scott Allen Export Sales.*

[4] E-mail "bombing" is described in America Online, Inc. v. Cyber Promotions, Inc.

[5] The author found regularly updated lists of unsolicited commercial e-mail cases at: [http://www.jmls.edu/cyber/cases/spam.html#aol-oa] [http://legal.web.aol.com/emailindex.html.

[6] Cranor and LaMacchia (1998) found support for the general perception among users that most spam advertises adult entertainment or offers fraudulent products or services.

[7] The author found a good explanation of filtering in the Electronic Frontier Foundation's "Final Comments to the Federal Trade Commission on Unsolicited Commercial Email." (www.eff.org).

[8] ISPs prefer to filter "upstream" at the point of delivery before bulk e-mail inundates a provider's server. The goal of achieving maximum user choice, however, is not best served by upstream filtering.